Unidade de Combate a Crimes Cibernéticos

Microsoft

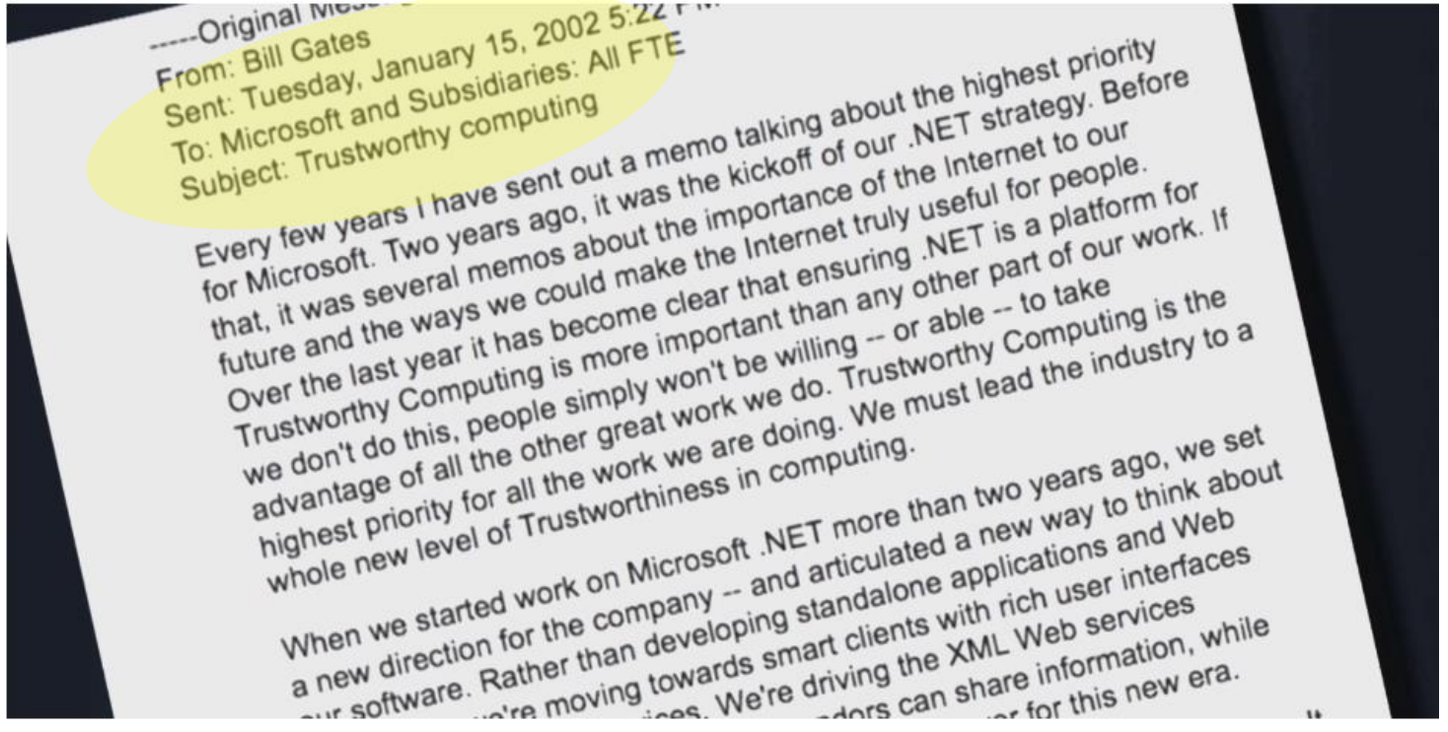
- 26 anos de operação da Microsoft no Brasil
- Maior Centro de Tecnologia da Companhia na América Latina
- Capacitação profissional de jovens e viabilização de oportunidades de emprego e empreendedorismo: mais de 11,6 milhões de jovens beneficiados
- Fomento à competitividade nacional - a cada R$1 real faturado pela Microsoft, outros 11 reais são gerados para a economia brasileira
- **Investimento no combate a crimes cibernéticos:**

  - ✓ Mais de U$ 10 Milhões investidos na criação do Centro de Combates a Crimes Cibernéticos
  - ✓ Mais de 100 profissionais dedicados
  - ✓ Pioneirismo, proatividade e investimentos constantes para manutenção e aperfeiçoamento das estratégias para fomentar um ambiente digital mais seguros para os usurários

Microsoft

15 DE JANEIRO DE 2002
MANIFESTO SOBRE A IMPORTÂNCIA DE UMA COMPUTAÇÃO CONFIÁVEL PARA A MICROSOFT

"Se nós não fizermos isso [computação confiável], as pessoas não poderão se beneficiar de todas as outras coisas boas que fazemos na Microsoft. Computação Confiável é a maior prioridade da Microsoft."



Iniciativa Pública

Inicitativa Privada

Ecosistema de segurança

Serviços Públicos
Empresas de tecnologia
Cadeia de Fornecedores

CERTs
Provedores de Acesso a Internet

Cada segmento define suas próprias estratégias de combate a ameaças cibernéticas

Estrategias Individuais: Impacto causado às organizações criminosas

UMA NOVA ERA NO COMBATE AOS CRIMES CIBERNÉTICOS

2002… PIONEIRISMO E PRÓ-ATIVIDADE

PARCERIAS COLABORATIVAS …2015…

Unidade de Combate a Digitais

- **Computação Confiável** — Segurança, Confiança, Privacidade
- **Setor Público** — Soluções, Iniciativas, Inovação
- **Setor Privado** — Soluções, Iniciativas, Inovação
- **Usuários da Internet** — Identificação de Riscos, Serviços de segurança cibernética

Autoridades Policiais · Governo · Iniciativa Privada

CRIMES CIBERNÉTICOS

- Virus
- Trojans
- Worms
- Botnets

EXPLORAÇÃO INFANTIL

- Pornografia infantil
- Crianças desaparecidas

MICROSOFT Digital Crimes Unit

Big data

Investigações

Medidas Legais

“Segurança cibernética é um assunto de responsabilidade do CEO.”

-McKinsey & Co, Riscos e responsabilidades em um mundo super conectado: Implicações corporativas, Janeiro 2014.

243
É a média de dias que dispositivos ficam infectados por malware antes que estes sejam detectados

USD 3 trilhões
É o prejuízo financeiro causado por ataques digitais (perda de produtividades e crescimento econômico

USD 3.5M
É o custo médio do vazamento de informações confidenciais de uma empresa (15% de aumento anual)

VISÃO

Promover uma experiência digital mais segura para usuários da internet

Missão

Redução de riscos digitais

Proteção de populações vulneráveis





Missão:Proteção de populações vulneráveis





O Problema

1 em cada 5 meninas

São abusadas **sexualmente**
antes de completarem
18 anos.

1 em cada 10 meninos

500 imagens de pornografia infantil circulam na internet a cada **60 segundos.**

O Problema

1.8 bilhão

imagens são salvas e compartilhadas online **diariamente**

Achar uma imagem específica de pornografia infantil entre bilhões é como **procurar uma agulha no palheiro.**

A Solução: Microsoft PhotoDNA

Tecnologia **doada** pela Microsoft ao Centro Internacional de Proteção a Crianças Exploradas e Desaparecidas (ICMEC)

Ferramenta licenciada gratuitamente para mais de 70 organizações de diversos países, incluindo Facebook, Twitter, Google

Outlook.com bing OneDrive

facebook Google

A Tecnologia PhotoDNA

IMAGENS CONTIDAS NA PLATAFORMA DO USUÁRIO

Photo DNA: Parceria entre Microsoft, NCMEC e a Universidade de Dartmouth – Tecnologia desenvolvida para ajudar encontrar imagens de crianças exploradas.

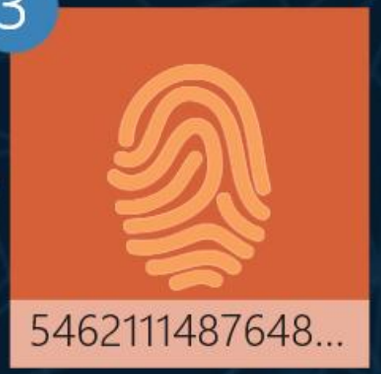
1

Imagem de pornografia infantil identificada pelo NCMEC ou outra autoridade competente

2

PhotoDNA cria uma assinatura digital única (impressão digital) para cada foto

3



As impressões digitais de imagens contidas no banco de dados do PhotoDNA são comparadas com imagens contidas na plataforma do usuário.

4

Mesmo quando alteradas as imagens são identificadas em função da impressão digital que lhe foi originalmente atribuída.

5

A comparação positiva de imagens do banco de dados com a imagem submetida pelo usuário dá origem a medidas legais promovidas por autoridades competentes.





Missão: Redução de Riscos Digitais





Estrutura
Crimes Cibernéticos

MALWARE: Programas de computador especificamente desenvolvidos para cometer crimes através ou por intermédio de um computador.

BOTNET: Programa que dispõe de mecanismos de comunicação entre a máquina infectada e o criminoso que permite que este envie instruções de ações criminosas.

MICROSOFT
Digital Crimes Unit

PARCERIAS PÚBLICO-PRIVADAS
OPERAÇÕES DE COMBATE A MALWARES E BOTNETS

OPERAÇÃO Conficker

Fevereiro 2010

Primeira operação mundial de desativação de malware liderada pela Microsoft.

Botnet Worm

OPERAÇÃO Waledac

Fevereiro 2010

Segunda operação de desativação de malware.

Libertou aproxim. 90,000 dispositivos infectados

Spam

OPERAÇÃO Rustock

Março 2011

Operação multisetorial realizada em parceria por diversos setores da indústria

Envolveu autoridades de inteligência dos EUA e Alemanha e o CN-CERT.

Spam

OPERAÇÃO Kelihos

Setembro 2011

Parceria entre Microsoft e outras empresas de software e segurança

Primeira operação em que o réu foi previamente identificado.

Spam, Bitcoin Mining, Ataques de negação de serviço (DDoS)

OPERAÇÃO Zeus

Março 2012

Parceria com instituições financeiras.

Operação de altíssima complexidade técnica.

Roubo de Identidade/ Fraude Financeira

OPERAÇÃO Nitol

Setembro 2012

Malware infectou uma cadeia de fornecedores de grandes empresas chinesas.

Acordo realizado com o operador do malware.

Disseminação de malwares e Ataques de negação de serviço (DDoS)

OPERAÇÃO Bamital

Fevereiro 2013

Roubo de resultado de buscas e substituição desses sites procurados por sites maliciosos.

Operação realizada em parceria com a Symantec. Notificações às vitimas e limpeza das máquinas infectadas.

Click Fraud de anúncios

OPERAÇÃO Citadel

Junho 2013

Fraudes financeiras online, tendo causado prejuízo estimado de mais US$ $500M

Operação coordenada através de parceria público-privada

Roubo de Identidade/ Fraude Financeira

OPERAÇÃO ZeroAccess

Dezembro 2013

Roubo de resultado de buscas e substituição desses sites procurados por sites maliciosos.

Anunciantes tiveram prejuízo mensal estimado em US$ $2.7 milhões

Click Fraud de Anúncios

OPERAÇÃO Game over Zeus

Junho 2014

Cavalo de Tróia (trojan) de ataques a banco

Roubo de Identidade/ Fraude Financeira

OPERAÇÃO Bladabindi & Jenxcus

Junho 2014

Utilização de DNS dinâmicos para controle remoto. Foco em roubo de identidade e senha, ativação de webcam e microfone.

Mais de 200 diferentes tipos de malware impactados.

Roubo de Identidade/ Fraude Financeira/ Invasão de Privacidade

OPERAÇÃO Caphaw

Julho 2014

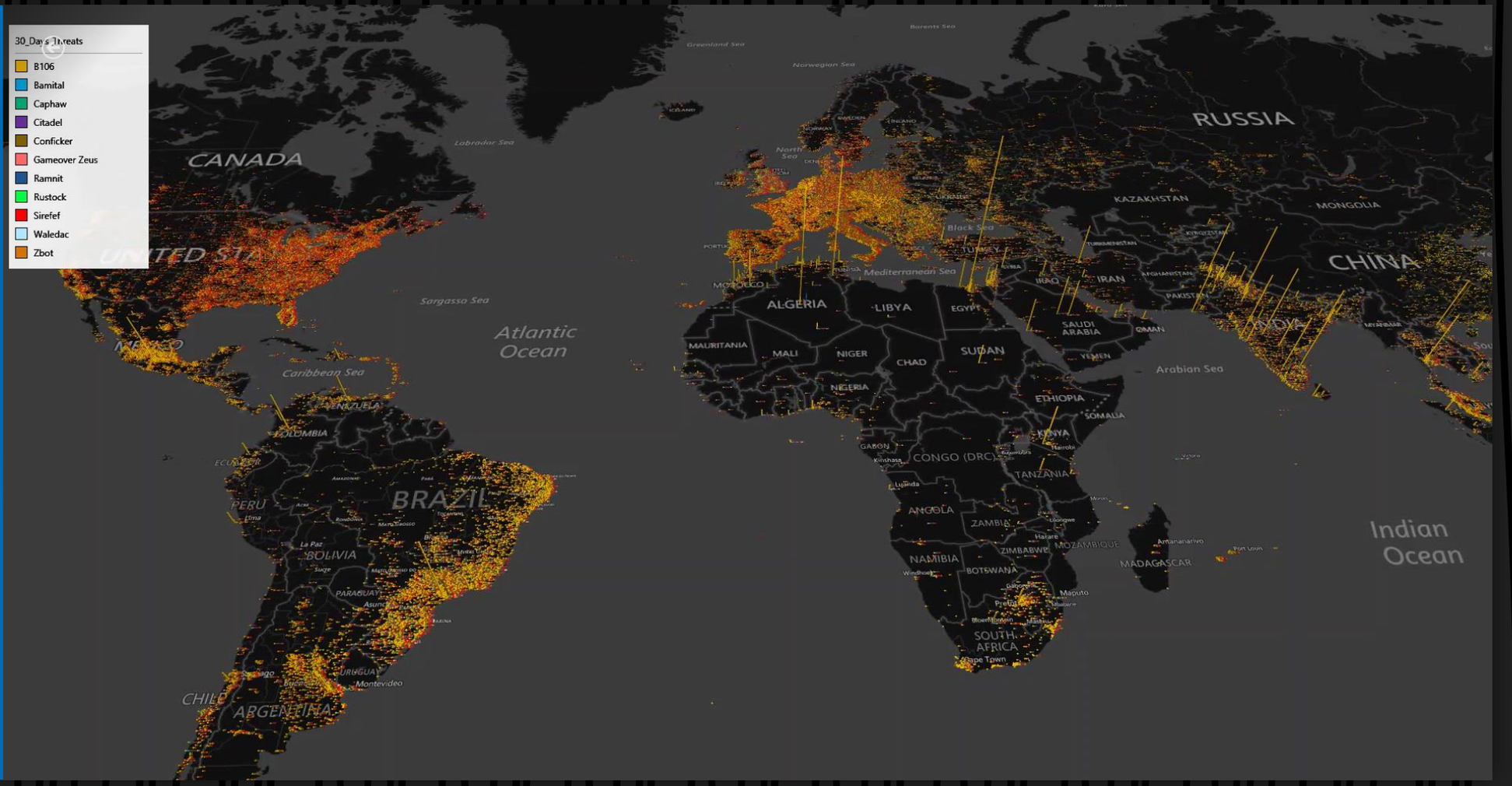
Malware de fraudes financeiras responsável por prejuízos estimados em US$250 milhões

Roubo de Identidade/ Fraude Financeira

Programa de Inteligência sobre Ameaças Cibernéticas (CTIP)

60 milhões de endereços IP comprometidos

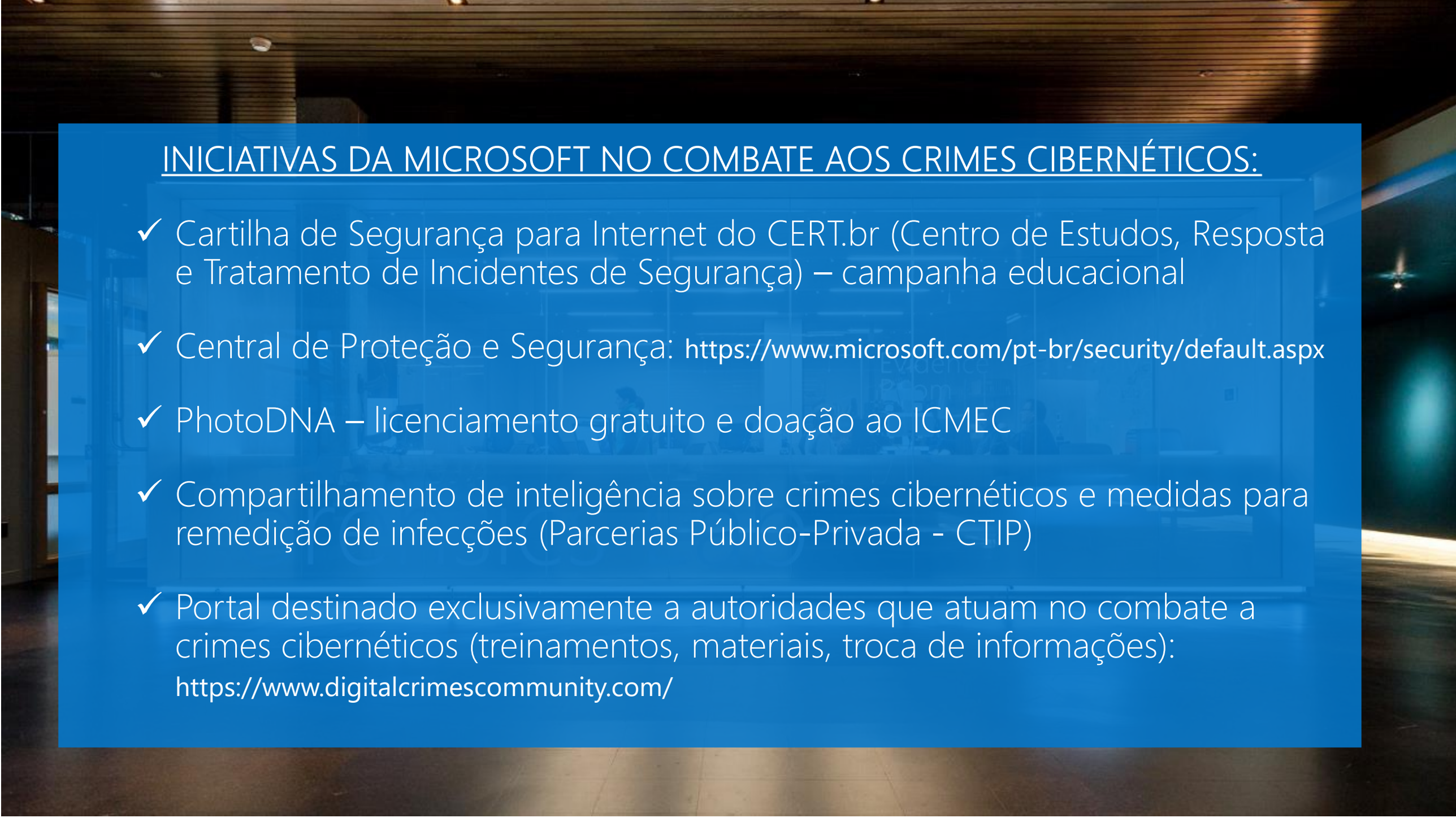
Compartilhamento dessas informações



Programa de Inteligência sobre Ameaças Cibernéticas (CTIP)

No Brasil, o número de IP comprometidos varia entre 2 a 5 milhões

Centros de Tecnologia Microsoft



INICIATIVAS DA MICROSOFT NO COMBATE AOS CRIMES CIBERNÉTICOS:

- ✓ Cartilha de Segurança para Internet do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança) – campanha educacional
- ✓ Central de Proteção e Segurança: https://www.microsoft.com/pt-br/security/default.aspx
- ✓ PhotoDNA – licenciamento gratuito e doação ao ICMEC
- ✓ Compartilhamento de inteligência sobre crimes cibernéticos e medidas para remedição de infecções (Parcerias Público-Privada - CTIP)
- ✓ Portal destinado exclusivamente a autoridades que atuam no combate a crimes cibernéticos (treinamentos, materiais, troca de informações): https://www.digitalcrimescommunity.com/