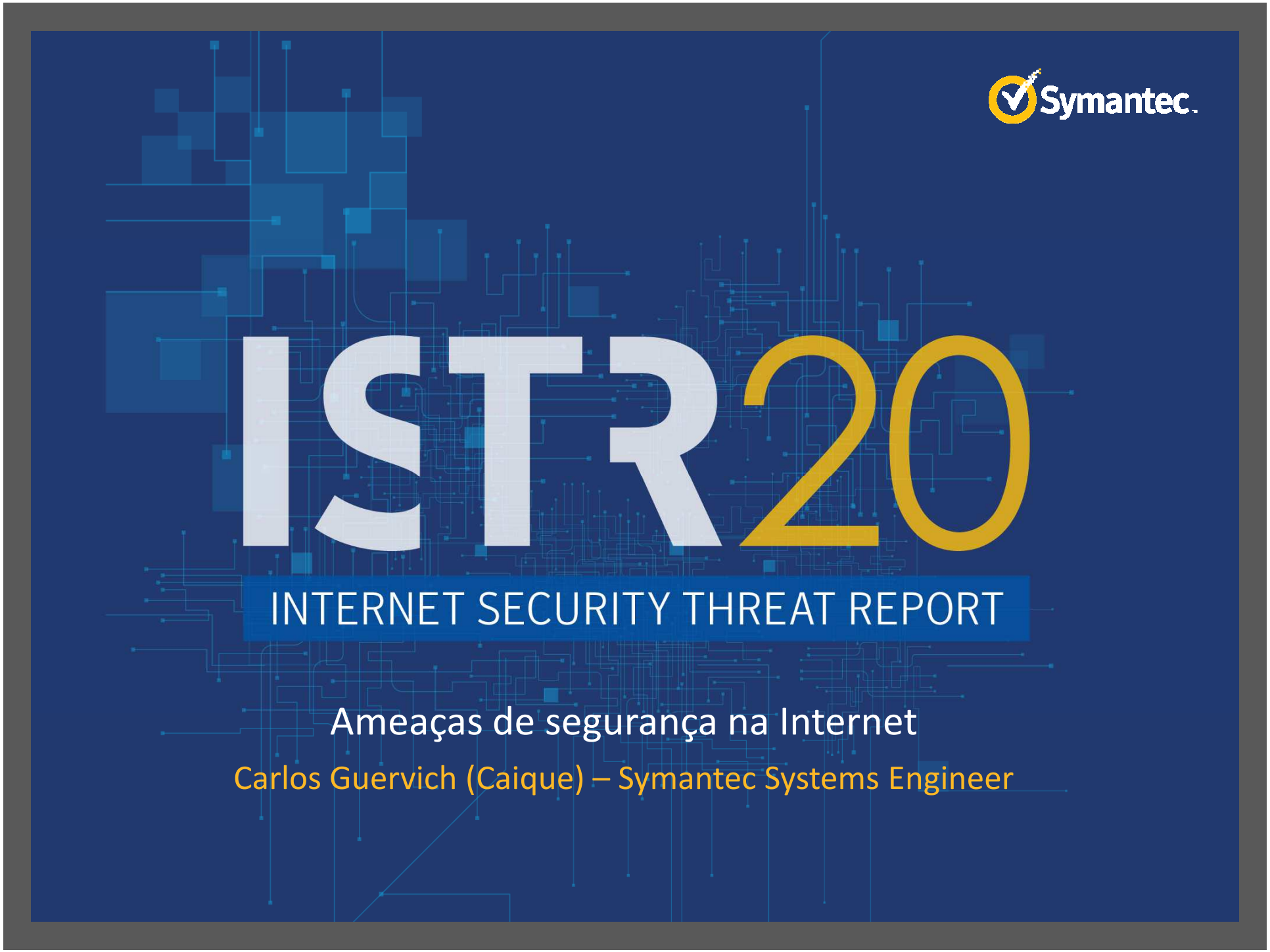

Symantec.
ISTR20
INTERNET SECURITY THREAT REPORT
Ameaças de segurança na Internet
Carlos Guervich (Caique) – Symantec Systems Engineer

Agenda

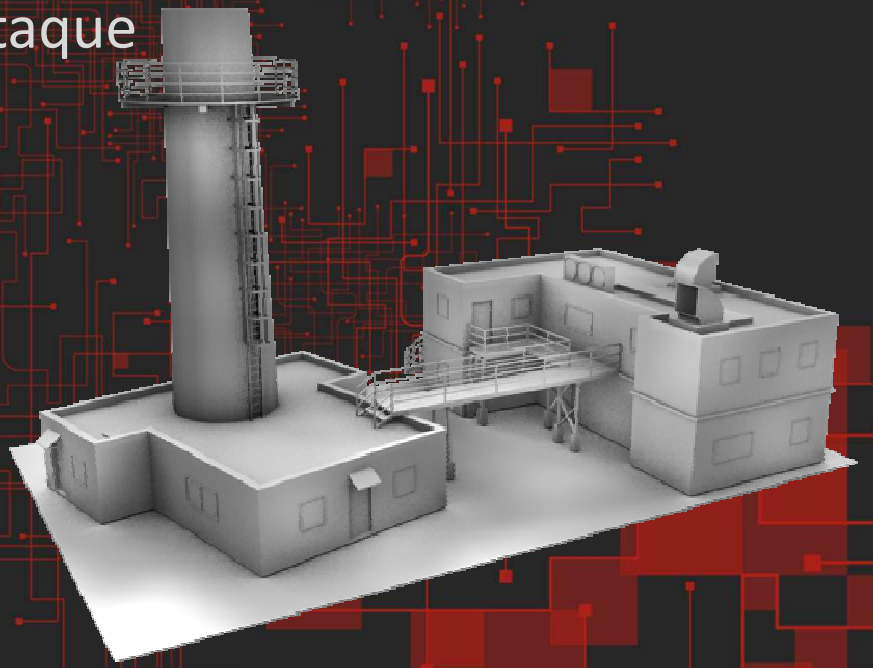
1. Os cyberattackers estão ultrapassando as defesas fazendo com que as empresas necessitem de uma visão atecipada destas ações
2. Os atacantes estão se movendo mais rápido que as defesas
3. Malware utilizados em ataques em massa estão aumentando e se adaptando
4. Extorsão digital em ascensão: 45 vezes mais pessoas tiveram seus dispositivos “reféns” em 2014
5. IoT não é um “problema” novo, mas está em evidência

Symantec.
ISTR20
INTERNET SECURITY THREAT REPORT

Os cyberattackers estão ultrapassando as defesas fazendo com que as empresas necessitem de uma visão atecipada destas ações

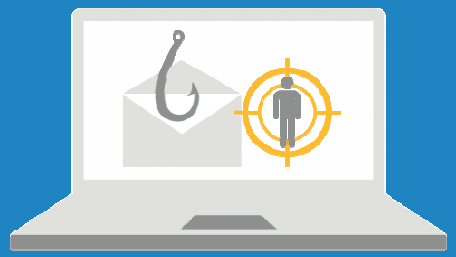
Inimigos atuais: Dragonfly (Exemplo)

- Em 2014, A Symantec identificou o grupo Dragonfly, que tinha como alvo empresas do setor público da Europa e U.S.
- Utilizam diversos métodos de ataque



Métodos de ataque

Spear Phishing

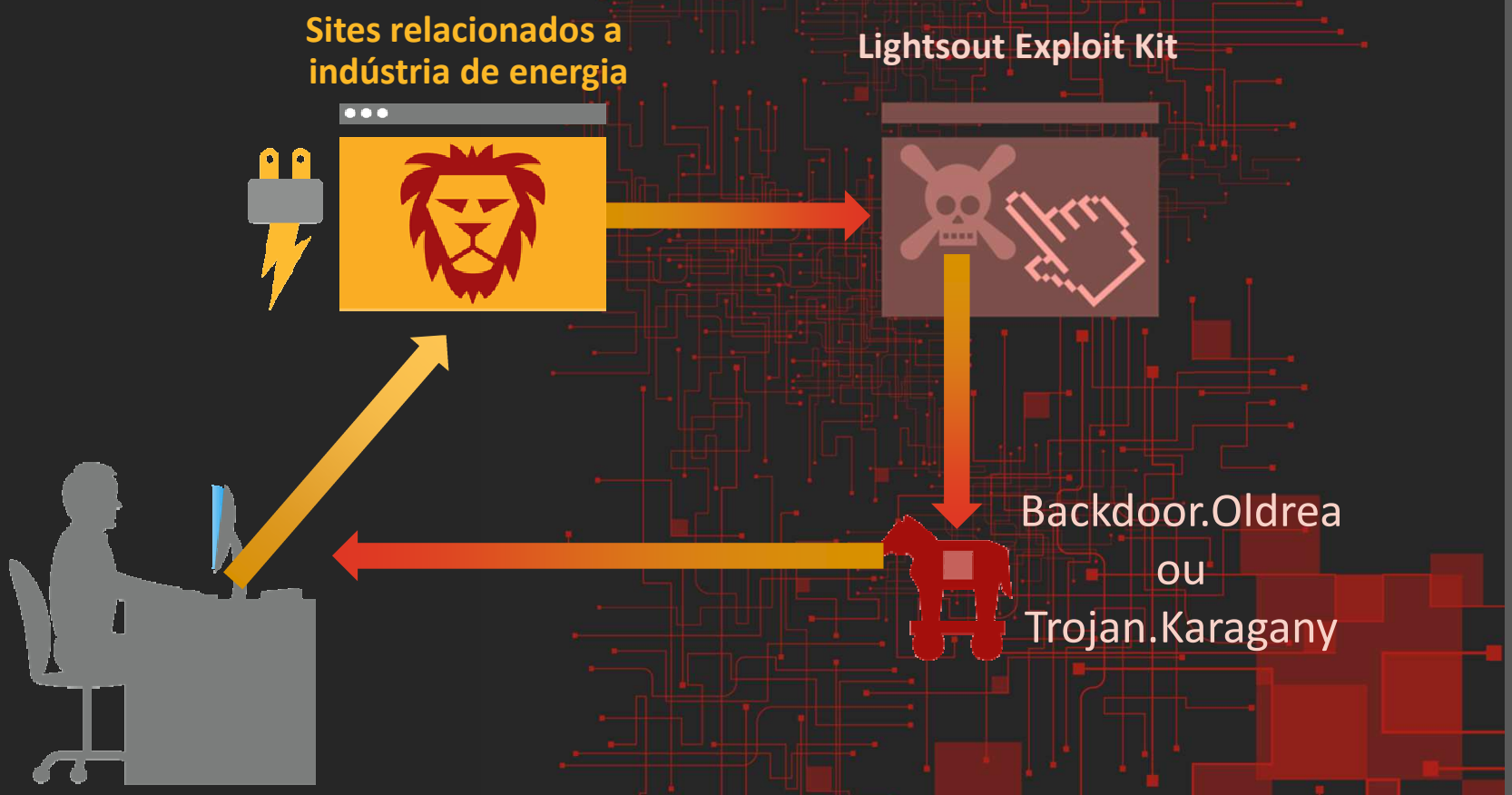


Envio de um email direcionado

Watering Hole Attack

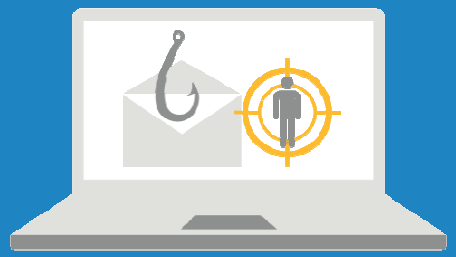
Infecção de site legítimo

Como funciona: Watering Hole Attack



Métodos de ataque

Spear Phishing

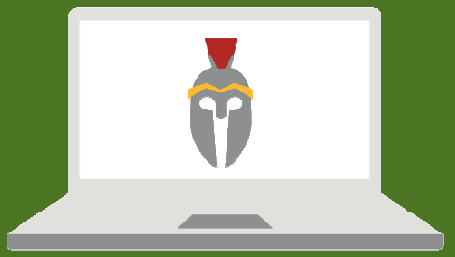


Envio de um email direcionado

Watering Hole Attack

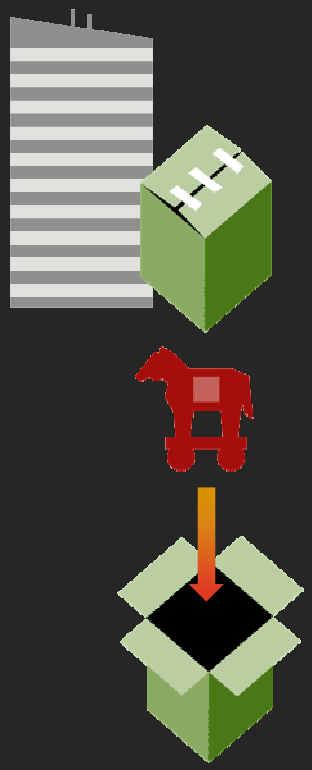
Infecção de site legítimo

Trojanized Update

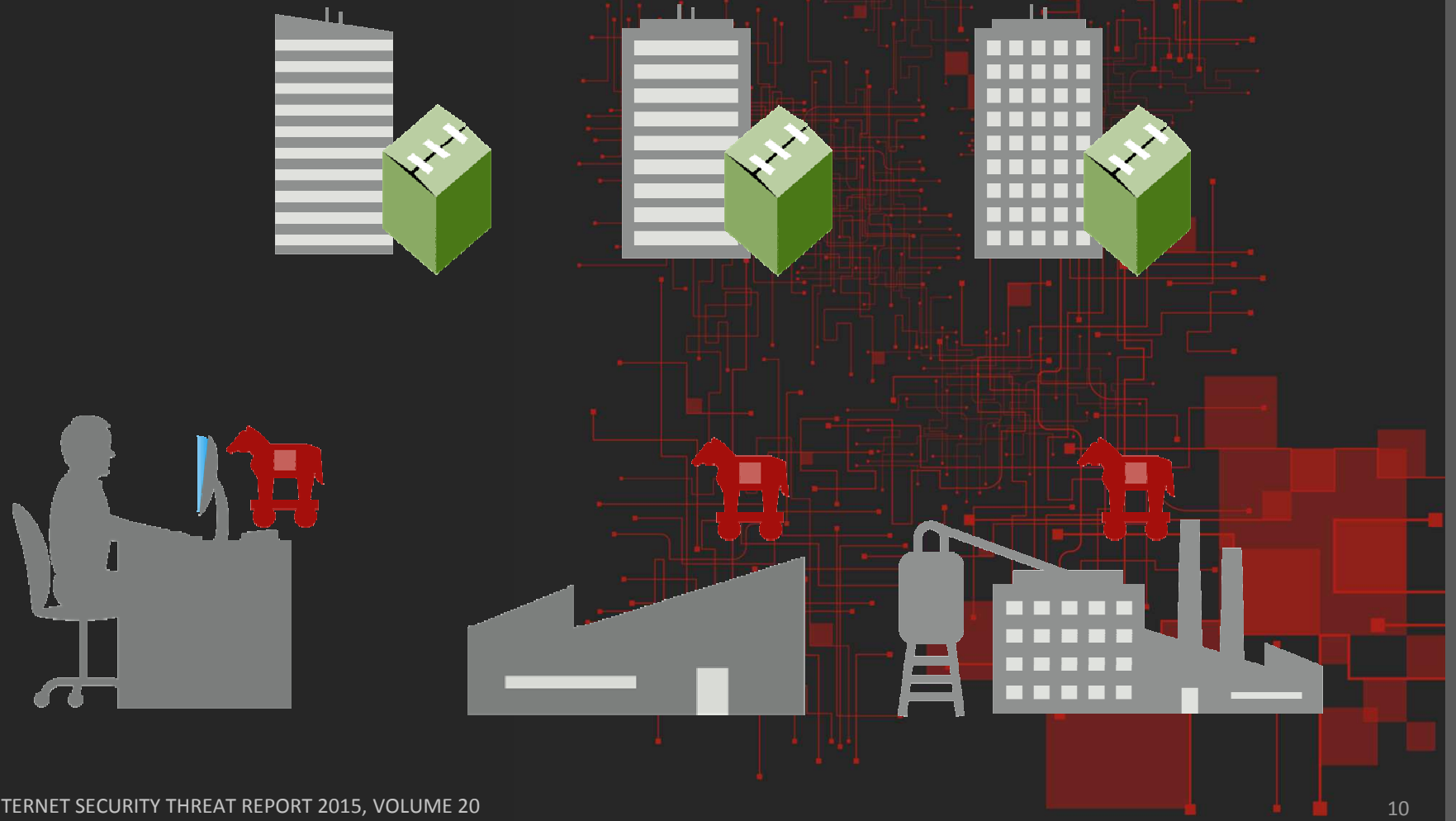


Infecção de softwares de atualização

Como funciona: Trojanized Update

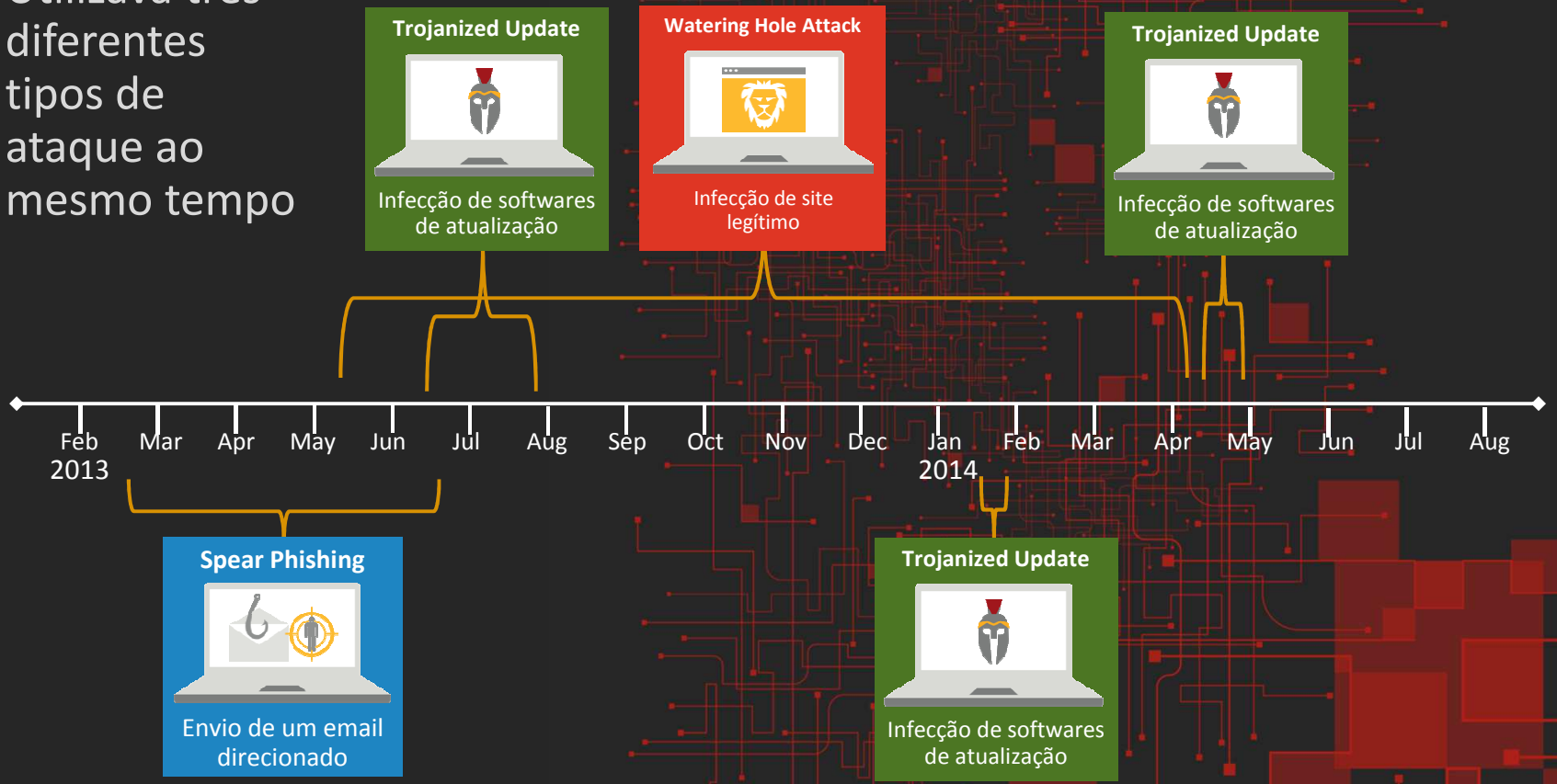


Como funciona: Trojanized Update

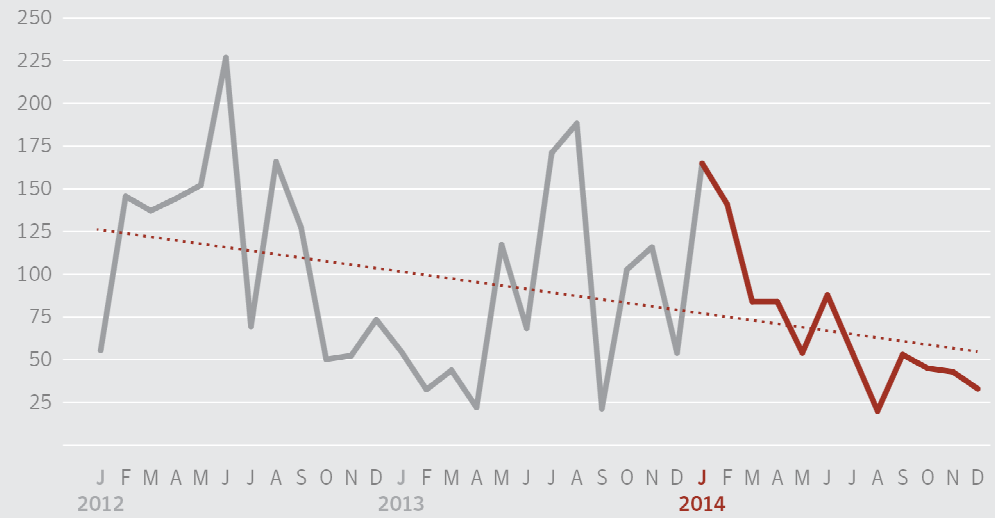


Capacidade avançada dos atacantes

- Utilizava três diferentes tipos de ataque ao mesmo tempo



Número médio de ataques Spear Phishing por dia



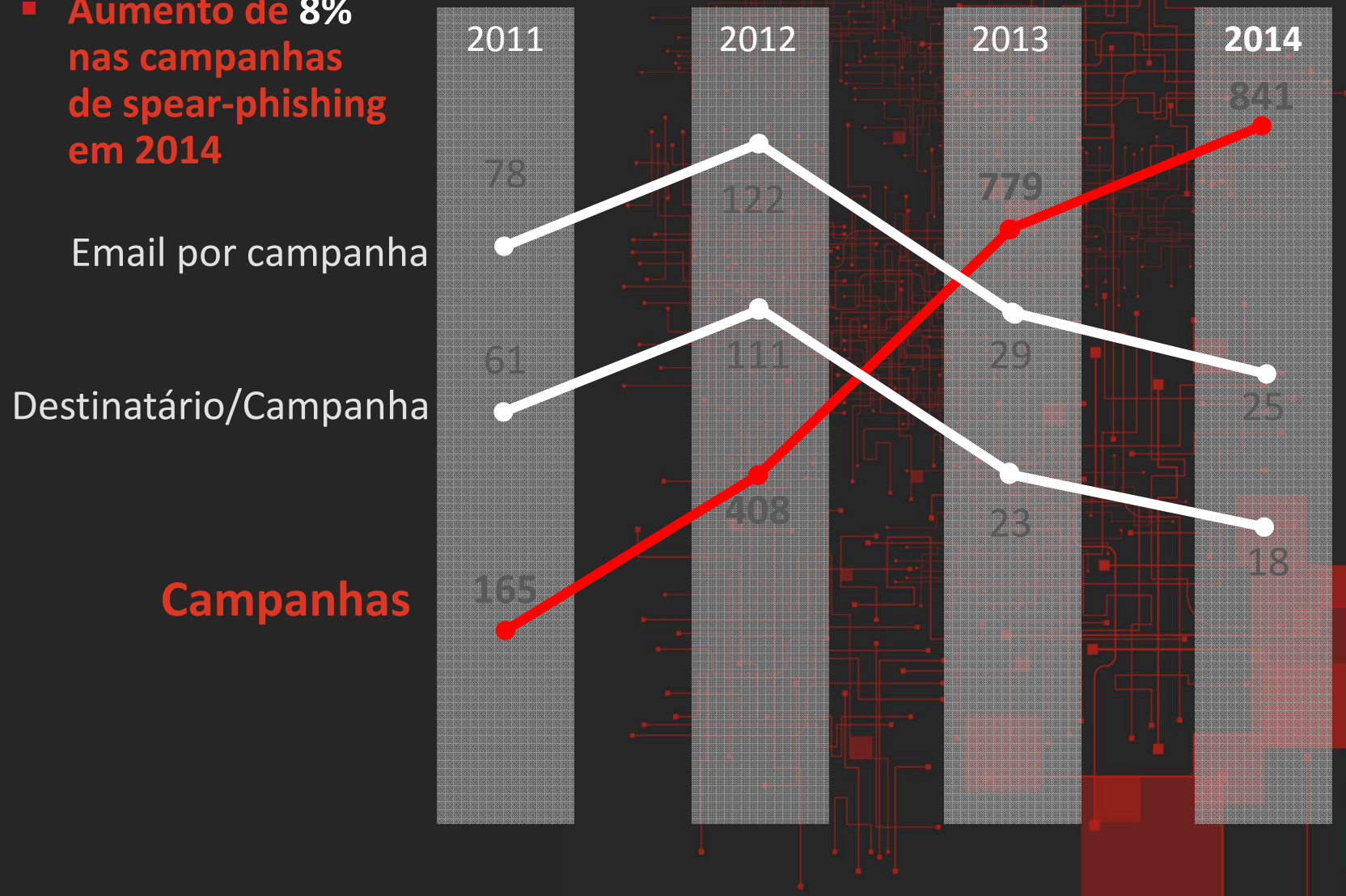
Average Number of Spear-Phishing Attacks per Day, 2012–2014

Source: Symantec

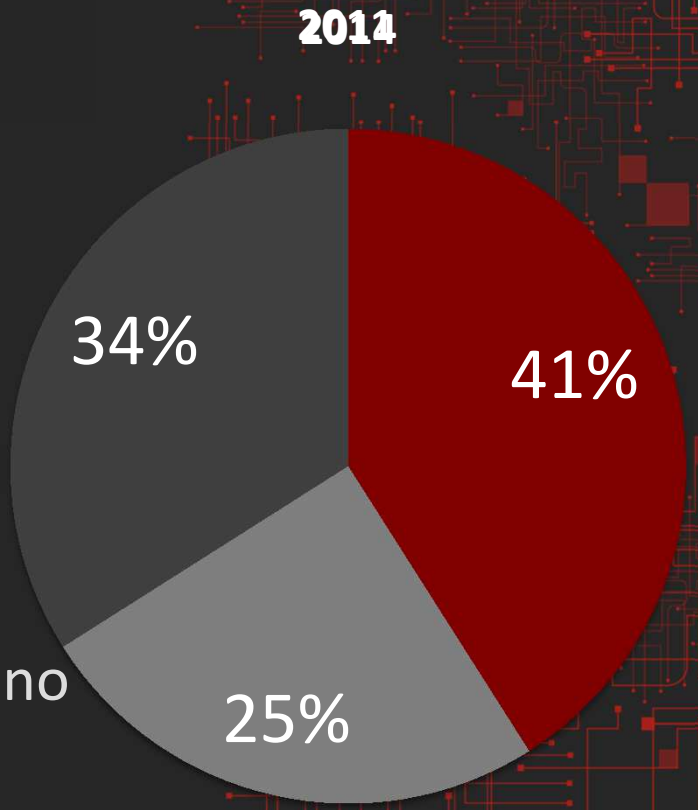
- Tendência de queda no volume de spear-phishing não significa que as campanhas diminuíram

Campanhas de ataque direcionado

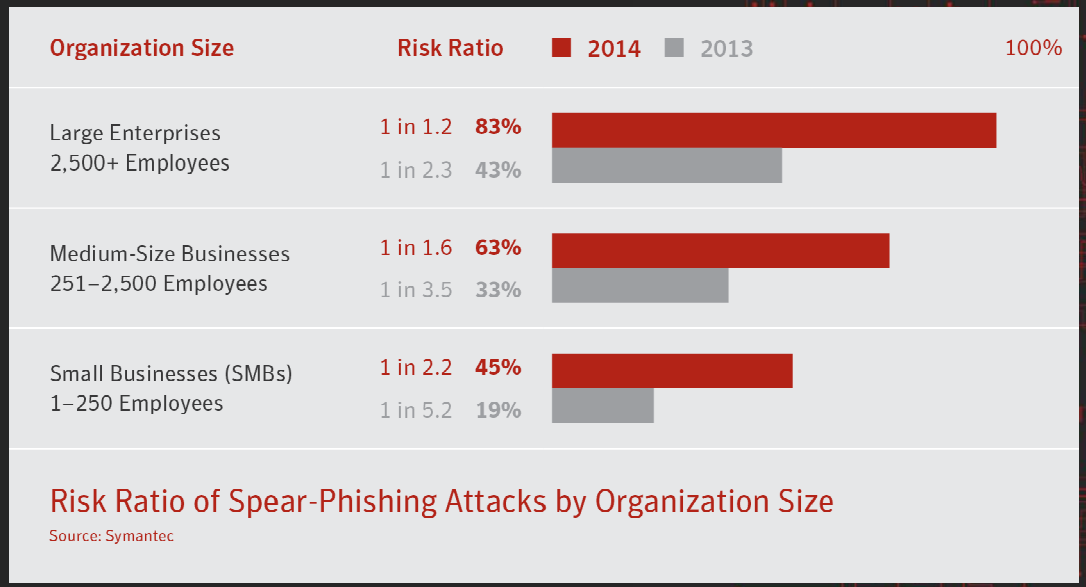
- **Aumento de 8% nas campanhas de spear-phishing em 2014**



Distribuição de ataques de Spear-Phishing



Taxa de risco de ataques de Spear-Phishing



Risk Ratio of Spear-Phishing Attacks by Organization Size

Source: Symantec

40% aumento

30% aumento

26% aumento

- **5** de **6** Empresas de grande porte são alvo (**83%**)

Análise de emails de Spear-Phishing usados em ataques direcionados

Rank	Attachment Type	2014 Overall Percentage	Attachment Type	2013 Overall Percentage
1	.doc	38.7%	.exe	31.3%
2	.exe	22.6%	.scr	18.4%
3	.scr	9.2%	.doc	7.9%
4	.au3	8.2%	.pdf	5.3%
5	.jpg	4.6%	.class	4.7%
6	.class	3.4%	.jpg	3.8%
7	.pdf	3.1%	.dmp	2.7%
8	.bin	1.9%	.dll	1.8%
9	.txt	1.4%	.au3	1.7%
10	.dmp	1.0%	.xls	1.2%

Analysis of Spear-Phishing Emails Used in Targeted Attacks, 2013–2014

Source: Symantec

- 40+% dos e-mails direcionados incluiu um anexo executável malicioso
- 40% dos e-mails direcionados possui um documento word malicioso

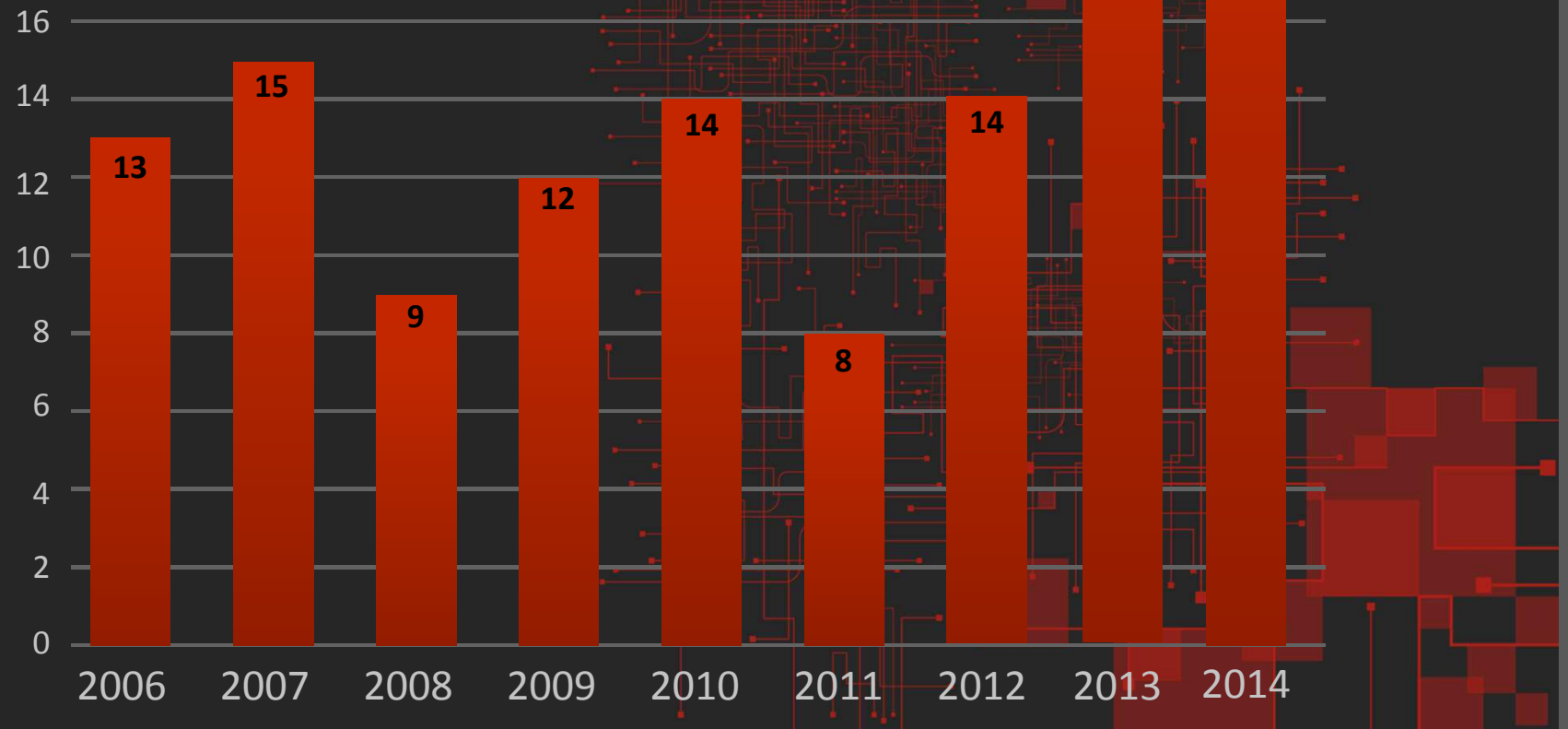
38.7% .doc

22.6% .exe

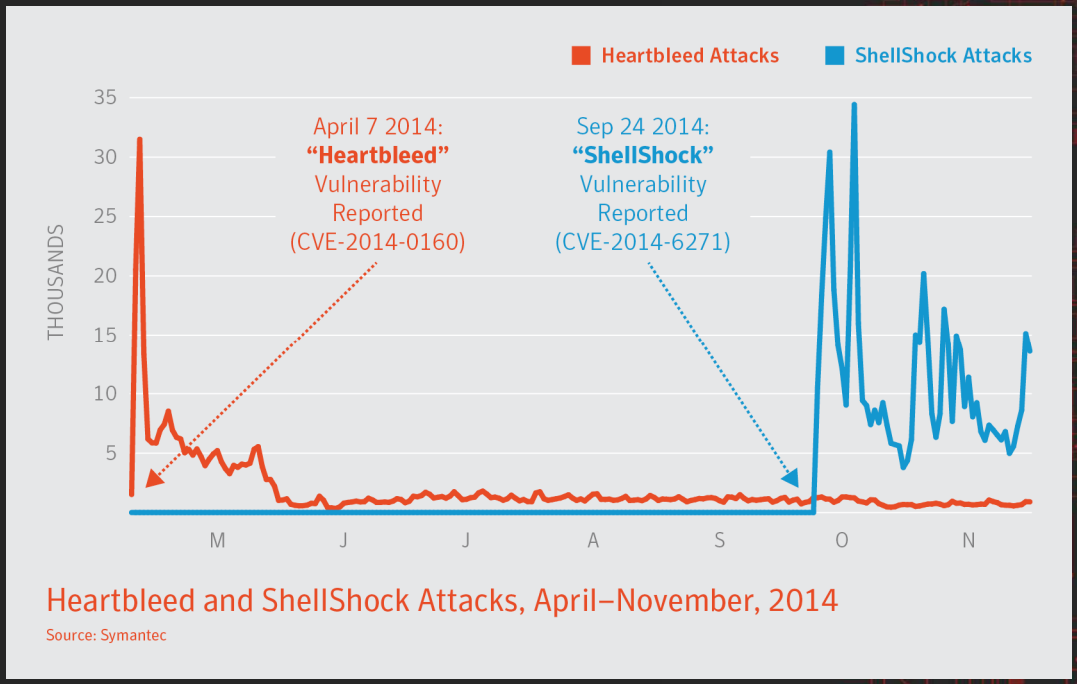
Os atacantes estão se movendo mais rápido que as defesas

Vulnerabilidades Zero-Day

- Vulnerabilidades Zero-day em alta
- O valor das explorações zero-day estão levando ao novo nível de descobertas



Ataques Heartbleed e Shellshock



Heartbleed and ShellShock Attacks, April–November, 2014

Source: Symantec

- Vulnerabilidade Heartbleed explorada em menos de **4** horas após se tornar pública

- Ataques direcionados utilizam os "zero days" antes de serem descobertos
- Outros aproveitam uma vez que se tornam públicos

Websites legítimos com vulnerabilidades

76%

-1%

2014

77%

+25% pts

2013

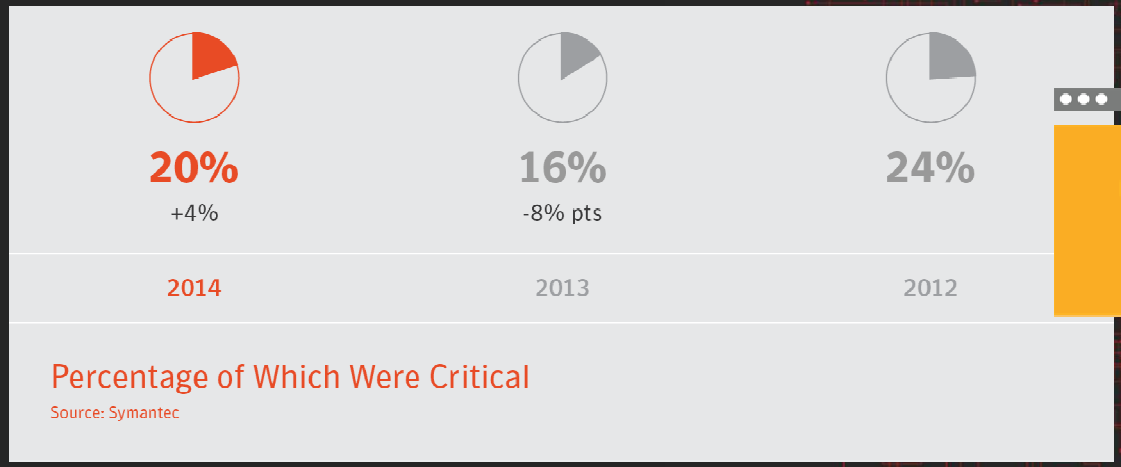
55%

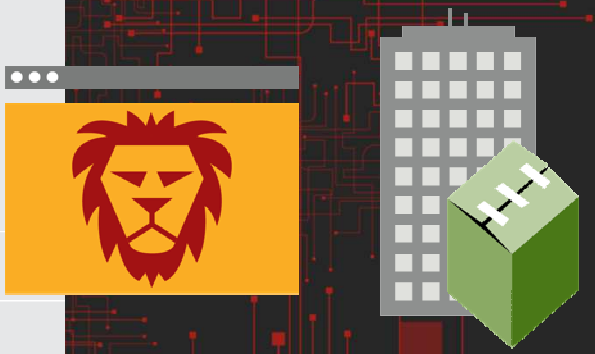
2012

Scanned Websites with Vulnerabilities

Websites legítimos com vulnerabilidades

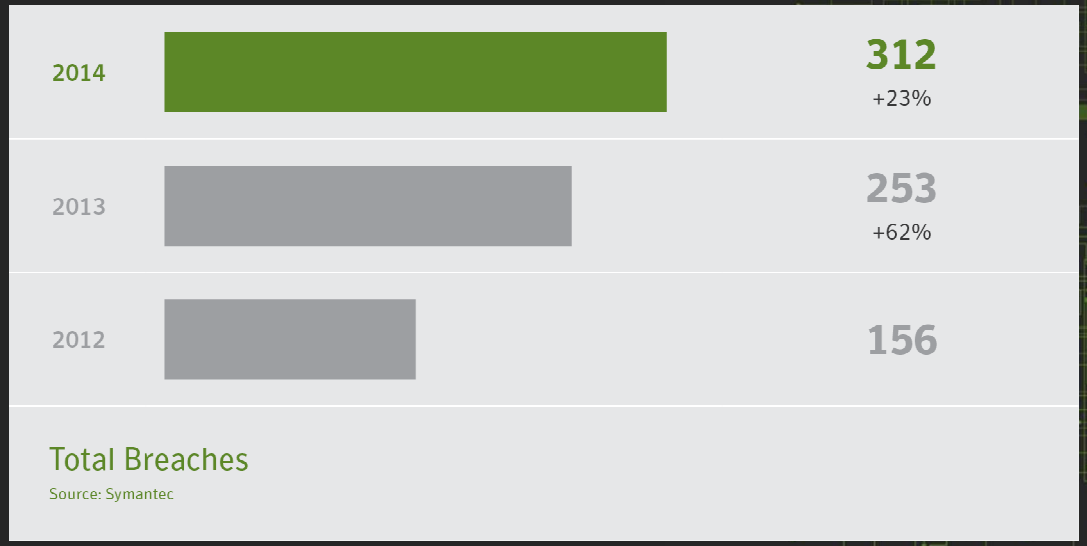
Porcentagem de vulnerabilidades críticas





- A falta de segurança em websites legítimos tornou mais fácil para os atacantes redirecionarem os usuários e hospedarem malwares
- Eles também dão aos atacantes uma “entrada” fácil na empresa
- Essas vulnerabilidades podem permitir que invasores infectem seus clientes ou realize um ataque a sua estrutura.

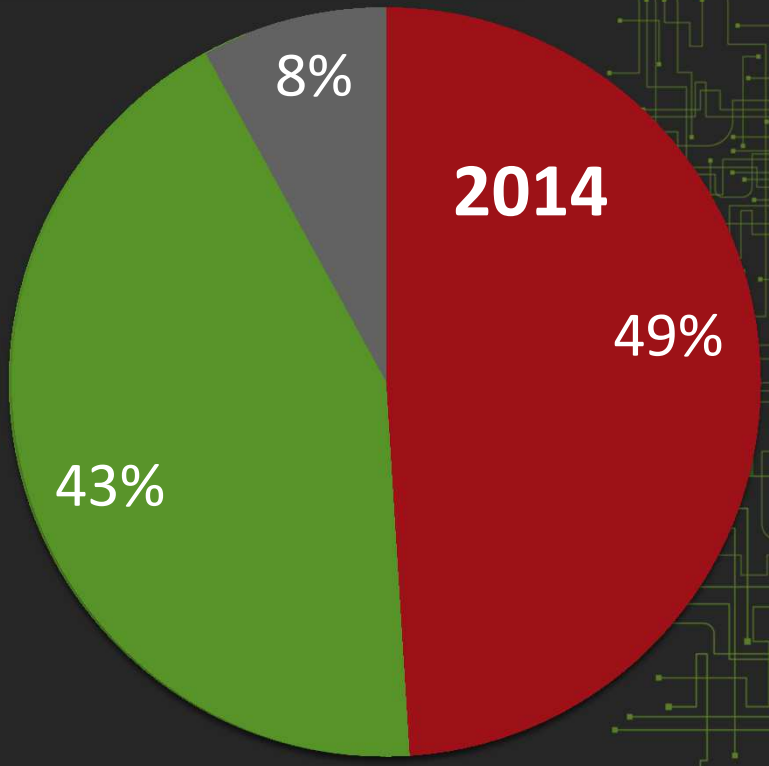
Total de violações



- **23%** aumento em 2014

- **"mega violções" menor em 2014** 4 incidentes envolvendo mais de 10 milhões de identidades expostas (comparada com 8 em 2013)
- **1 em 5** companhias violadas não reportaram informações dos dados expostos. (1 em 6 em 2013)

Principais causas das violações de dados



- Ataques
- Acidentamente exposta/ Roubo ou perda dispositivos
- "Ladrão" interno

Top 10 – Setores violados (Identidades expostas)

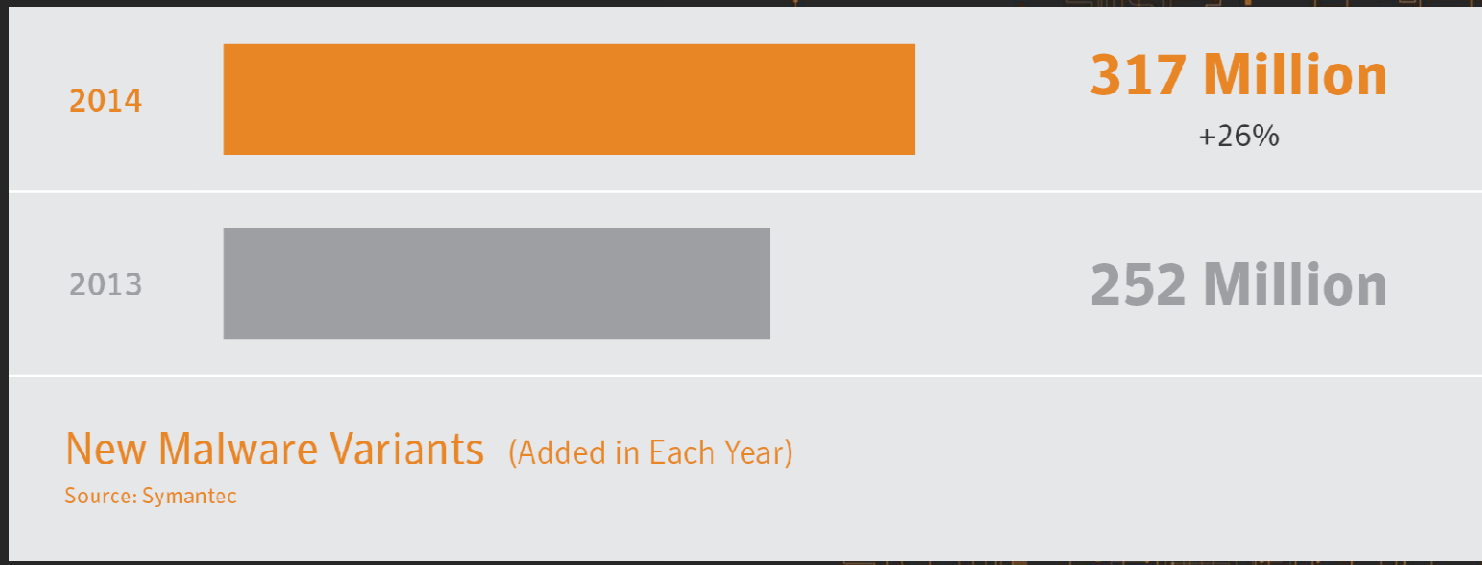
Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed (100%)
1	Retail	205,446,276	59%
2	Financial	79,465,597	23%
3	Computer Software	35,068,405	10%
4	Healthcare	7,230,517	2%
5	Gov. & Public Sector	7,127,263	2%
6	Social Networking	4,600,000	1%
7	Telecom	2,124,021	.6%
8	Hospitality	1,818,600	.5%
9	Education	1,359,190	.4%
10	Arts and Media	1,082,690	.3%

Top 10 Sectors Breached by Number of Identities Exposed

Source: Symantec

Malware utilizados em ataques em massa estão aumentando e se adaptando

Novas variantes de malware



- Quase 1 milhão de novas ameaças criadas **cada** dia em 2014

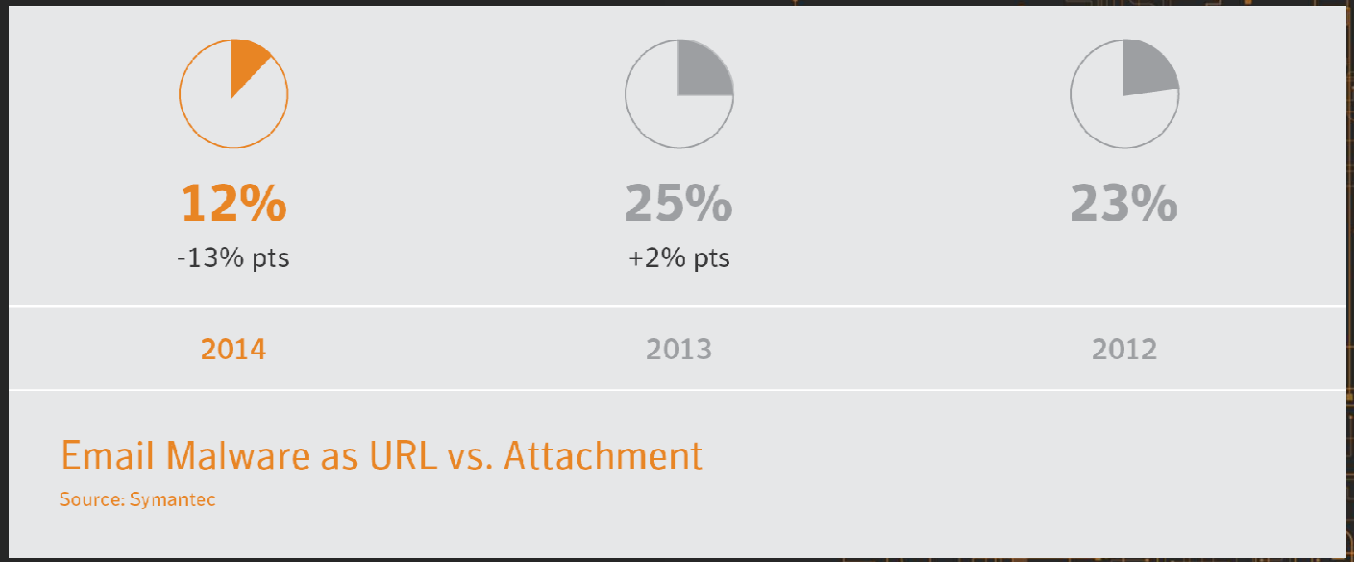
Malware Virtually-Aware

```
If Virtual Machine
Then
        Stop Running
Or
        Send False Data
Or
        Take Evasive Action
        -Delay Execution
        -Wait for User Action
        -Hide
```

```
If VMDK exists
Then
        Mount VM
        Infect
Repeat
```

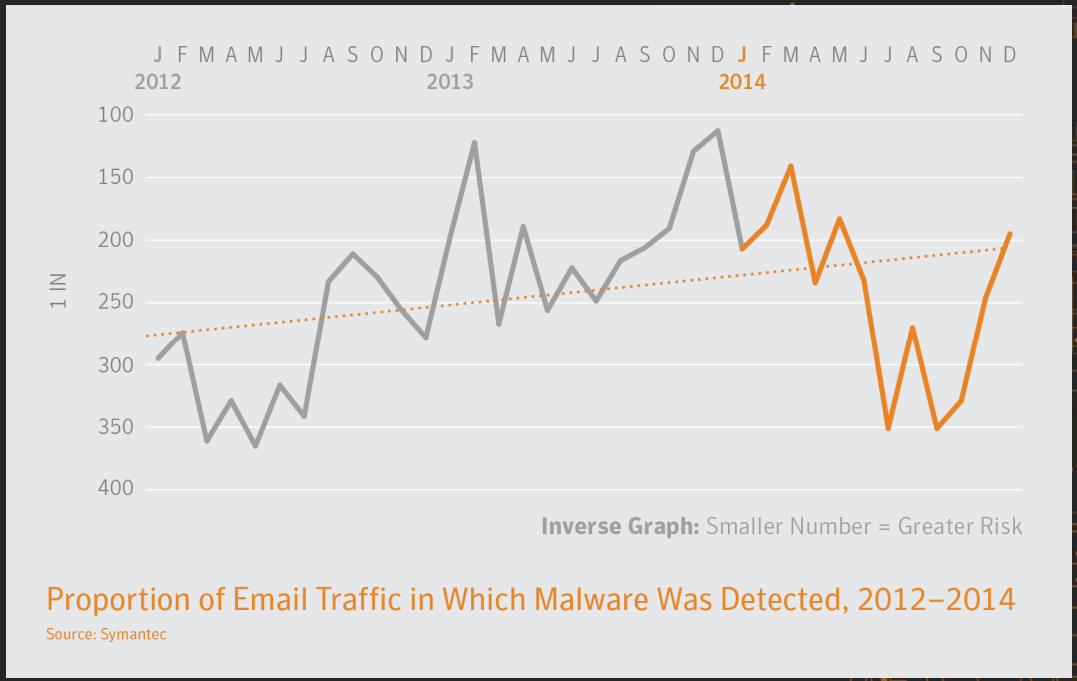
- Em 2014, **cerca de 28%** dos malwarees eram “virtual machine aware”
- Alguns malwares buscavam por imagens virtuais (Ex: Crisis)

Malware enviados por email – URL x Anexo



- Os atacantes não precisam esconder o malware em URLs no email
- Anexos ainda são funcionais para infectar usuários

Proporção de emails identificados com malware



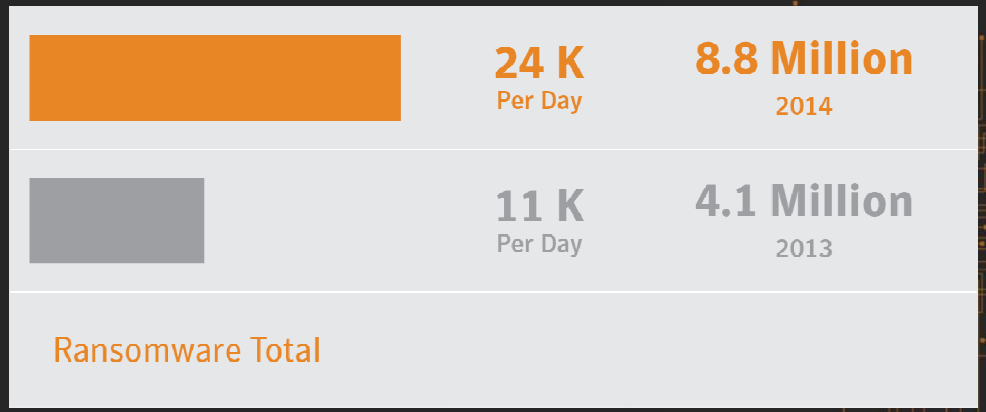
Proportion of Email Traffic in Which Malware Was Detected, 2012–2014

Source: Symantec

- Proporção de malware no e-mail continua a crescer

Extorsão digital em ascensão: 45 vezes mais pessoas tiveram seus dispositivos “reféns” em 2014

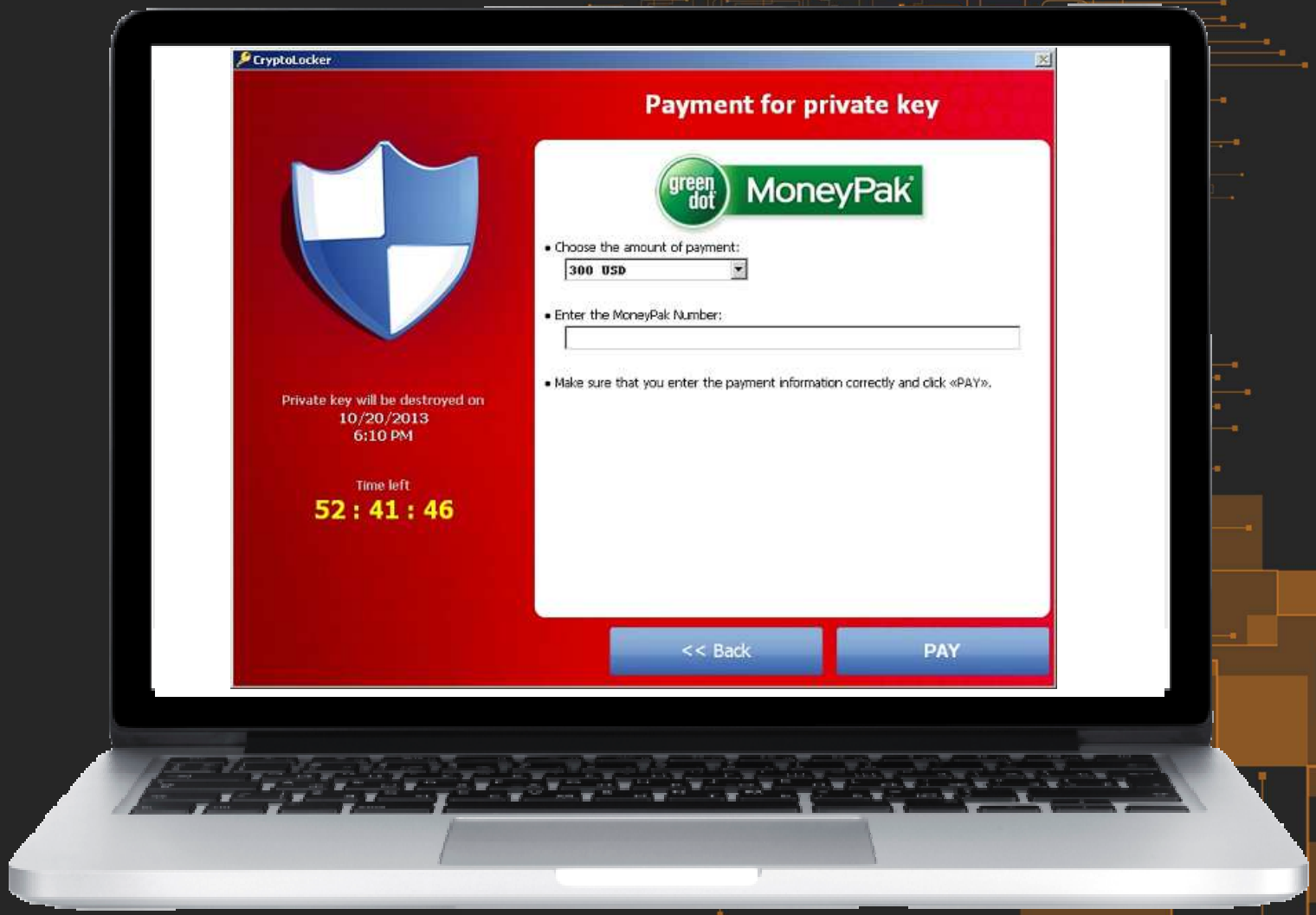
Ransomware



- **Aumento de 113%** em 2014
- Ransomware continua sendo uma crescente ameaça para empresas e usuários domésticos

Ransomware – Evolução (2013)

Ransomware - Evolução (2014) Crypto-Ransomware



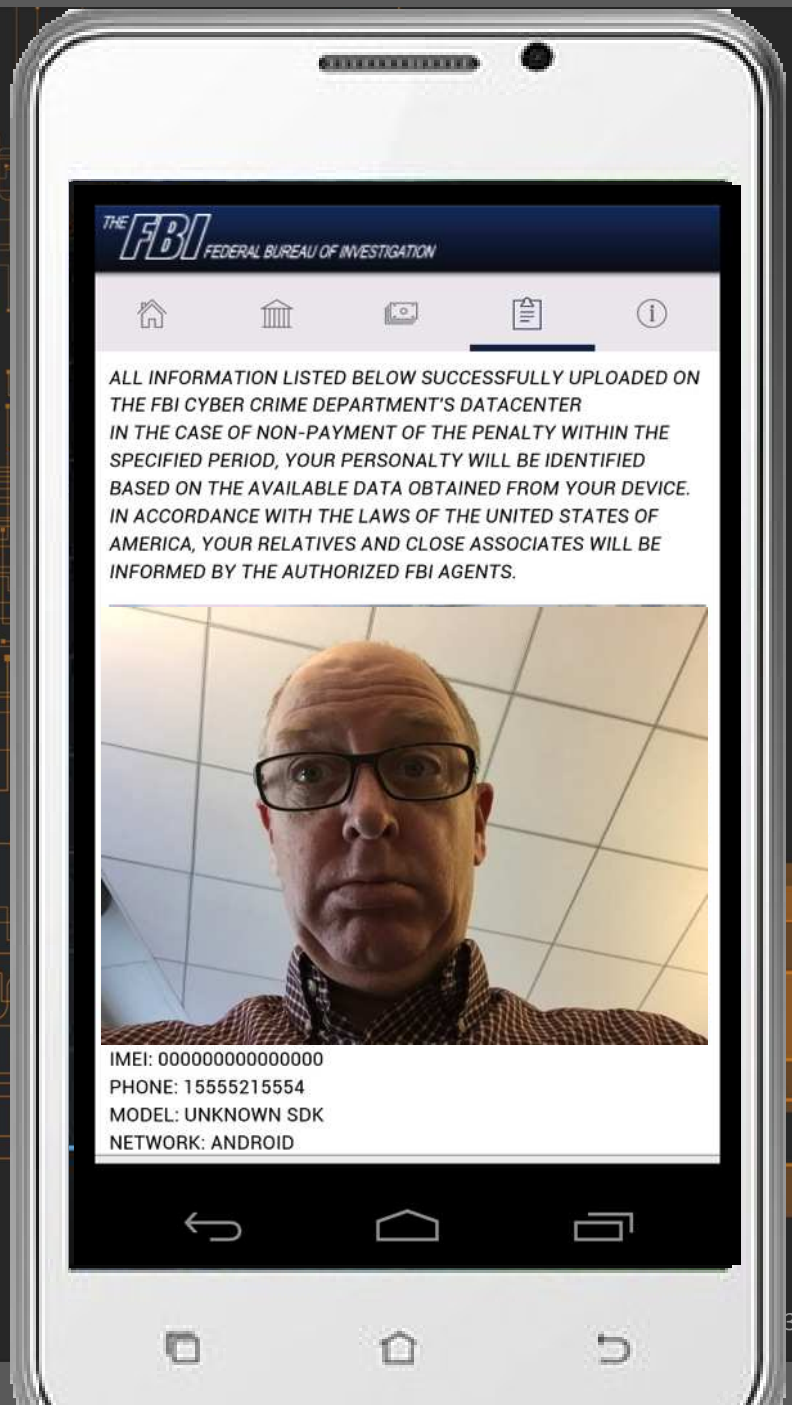
Ransomware – Evolução (futuro)

- Crypto-Ransomware continua tendo como alvo:
  - Aquivos Office e PDF
  - Arquivos pessoais e fotos
- Crypto-Ransomware continua tendo como alvo:
  - Mapeamentos de rede
  - Attached storage
  - Cloud storage (como mapeamento de rede)
- Mas está procurando novos alvos:
  - Em 2014, Synolocker “mirou” drives NAS
  - Em 2014, surigiu o primeiro crypto-ransomware para smartphones

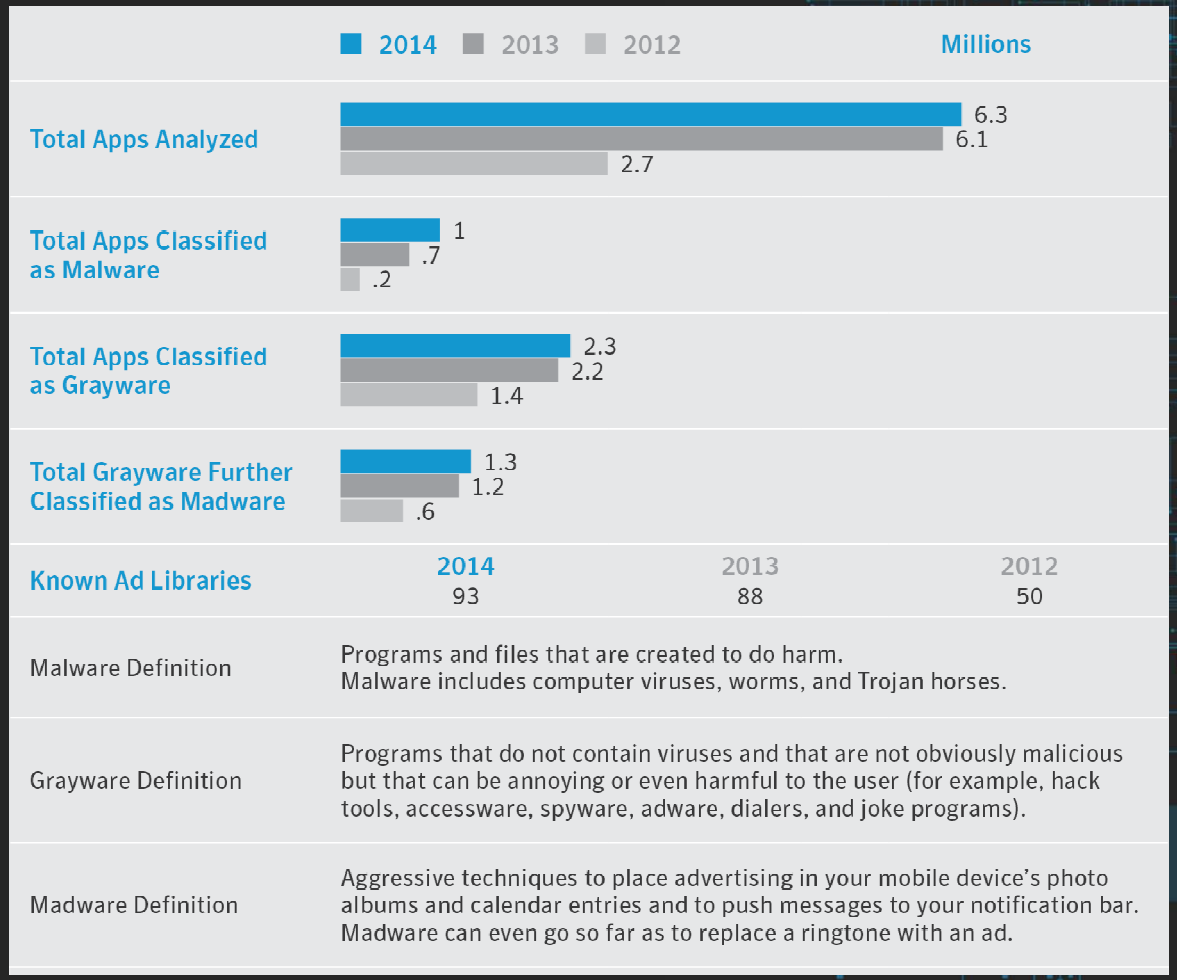
Ransomware Evolução

Mobile - Android.Simplocker

- Simplocker: 1st crypto-ransomware para Android
- A camera do telefone também é alvo do hijacking (sequestro)



Análise das aplicações pelo Symantec's Mobile Insight



	2014	2013	2012
Known Ad Libraries	93	88	50

Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious but that can be annoying or even harmful to the user (for example, hack tools, accessware, spyware, adware, dialers, and joke programs).
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.

IoT não é um “problema” novo, mas está em evidência

Ploutus: 2013

Symantec Official Blog

Criminals Hit the ATM Jackpot

By: Daniel Regalado SYMANTEC EMPLOYEE

Created 11 Oct 2013

0 Comments | Translations | Share

It's well-known that organized crime in Mexico is always finding new ways to steal money from people. Automatic teller machines (ATMs) are one of the common targets in this effort, but the challenge there is actually getting the money out of the machine. The three most common ways to accomplish this are:

Backoff: 2014

Darlloz: 2014

Symantec Official Blog

IoT Worm Used to Mine Cryptocurrency

By: Kaoru Hayashi

Created 19 Mar 2014

0 Comments | Translations | Share

Last November, we found an Internet of Things (IoT) worm named Linux.Darlloz. The worm targets computers running Intel x86 architectures. Not only that, but the worm also focuses on devices running the ARM, MIPS and PowerPC architectures, which are usually found on routers and set-top boxes. Since the initial discovery of Linux.Darlloz, we have found a new variant of the worm in mid-January. According to our analysis, the author of the worm continuously updates the code and adds new features, particularly focusing on making money with the worm.

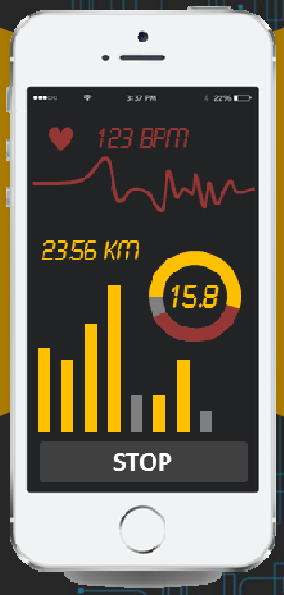
IoT: Arquitetura de risco

- Mesmo considerando ou não smartphones parte da IoT, eles são parte da arquitetura de riscos, com aplicativos muitas vezes sendo a interface do usuário para a IoT.

Aplicativos de saúde e segurança: Exemplo

SEM POLÍTICAS DE PRIVACIDADE

52%



PII/LOGIN TEXTO CLARO

20%*

- Quantos outros aplicativos e sites a mesma senha é usada?

*Serviços de necessitam de login

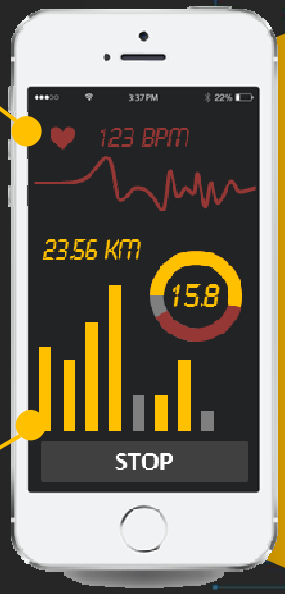
Como os dados dos aplicativos são compartilhandos?

MAX DOMÍNIOS CONTACTADOS

14

AVG DOMÍNIOS CONTACTADOS

5



PP ANALYTICS

D NETWORKS

PP PROVIDER

S PROVIDER

OCIAL MEDIA

PP FRAMEWORKS

RM/MARKETING

TILITY API

- Cada um desses fornecedores poderia compartilhar seus dados novamente

Internet of Things e a Privacidade

1 em 4 Usuários finais *admitem* não saber que tipo de acesso estão permitindo quando concordam com os termos de uso do app

68% Estão dispostos a trocar privacidade para utilizar um app *grátis*

Source: 2014 Norton Global Survey

Symantec.

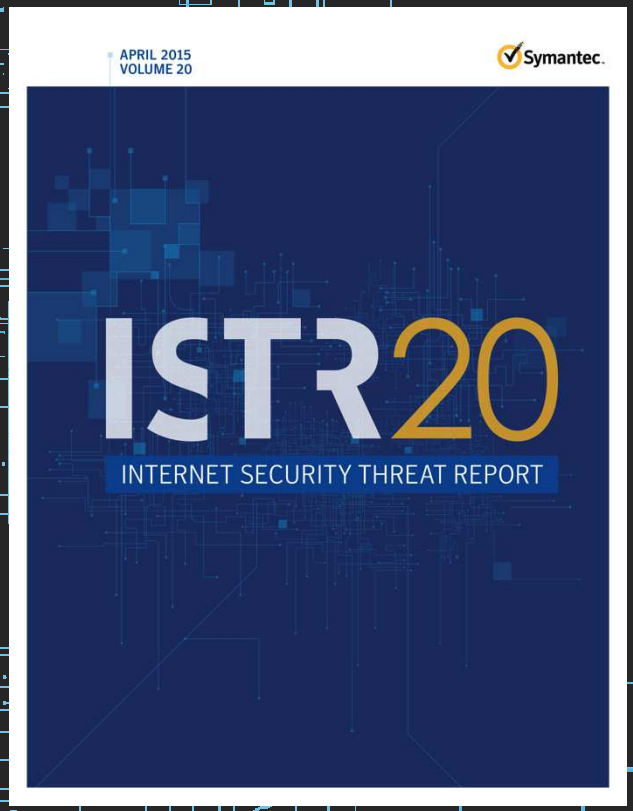
ISTR20

INTERNET SECURITY THREAT REPORT

Melhores práticas & Soluções

Melhores práticas

Não seja pego de surpresa	Use soluções de inteligência contra ameaças avançadas para ajudá-lo a encontrar indicadores de exposisão e que ajudem responder mais rapidamente a incidentes.
Adote uma postura de segurança forte	Implemente uma segurança de endpoint em múltiplas camadas, proteção de rede, criptografia, autenticação forte e tecnologias baseadas em reputação. Parceria com provedor de serviços gerenciados de segurança para aumentar seu time de TI.
Prepare-se para o pior	Gerenciamento de incidentes garante que sua estrutura de segurança está otimizada, mensurável e repetível, e que as lições aprendidas irão melhorar sua postura de segurança. Considere utilizar um especialista externo para ajudar a gerenciar as crises.
Fornecer treinamento e educação contínua	Estabelecer diretrizes e políticas da empresa e procedimentos para proteger dados sensíveis em dispositivos pessoais e corporativos. Regularmente avaliar suas equipes e usuários com relação a postura de segurança. Manter as equipes de resposta a incidentes sempre treinadas e atualizadas.



Obrigado!

symantec.com/threatreport

@threatintel

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.