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.**

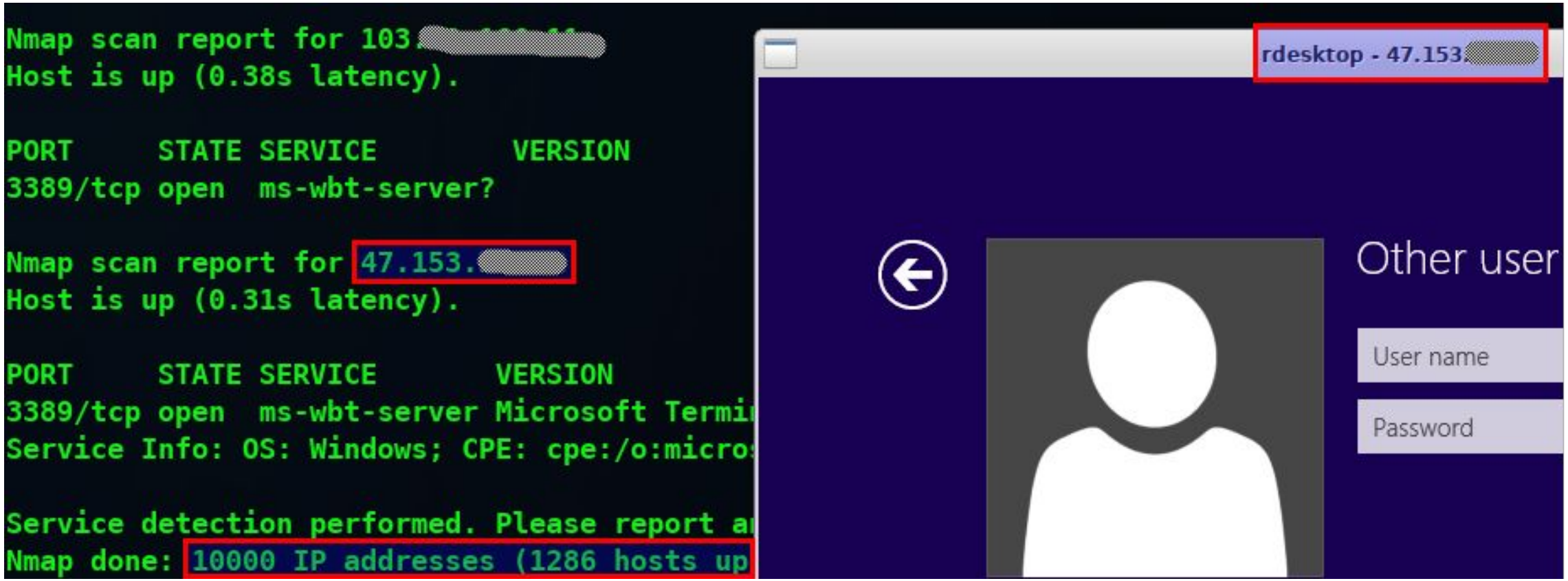
Tecnologia

- **Serviços expostos**

Fonte: Shodan - https://www.shodan.io/report/jlZ35E7s

Tecnologia

- **Serviços expostos**



Fonte: Arquivo pessoal

Demo

Pessoas

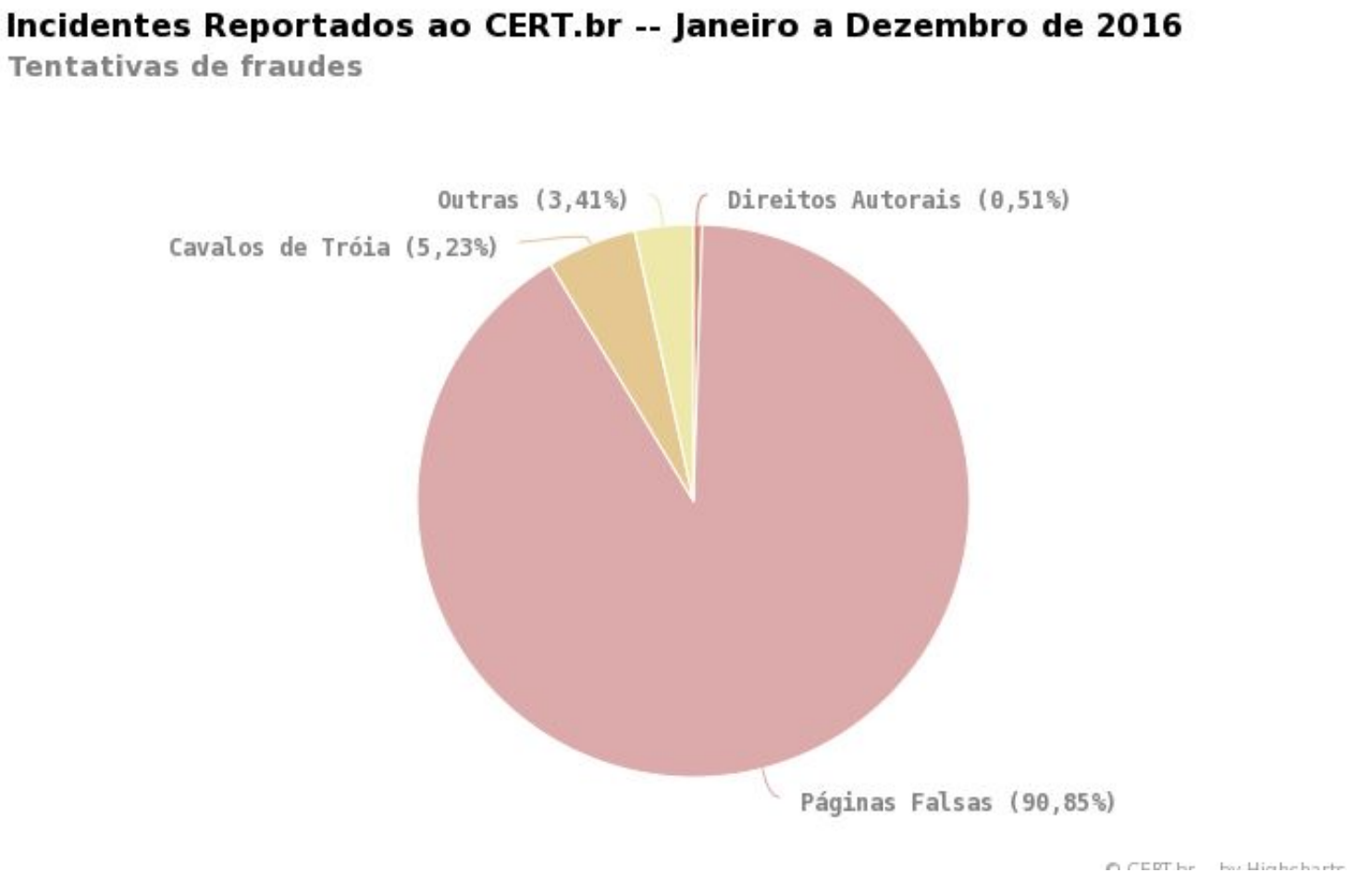
Pessoas

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



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

Pessoas

- **Combinando spear phishing e ransomware**

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

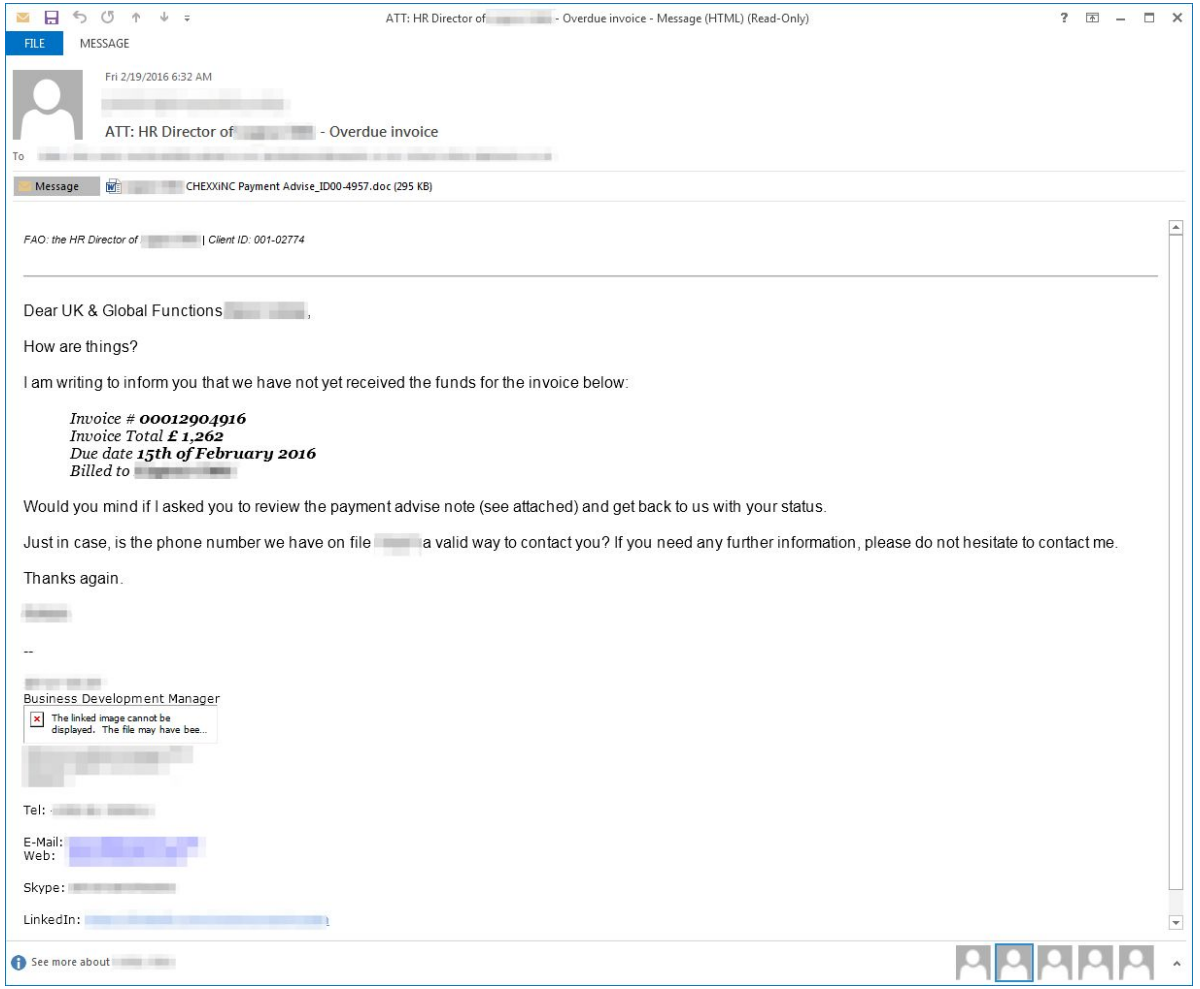
APRIL 05, 2016 Matthew Mesa

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.

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

Pessoas

- **Combinando spear phishing e ransomware**

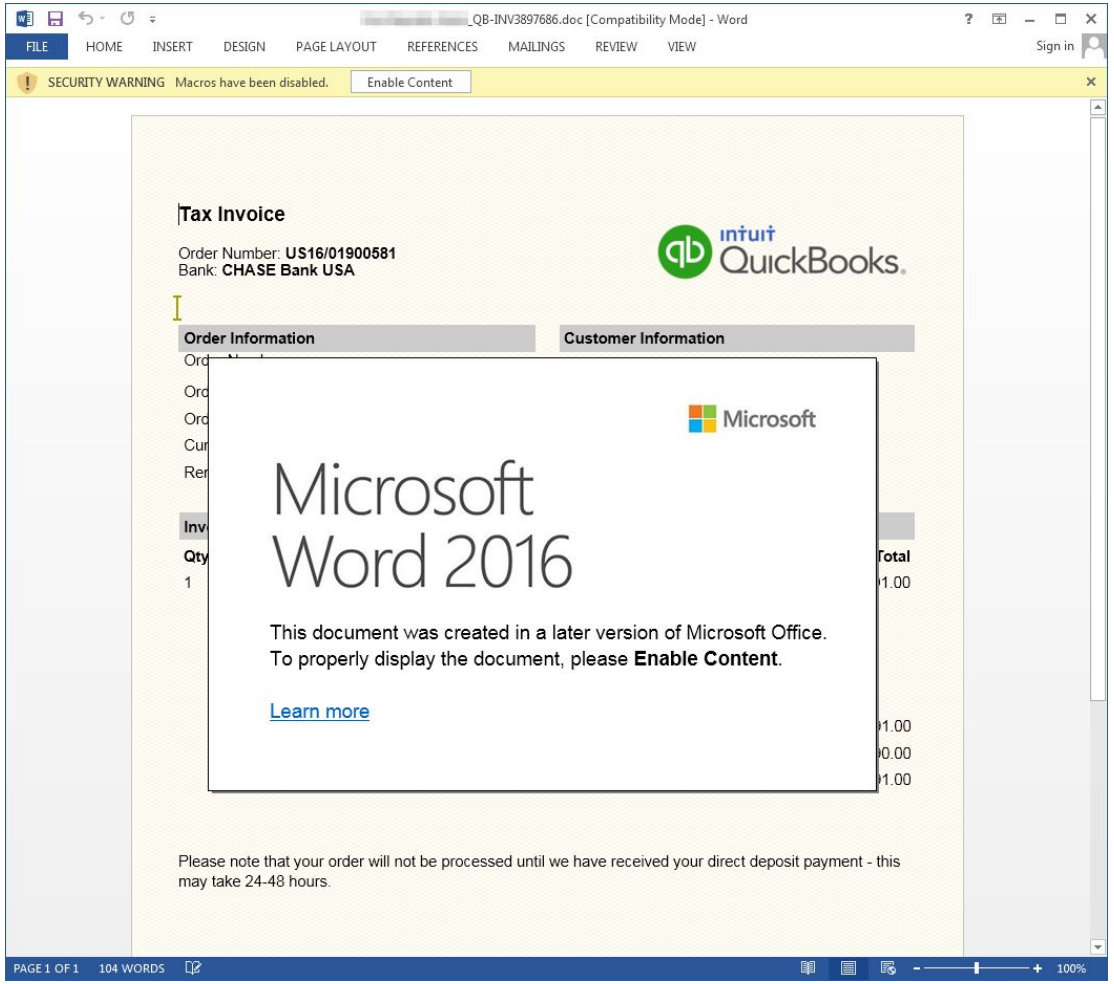


Fonte: https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs/

iBLISS

Pessoas

- **Combinando spear phishing e ransomware**



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

Demo

Mitigando

Mitigando

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

Perguntas?

Obrigado

iBLISS