

'17 DISI

DIA INTERNACIONAL DE SEGURANÇA  
EM INFORMÁTICA

**RANSOMWARE**  
NÃO SEJA VÍTIMA DE  
SEQUESTRO VIRTUAL



# iBLISS

Vetores de acesso para  
ataques de ransomware

Alexandro Silva

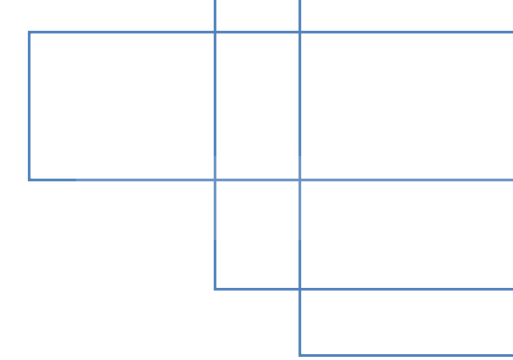
# \$ Intro

- ❖ **Gerente de Operações na IBLISS Digital Security;**
- ❖ **Professor;**
- ❖ **Co-fundador da Nullbyte Security Conference;**
- ❖ **Github: <https://github.com/alexoslabs>**

# Vetores de ataque



# Vetores de ataque



Tecnologia

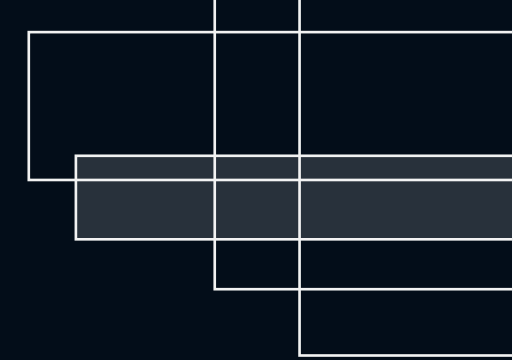


Processos



Pessoas

# Tecnologia



# Tecnologia



**70%**  
das vulnerabilidades  
encontradas podem  
impactar  
significativamente o  
negócio



**92%**  
das vulnerabilidades  
críticas correspondem  
a desatualização

Fonte: Relatório de ameaças 2016 IBLISS Digital Security

# Tecnologia

## ❖ Principais fatores:

- ❑ **Sistemas desatualizados;**
- ❑ **Servidores e serviços com falhas de configuração;**
- ❑ **Serviços expostos indevidamente;**
- ❑ **Falta ou falhas de monitoramento.**

# Tecnologia

## ❖ Serviços expostos

### SMB

returned 798,426 results on 14-10-2017

#### Top Countries

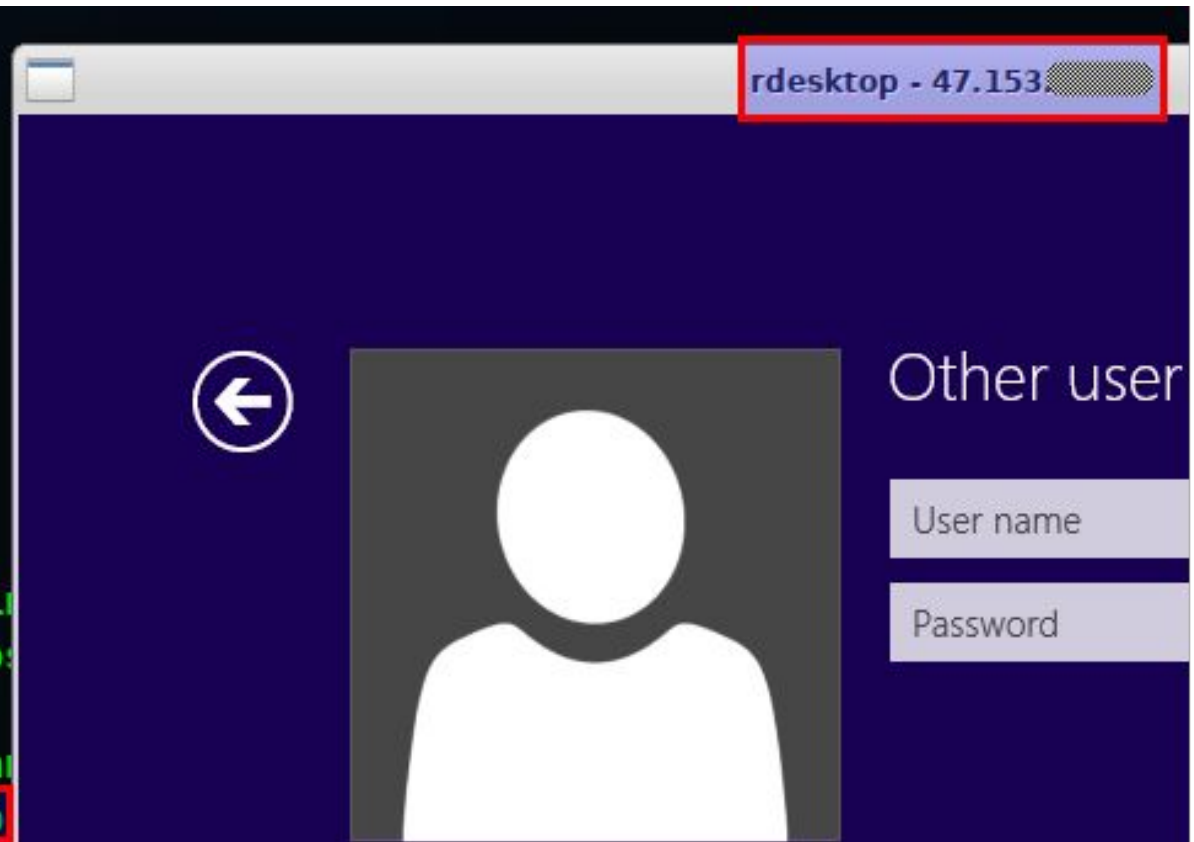
1. United Arab Emirates	471,084
2. Brazil	52,465
3. United States	35,698
4. Argentina	29,828
5. Italy	24,475
6. Russian Federation	19,472
7. Philippines	16,342
8. Germany	12,113
9. Guam	9,773
10. Israel	8,706



# Tecnologia

## ❖ Serviços expostos

```
Nmap scan report for 103.███  
Host is up (0.38s latency).  
  
PORT      STATE SERVICE      VERSION  
3389/tcp  open  ms-wbt-server?  
  
Nmap scan report for 47.153.███  
Host is up (0.31s latency).  
  
PORT      STATE SERVICE      VERSION  
3389/tcp  open  ms-wbt-server Microsoft Termi  
Service Info: OS: Windows; CPE: cpe:/o:micro  
  
Service detection performed. Please report at  
Nmap done: 10000 IP addresses (1286 hosts up
```



Fonte: Arquivo pessoal

# Demo



# Pessoas



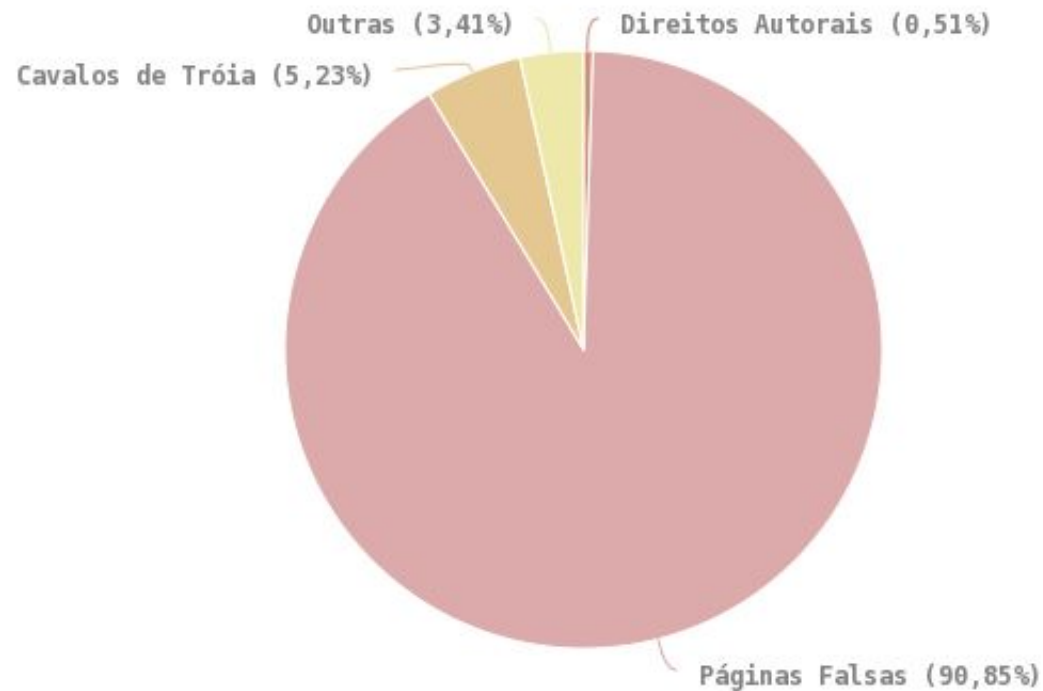
**Muitos incidentes ocorrem devido a falta de ações de conscientização focadas no uso adequado da tecnologia.**

# Pessoas

## ❖ Páginas falsas

### Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016

#### Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2016 Tentativas de fraudes



© CERT.br - by: Michalek

Fonte: <https://www.cert.br/stats/incidentes/2016-jan-dec/fraude.html>

## ❖ Combinando spear phishing e ransomware

### PHISH SCALES: MALICIOUS ACTOR COMBINES PERSONALIZED EMAIL, VARIETY OF MALWARE TO TARGET EXECs

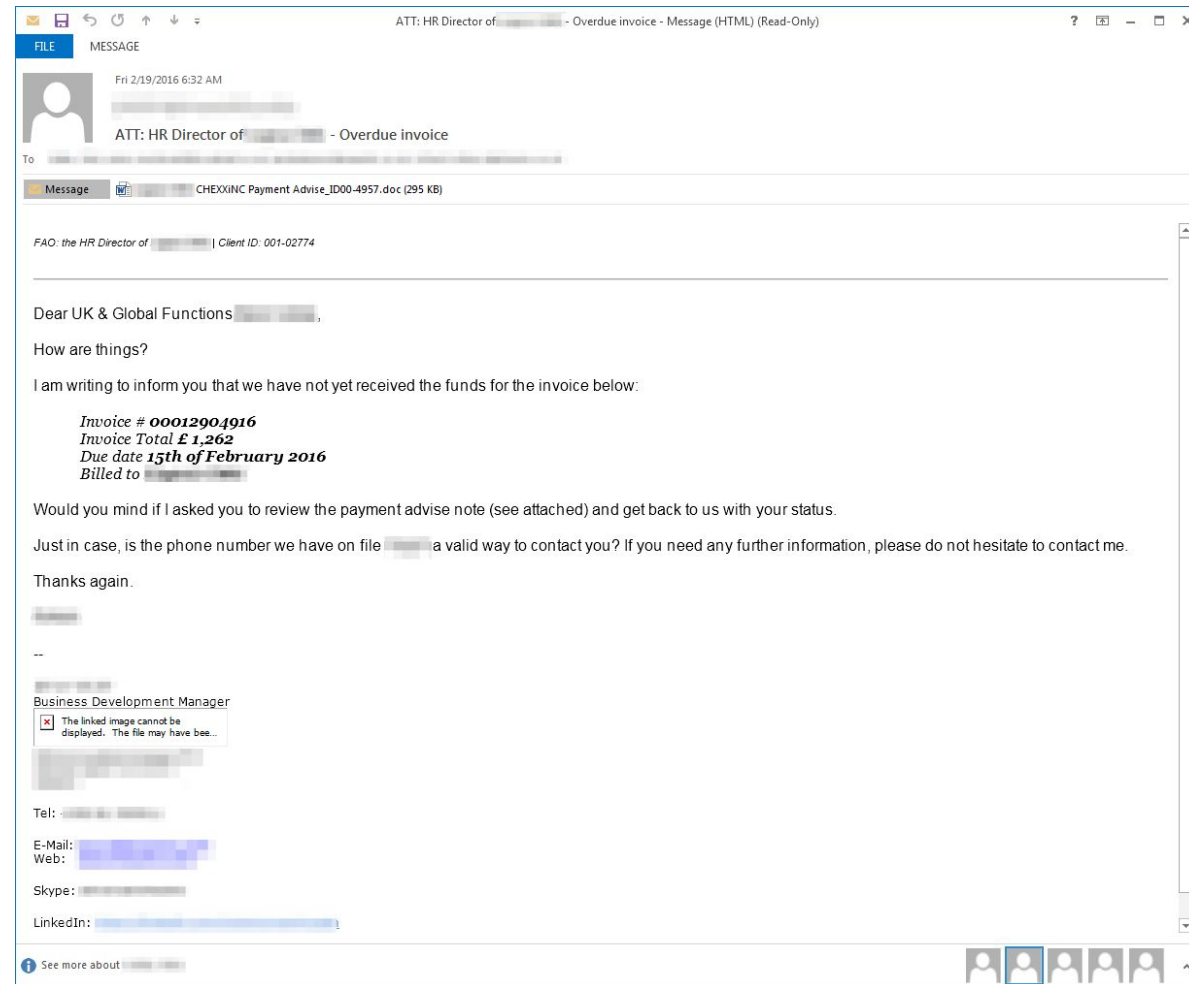
APRIL 05, 2016 Matthew Mesa



The rule of thumb for phishing emails is that the more personalized they are, the more effective they will be. Personalization, though, is expensive, both in terms of the necessary research and preparation of highly targeted malicious emails. The tradeoff between efficacy and cost has always been a constraint on attackers. Unfortunately, Proofpoint has recently observed one actor who appears to have found a way to scale spear phishing. **One recent study** puts the average cost of a successful spear phishing campaign at \$1.6 million per incident - if **spear phishing** becomes the norm instead of the outlier, the math becomes fairly intimidating for targeted organizations.

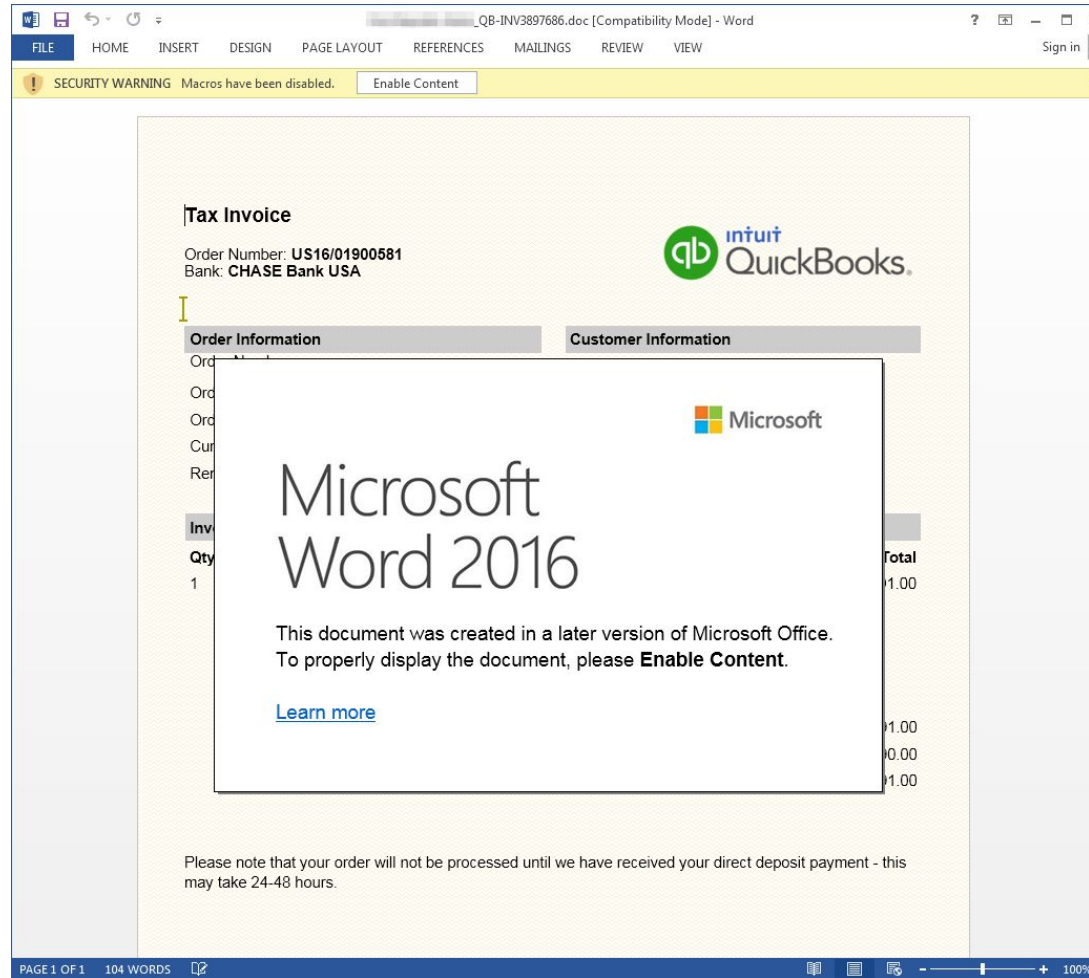


## ❖ Combinando spear phishing e ransomware



Fonte: <https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs/>

## ❖ Combinando spear phishing e ransomware





# Demo



# Mitigando



# Mitigando

- ❖ Adoção de boas práticas de segurança na infraestrutura;
- ❖ Backup de dados;
- ❖ Atualização contínua;
- ❖ Monitoramento;
- ❖ Conscientização.

# Perguntas?



# Obrigado

# iBLISS

