SUSCEPTIBILIDADE DOS USUÁRIOS AOS RISCOS DE REDES WIRELESS PÚBLICAS

RENATO MARINHO

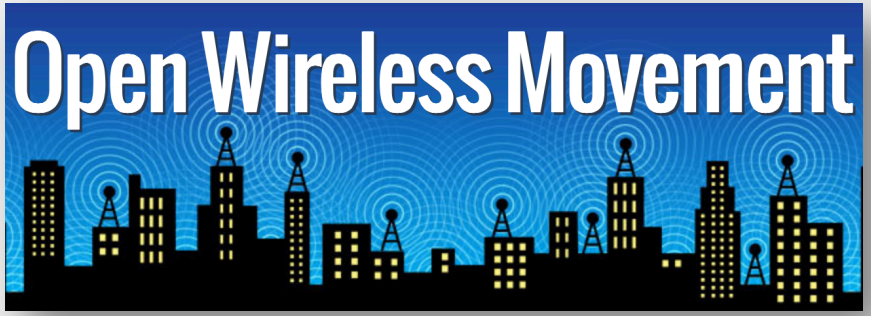
MSc, CISSP, CRISC

MORPHUS LABS

MORPHUS
SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

IMAGINE A FUTURE WITH UBIQUITOUS OPEN INTERNET.



INTRODUÇÃO

PROJETO LINKNYC

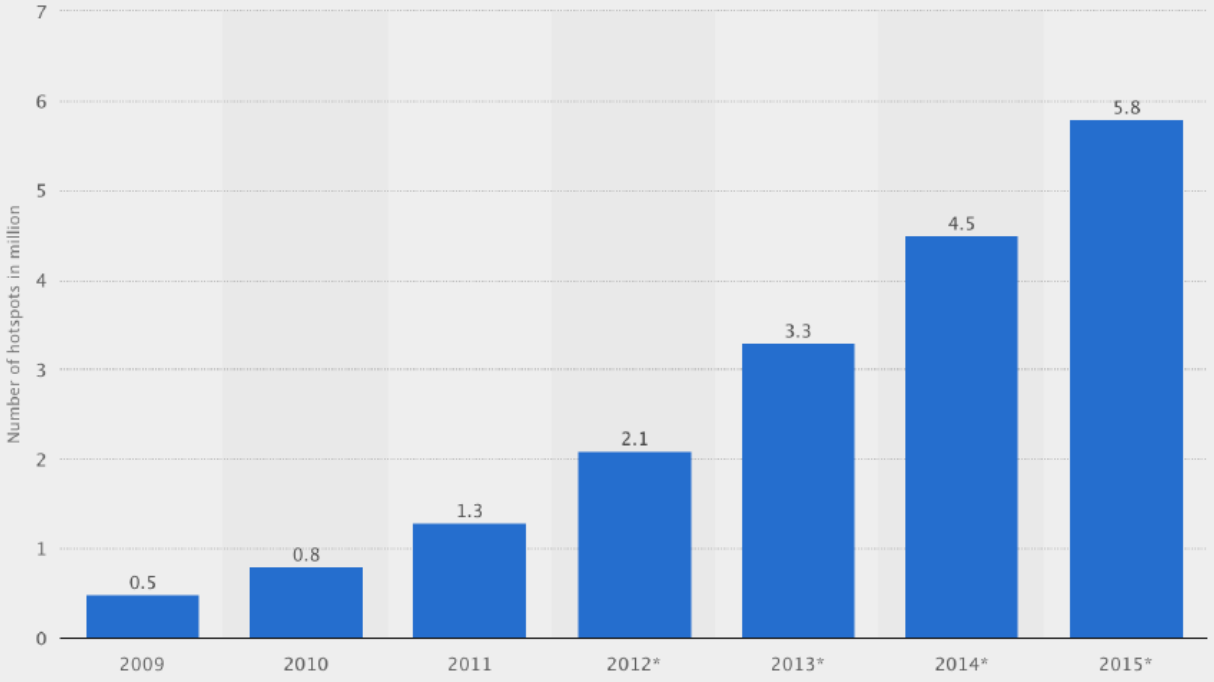
10.000 FREE WIFI HOTSPOTS

MORPHUSLABS

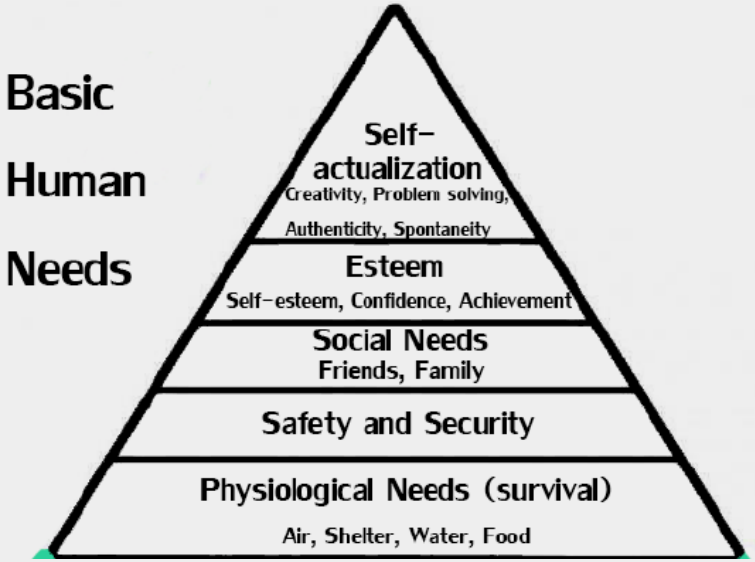
MORPHUS
SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

2015 - 5.8 MILLION PUBLIC WIFI HOTSPOTS



INTRODUÇÃO


Basic
Human
Needs
Self-actualization
Creativity, Problem solving,
Authenticity, Spontaneity
Esteem
Self-esteem, Confidence, Achievement
Social Needs
Friends, Family
Safety and Security
Physiological Needs (survival)
Air, Shelter, Water, Food

SEGURANÇA

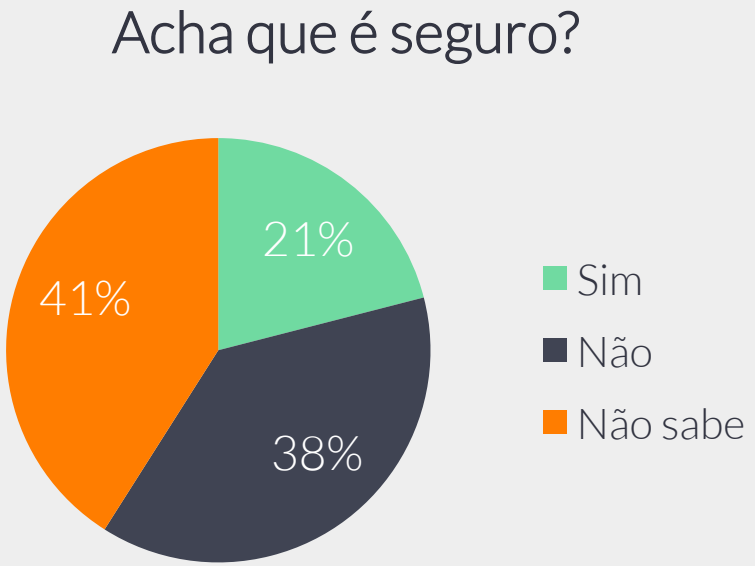
AMEAÇAS
- Evil twin
- Man-in-the-middle
- Ssl strip
- Jasager

IMPACTOS
- Vazamento de dados
- Roubo de identidade
- Ataques e implantação de malware
- Redirecionamentos

Jasager + SSL Strip Attack

Trabalho Relacionado

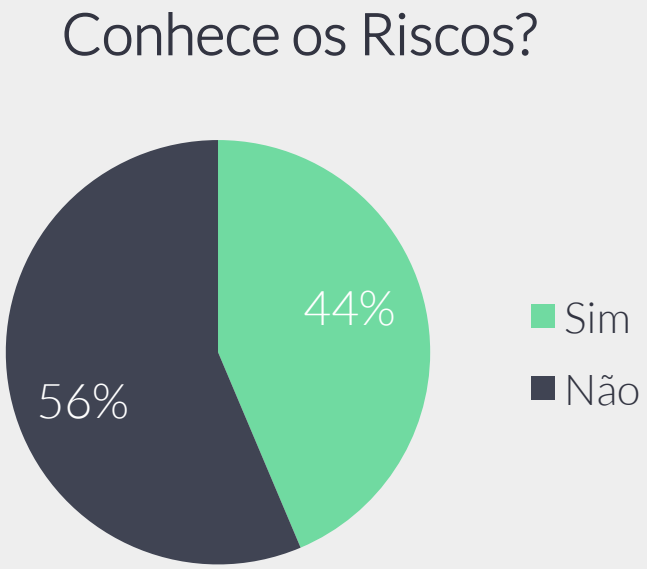
PERCEPÇÃO DO USUÁRIO
FINAL SOBRE A SEGURANÇA
DE REDES WIRELESS
PÚBLICAS [1]



[1] Attipoe, Elliot Kojo, et al. "End User's Perception about Security of the Public Wireless Network." *International Journal of Societal Applications of Computer Science* 2.8 (2013).

Trabalho Relacionado

PERCEPÇÃO DO USUÁRIO FINAL SOBRE A SEGURANÇA DE REDES WIRELESS PÚBLICAS [1]

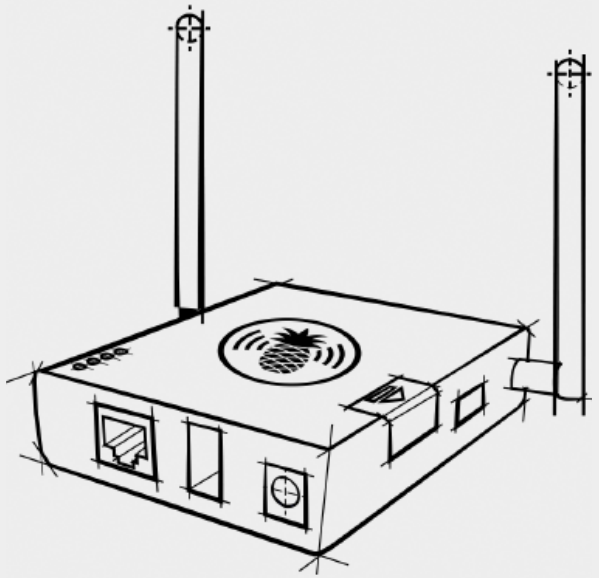


Apenas 29% foi capaz de diferenciar um site seguro de um inseguro

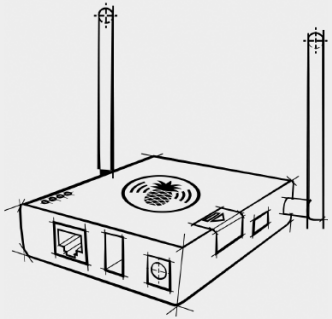
PESQUISA - OBJETIVOS

- Avaliar, na prática, o nível mínimo de consciência dos usuários sobre os riscos de redes Wireless Públicas;
    - Os usuários seriam capazes de aceitar um **certificado digital inválido** numa conexão pública e desconhecida?
    - Os usuários seriam capazes de aceitar **abusivos termos de uso** da rede? Quanto tempo dedicam à sua leitura?
    - O **nome da rede** sem fio influenciaria na confiança do usuário? Em qual proporção?
    - Os ambientes que oferecem redes WiFi públicas oferecem alguma **proteção física ou tecnológica** aos seus visitantes?
    - A **plataforma do dispositivo** do usuário influeniaria nos resultados? De que forma?

METODOLOGIA



METODOLOGIA



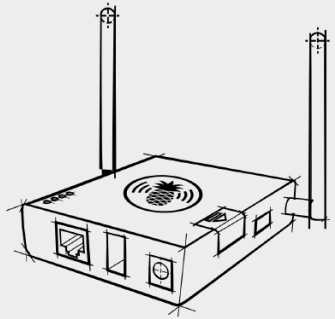
Roteador Wifi

- Portátil
- Bateria de longa duração
- Flexível – permitir ajustes de configurações

WiFi Pineapple Mark V

METODOLOGIA

SSID
de contexto



SSID
Genérico

Rede e Internet

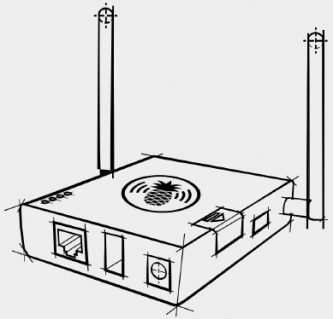
- Anúncio de 2 SSIDs – um dentro do conexto do ambiente e outro for a;
- Não foi oferecida conexão Internet aos participantes da pesquisa;
- Dnsmasq para resolução de nomes e abertura do Captive Portal

```
# Provide an alias for a "local" DNS name. Note that this _only_ works
# for targets which are names from DHCP or /etc/hosts. Give host
# "bert" another name, bertrand
# The fields are <cname>,<target>
#cname=bertand,bert
address=/#/200.200.200.200


root@Pineapple:/etc# nslookup www.uol.com.br 127.0.0.1
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      www.uol.com.br
Address 1: 200.200.200.200
root@Pineapple:/etc#
```

MORPHUS LABS MORPHUS SEGURANÇA DA INFORMAÇÃO

METODOLOGIA

SSID
de contexto



SSID
Genérico

Device	IP	MAC	SSID	Certificado?	Termos
MBP-de-Renato	172.16.43.192	60:03:08:8e:56:54	CIO FREE	Sim	Sim
android-e82af3a02e0f7267	172.16.44.113	00:37:6d:de:8a:eb	GVT-B301	Sim	Sim
iPhonediColares	172.16.43.249	64:9a:be:9e:71:1d	CIO FREE	Sim	Sim
iPhonedeWALLACE	172.16.43.130	b4:f0:ab:8b:f2:32	CIO FREE	Sim	Sim
android-b999f7292efe545	172.16.44.101	9c:d9:17:9f:5d:93	GVT-B301	Nao	Nao
android-d39cd9ae1aee619c	172.16.43.131	9c:d9:17:fd:2a:32	CIO FREE	Nao	Nao
android-d39cd9ae1aee619c	172.16.44.130	9c:d9:17:fd:2a:32	GVT-B301	Nao	Nao
iPhonedeKatrine	172.16.43.219	84:38:35:aa:e1:75	CIO FREE	Sim	Nao
android-f960466c764cbcef	172.16.43.204	64:89:9a:04:dc:20	CIO FREE	Sim	Sim
android-496dba4b6bbd7274	172.16.44.227	84:38:38:0c:ec:ab	GVT-B301	Nao	Nao
android-496dba4b6bbd7274	172.16.43.227	84:38:38:0c:ec:ab	CIO FREE	Nao	Nao
android-2995fbff64252843	172.16.43.153	60:be:b5:97:25:65	CIO FREE	Nao	Nao
riquephone	172.16.43.245	d8:bb:2c:1e:3f:a9	CIO FREE	Sim	Sim
android-17187df5a765219	172.16.43.158	14:1a:a3:ab:da:1e	CIO FREE	Nao	Nao
iPhonedeRaissa	172.16.44.138	28:e1:4e:5b:79:02	GVT-B301	Nao	Nao
iPhonedeRaissa	172.16.43.138	28:e1:4e:5b:79:02	CIO FREE	Nao	Nao
iPhone-de-Alyne	172.16.43.226	ac:fd:ec:98:a4:9e	CIO FREE	Sim	Sim
android-1bd0fd5c6b7c559b	172.16.43.121	84:38:38:fc:be:e9	CIO FREE	Nao	Nao
android-9c6335fcfcfbb535f	172.16.43.120	00:1a:13:72:7e:08	CIO FREE	Nao	Nao
android-d39cd9ae1aee619c	172.16.43.130	9c:d9:17:fd:2a:32	CIO FREE	Sim	Nao
MacBook-Pro	172.16.43.117	e8:bc:e8:e1:99:ef	CIO FREE	Nao	Nao
android-817ce43efdf31443	172.16.43.173	78:4b:87:75:99:23	CIO FREE	Nao	Nao
Tiberio	172.16.43.216	98:03:d8:ae:32:14	CIO FREE	Sim	Nao
MBP-de-Marcelo	172.16.43.228	3c:15:c2:dc:c6:8a	CIO FREE	Sim	Sim
Air-de-oswaldo	172.16.44.242	8c:29:37:eb:a6:60	GVT-B301	Sim	Sim
Air-de-oswaldo	172.16.43.242	8c:29:37:eb:a6:60	CIO FREE	Sim	Sim
android-f66a8469852954fd	172.16.44.229	1c:af:05:e1:b7:59	GVT-B301	Nao	Nao
android-f7e19d019846aaf3	172.16.44.235	18:22:7e:01:57:85	GVT-B301	Nao	Nao
iPhoneMarcelo80ares	172.16.43.128	80:ea:96:d2:a5:e4	CIO FREE	Sim	Sim
android-9a40cfbfb162b898	172.16.43.221	cc:07:ab:12:9e:9d	CIO FREE	Nao	Nao
android-2a624e7d0a87a72d	172.16.44.170	a8:7e:01:33:5f:46	GVT-B301	Nao	Nao
android_bae1a865fcf5ab2	172.16.44.109	80:96:b1:3e:af:37	GVT-B301	Nao	Nao

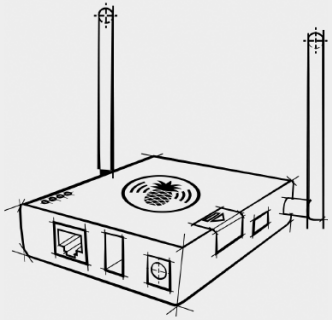
Download CSV

Locais de Pesquisa

- 8 locais de acesso público em Fortaleza
- Restaurantes, Salas de Cinema e Shopping Centers;
- Equipamento exposto ;
- 3 horas em média em cada local aguardando os usuários.

METODOLOGIA

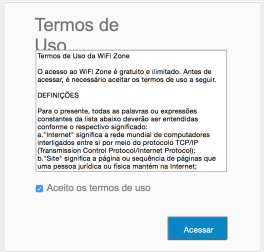
SSID
de contexto



SSID
Genérico

Certificado Digital Inválido

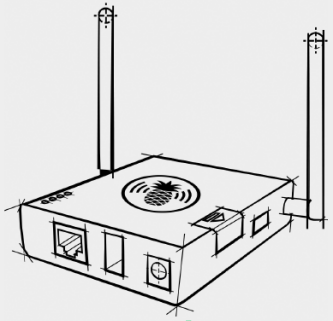
- Usuário direcionado a URL HTTP;
- Redirecionamento HTTPs;
- de Certificado Digital Auto Assinado;
- Registro da atitude dos usuários.



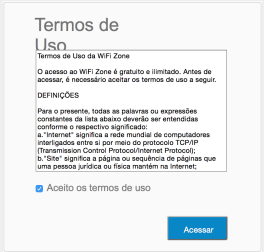
MORPHUSLABS MORPHUS SEGURANÇA DA INFORMAÇÃO

METODOLOGIA

SSID
de contexto



SSID
Genérico

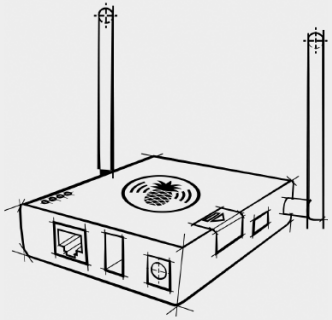


Termos de Uso da Rede

- Texto genérico de 72 linhas;
- Cláusulas abusivas: “informações sigilosas, como senhas e e números de cartões de crédito, serão capturadas durante a conexão”;
- Registro do tempo de leitura.

METODOLOGIA

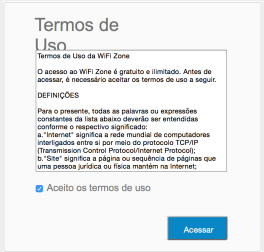
SSID
de contexto

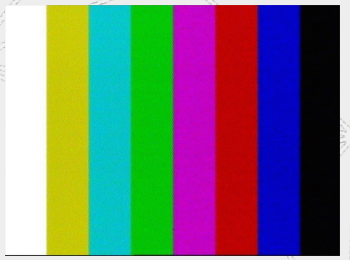


SSID
Genérico

Encerramento

- Tela indicando que o hotspot estava for a de serviço.





MORPHUSLABS
MORPHUS
SEGURANÇA DA INFORMAÇÃO

METODOLOGIA – INDICADORES

INDICADORES

SSID selecionado (nome da rede)

Endereço IP

Endereço MAC

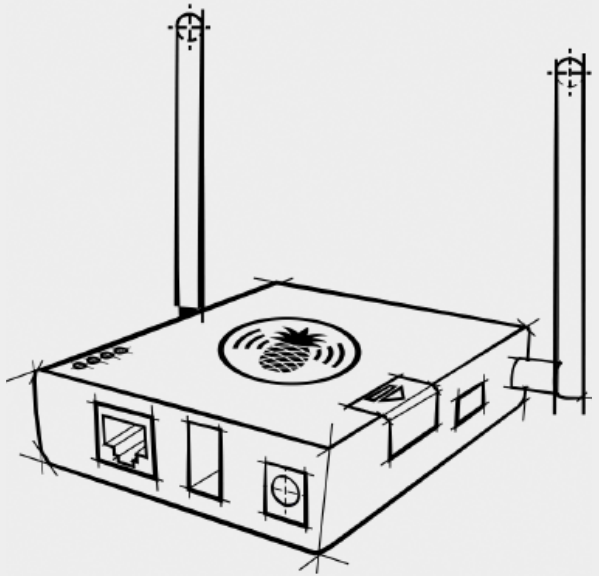
Tipo de dispositivo

Aceite do Certificado Digital Inválido

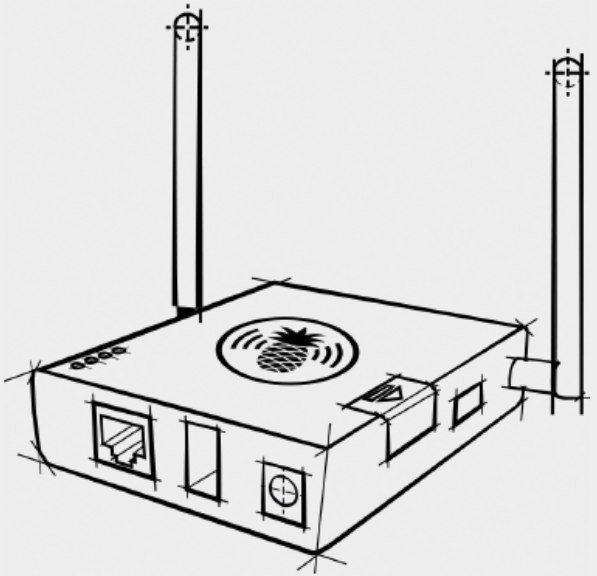
Aceite dos Termos de Uso

Tempo de leitura dos Termos

Possíveis impedimentos físicos ou tecnológicos



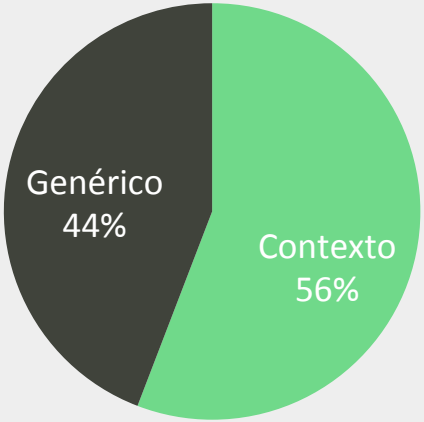
RESULTADOS



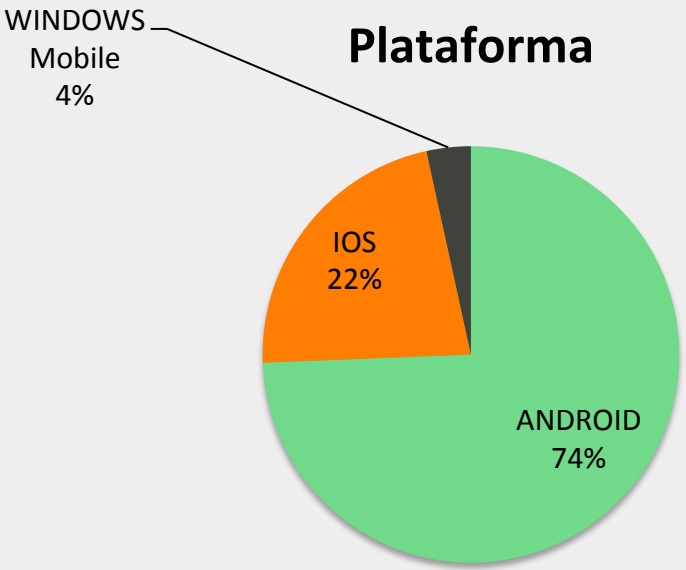
RESULTADOS

Total de 437 participantes

SSID (Rede)



Plataforma



RESULTADOS

Indicador	Aceite Certificado Digital	Aceite Termos de Uso	Tempo de Leitura dos Termos
Global			
SSID Contexto			
SSID Genérico			
Android			
IOS			
Windows Mob			
Android + SSID Contexto			
IOS + SSID Contexto			
Windows Mob + SSID Contexto			

CONCLUSÕES

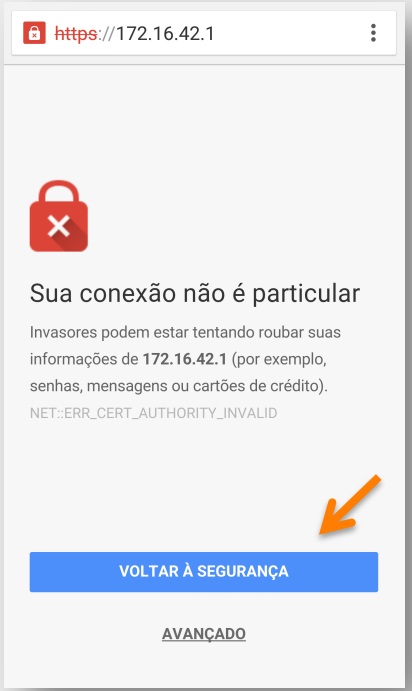
- Mesmo em um cenário com ameaça explícita, **39% dos usuários** aceitaram o risco;
- **82% dos usuários** concordaram que suas informações seriam capturadas naquele acesso. Em média 27 segundos na leitura dos termos;
- O **nome da rede** sem fio aumenta a confiança dos usuários em **77%**;
- Nenhum ambiente ofereceu resistência ou proteção aos experimentos;
- A **plataforma do dispositivo** do usuário teve uma forte influência: um atacante teria sucesso em **71% dos usuários de IOS.**

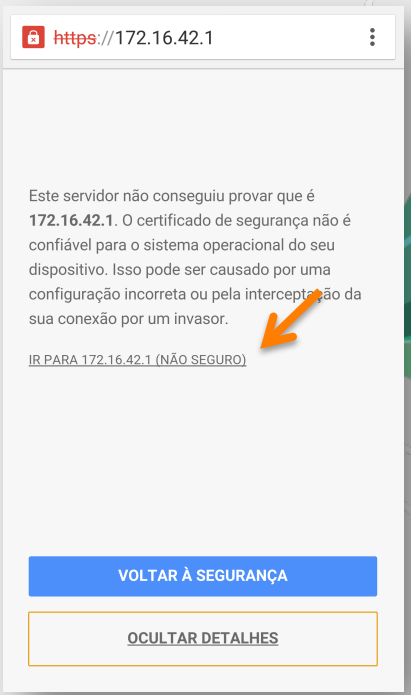
CONCLUSÕES

AMBIENTE IOS/MAC OS

CONCLUSÕES

AMBIENTE ANDROID





TRABALHOS FUTUROS

Estamos trabalhando em uma proposta de segurança colaborativa para redes wifi públicas.

OBRIGADO!

MORPHUS LABS

MORPHUS
SEGURANÇA DA INFORMAÇÃO