Hewlett Packard
Enterprise

CyberSecurity

Paulo Veloso
Regional Director, Latam
HPE Security

7 de junho de 2016

O que é CyberSecurity?

Hewlett Packard
Enterprise

Segurança Cibernética é o conjunto de **tecnologias, processos, pessoas e práticas** destinado a proteger redes, computadores, programas e dados de ataques, danos ou acessos não autorizados.

A empresa digital precisa de um novo estilo de proteção

Hewlett Packard Enterprise

Quem são os adversários?

Hewlett Packard
Enterprise

Criminosos digitais

Motivação: Lucro

Alvos: Propriedade intelectual, dados pessoais, credenciais de acesso e dados de cartões de crédito e débito

Nível de Sofisticação: Variado

Defesas: Criptografia

Pode incluir desenvolvedores, especialistas em segurança de alto nível, black hats contratados sob demanda e crime organizado.

Adversários motivados pelo ego

Motivação: Fama ou reconhecimento

Alvos: Alteração de websites e vazamento de dados corporativos

Nível de Sofisticação: Médio, normalmente têm conhecimento interno sobre seus alvos

Defesas: Monitoramento de usuários com acessos privilegiados e/ou de alto risco

Sentem satisfação quando suas ações são divulgadas enquanto suas identidades permanecem desconhecidas.

Hacktivismo

Motivação: Ideologia, justiça social, tendências religiosas ou políticas

Alvos: Grandes empresas, mídia e governos

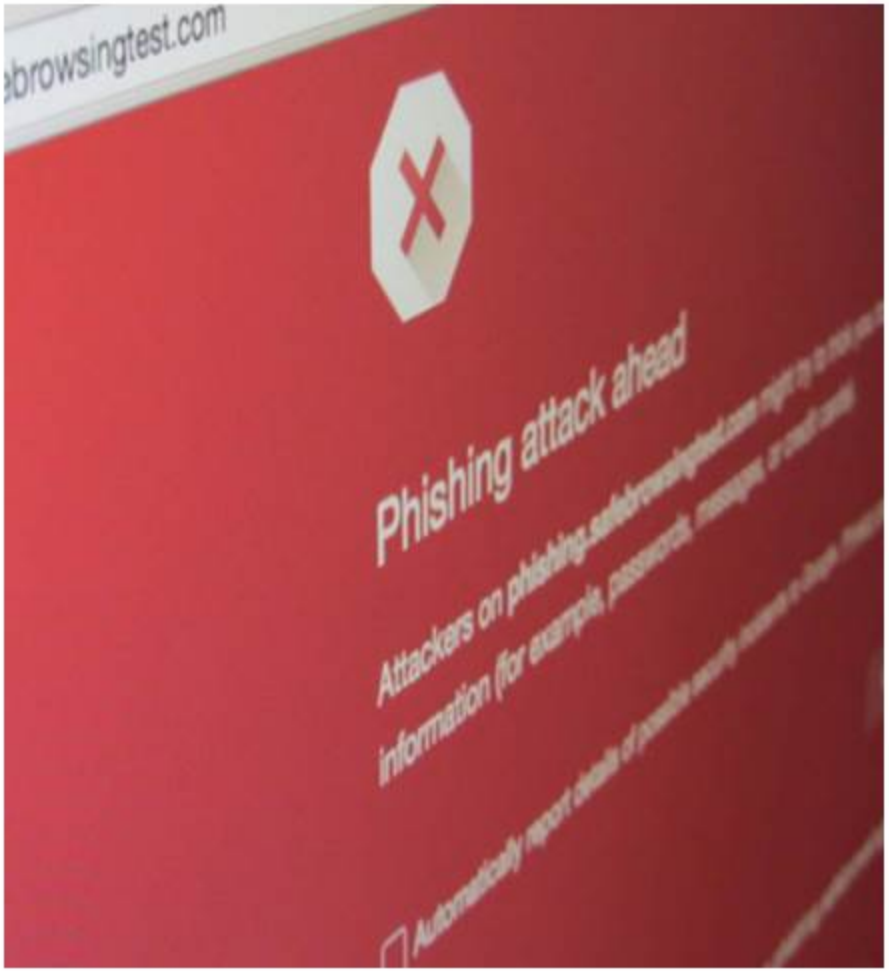
Nível de Sofisticação: Baixo, normalmente composto por script kiddies em sua maioria

Defesas: Firewall e IPS

Facilmente influenciáveis e em busca de uma sensação de pertencimento a um determinado grupo.

Hewlett Packard
Enterprise

Hackers profissionais / hobby



Motivação: Gosto por hacking, bug bounties, apresentações em conferências de segurança

Alvos: Responsible Disclosure de qualquer vulnerabilidade

Nível de Sofisticação: Desde iniciantes até profissionais renomados

Defesas: White Listing

Muitos têm empregos fixos e praticam hacking como hobby.

O modelo de negócios deles, parece muito com o nosso.

Hewlett Packard
Enterprise

O modelo de negócios deles, parece muito com o nosso.

Recursos Humanos
- Verificação de antecedentes
- Recrutamento e seleção

Desenvolvimento
- Spiders
- Black hats for hire

Finanças
- Lavagem de dinheiro
- Garantias de pagamentos

Vendas e marketing
- Promoção de vendas
- Marketing de produtos
- Anúncios

Legal
- Direito internacional
- Análise de contratos

Operações
- Gestores de processos
- Gerentes de projetos
- Mulas
- Suporte ao cliente

Hewlett Packard Enterprise

Dividido em verticais

Crime organizado

Furto de IP

Guerra digital

Fraude em meios de pagamento

Fraude em cartões

Fraude em anúncios

Furto de identidade

Colheita de credenciais

Fraude em registros médicos

Bug bounty

Hacktivismo

Fraude bancária

Extorsão

Hewlett Packard Enterprise

Alguns casos mais recentes...

Hewlett Packard
Enterprise

O resultado é um aumento no número de casos e no tamanho dos prejuízos com ataques digitais.

Heartland Payment Systems

- 130 milhões de cartões de crédito e debito
- U$ 140 milhões em multas

Sony

- 102 milhões de contas da PlayStation Network
- U$ 171 milhões em prejuízos estimados

Target

- 110 milhões de dados pessoais de clientes, incluindo cartões de crédito e débito
- 46% de queda no lucro comparado com o ano anterior

Neiman Marcus

- 350 milhões de cartões de crédito e debito
- Modificação potencial da cláusula "Clapper" da Suprema Corte dos EUA

Anthem

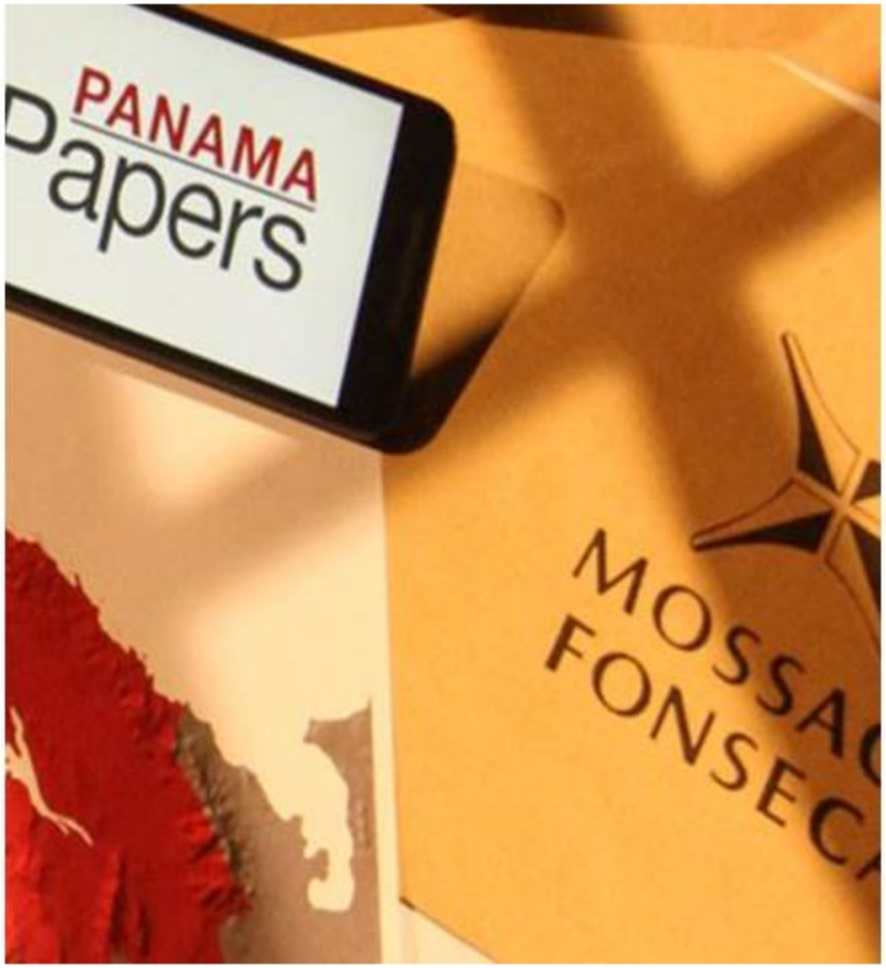
- 80 milhões de dados médicos pessoais

898.587.384 registros comprometidos

4.834 ataques bem-sucedidos em 2015

Hewlett Packard Enterprise

Panama Papers



Panama Papers

- Ataque fora do eixo financeiro
- Vulnerabilidade explorada há vários anos
- Todos os e-mails e documentos foram expostos
- Queda de um primeiro-ministro
- Vários empresários e políticos investigados

Hewlett Packard
Enterprise

SWIFT

Rede Swift

- Começou por um ataque isolado via Banco de Bangladesh que desviou US$ 81M
- Após investigações, viu-se uma vulnerabilidade em toda a rede de comunicação, permitindo aos atacantes cometerem fraudes internacionais sem deixar rastros, via PCs comuns
- Roubo de credenciais para uso em envio e recepção de mensagens dentro da rede com escalação de privilégios

Banco el Austro- Equador

Banco Equador

- Início de exploração de uma falha na Swift
- 12 milhões em prejuízo
- Aconteceu em 2015, e a Swift só ficou sabendo em março de 2016

Saque ATM - Japão

Saque ATM - Japão

- Roubo de dados de banco na África do Sul
- Emissão de 1.600 cartões fraudados
- Saques sincronizados no Japão usando cartões fraudados
- 14 mil transações realizadas em menos de um dia

Hewlett Packard Enterprise

Como você alcança seus objetivos?

~~Aumenta os lucros~~
- **Reduza os lucros deles**
- Criptografia aplicada
- Dados falsos como honey pot

~~Reduz os riscos~~
- **Aumente os riscos para eles**
- Regulamentação / enforcement
- Monitoramento sofisticado

~~Incrementa o pipeline~~ de vendas
- **Reduza a quantidade de alvos**
- Fortalecimento de aplicações
- Higiene nas questões básicas de segurança

~~Reduz o tempo de~~ entrega
- **Aumente o tempo de entrega para eles**
- Identificação de DNS malware
- Uso de sistemas de pagamento com maior controle

~~Aumenta os~~ recursos disponíveis
- **Reduza a quantidade de recursos disponíveis**
- Melhores iniciativas para white hats
- Análise de reputação

~~Reduza o custo de~~ fazer negócios
- **Aumente o custo que eles têm para fazer negócios**
- Todos os pontos anteriores

Hewlett Packard
Enterprise

Obrigado.