(ISC)²

SECURITY CONGRESS | LATIN AMERICA 2015

Patrocinador Platinum:

DELL

Patrocinadores Gold:

Deloitte. Level(3) BLUE COAT

Parceria e Organização:

(ISC)² SEMINÁRIOS Valor mci

(ISC)²

SECURITY CONGRESS | LATIN AMERICA 2015

DFIR – A new paradigm

- Marcelo Caiado

Sumário

- Crimes Digitais
- Forense Digital
- Resposta a Incidentes
- Novo Paradigma
- Conclusões

01.

CRIMES DIGITAIS

(ISC)
SECURITY CONGRESS
LATIN AMERICA
2015

Crimes Digitais

Kansas serial killer, the BTK Killer, installed alarms as a part of his job, and many of his clients had booked the company to stop BTK from ever entering their homes, unaware that BTK himself was installing them.

Teenage killer who tortured and suffocated classmate, 18, had left digital trail of sick plot and confessed on World of Warcraft

By HANNAH ROBERTS
UPDATED: 19:56 GMT, 9 November 2011

Share 21 View comments

Like many teens, 16-year-old Kruse Wellwood, from British Columbia spent as much time with his friends online as in the real world.

So when he messaged his classmate Kim Proctor on MSN, asking why she hadn't met up with him, there was nothing strange in it.

The only unusual thing, on this day, was that he wasn't expecting a reply.

Hackers são educados e financiados, afirma especialista

Golpe no WhatsApp usa McDonald's para roubar dados

Recomende

Malware rouba mais

Autor: **Redação**
Fonte: **IT Forum 365**
Publicado em 31 de Agosto de 2015 às 16h05

Usuários de 18 países foram

Canadá, Estados Unidos, Itália, Espanha, Coreia do Sul.

As credenciais foram capturadas por meio chamado de KeyRaider realizou o upload conta disso, os pequisadores puderam rea servidor de controle para identificar o probl

De acordo com o pesquisador da Palo Alt divulgado.

O malware, por meio do MobileSubstrate, dispositivo. O KeyRaider também rouba os certificados do serviço de notificações push da Apple e chaves privadas, rouba e compartilha informações de compras feitas por meio da App Store, bem como desabilita remotamente funções de iPhones e iPads.

Pedófilos assediam participante do MasterChef pelo Twitter

Recomende

546.059 views - Salvar notícia

Reprodução/Facebook

Valentina Schulz, do MasterChef Júnior, com o jurado Erick Jacquin

10.802 views - Salvar notícia

Brent Lewin/Bloomberg

dados dos usuários do app

Exibir online

zip

MAÇAO-MPF.rar (342k).

Crimes Digitais

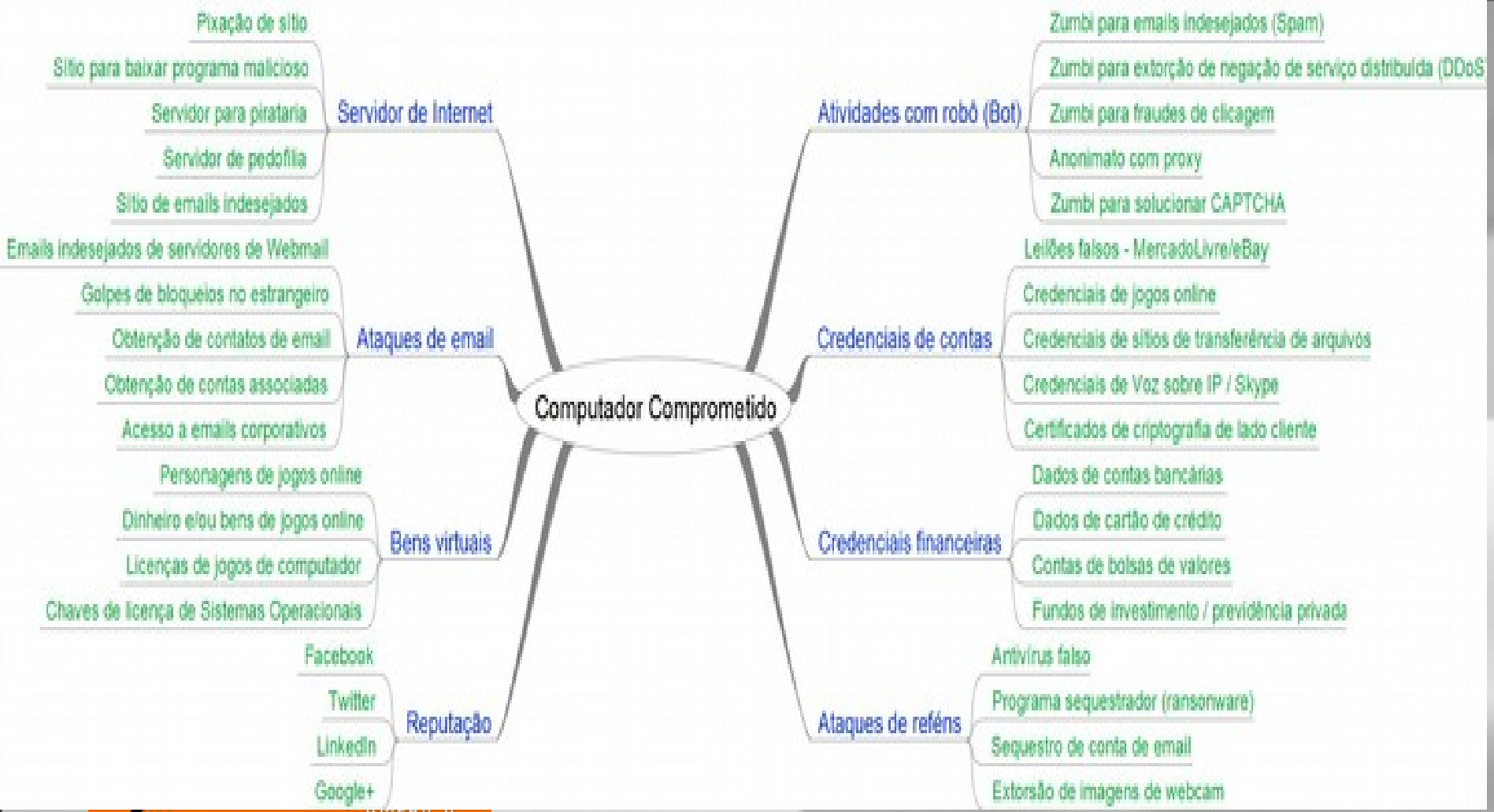
- O crime é organizado
  - Transnacional: ShadowCrew, Russian Business Network, Superzonda (América do Sul), Yakuza
  - Ubíquo

Crimes Digitais

- Classificação
  - Crimes digitais próprios (ou puros)
  - Crimes digitais impróprios (ou mistos)

Crimes Digitais

- Estratégias dos criminosos
  - Fazem forte uso da Engenharia Social
  - Criam oportunidades a partir de notícias: atentado terrorista em Paris, escândalo no Vaticano, etc
  - Exploram vulnerabilidades muitas vezes já conhecidas (e que possuem correções)



Fonte: http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

02.

FORENSE DIGITAL

(ISC)
SECURITY CONGRESS | LATIN AMERICA 2015

Forense Digital

- Perícia Digital
  - “É a preservação, aquisição, análise, descoberta, documentação e apresentação de evidência presente em meio digital” – Dan Farmer & Wietse Venema

Forense Digital

(ISC)²
SECURITY CONGRESS | LATIN AMERICA 2015

Forense Digital

Forense Digital

Technical review of the Trial Testimony
State of Connecticut vs. Julie Amero

March 21, 2007

Contributors (alphabetical order):

Alex Eckelberry
Glenn Dardick, Ph.D.
Joel A. Folkerts
Alex Shipp
Eric Sites
Joe Stewart
Robin Stuart

Forense Digital

- Casos emblemáticos
  - Invasão da RSA e Lockheed Martin
  - Empresa varejista Target (US$ 148 milhões de prejuízo)
  - Privatização (?!?) do Ministério Público
  - Operação Darknet

03.

RESPOSTA A INCIDENTES

(ISC)²
SECURITY CONGRESS | LATIN AMERICA 2015

Resposta a Incidentes

Ashley Madison: CEO se demite após escândalo de vazamento de dados

Executivo Noel Biderman entrou em acordo com empresa que opera site. Hackers vazaram 2 pacotes de dados do site: um de 10 GB e outro de 13 GB.

Da France Presse

FACEBOOK

Resposta a Incidentes

Vítimas de ciberataque não recebem informações

Reuters

Menos de um quarto dos 21 milhões de funcionários federais dos Estados Unidos atingidos por um grande ataque hacker foram oficialmente comunicados de que suas informações pessoais foram comprometidas, seis meses após o vazamento ter sido detectados, disse uma autoridade do governo norte-americano nesta terça-feira.

Cerca de 5 milhões de notificações sobre o ataque foram enviadas até agora, disse um porta-voz do Escritório de Gestão de Pessoas dos EUA (OPM, na sigla em inglês) à Reuters via e-mail.

A lentidão no processo de notificação ressalta a dificuldade de Washington em lidar com suas vulnerabilidades em informática, um crescente problema que o governo do presidente Barack Obama tem tentado solucionar.

Após ser vítima de dois ciberataques sucessivos, ambos iniciados em 2014 e revelados este ano, o OPM foi muito criticado por parlamentares.

O OPM não tinha comentários adicionais a fazer imediatamente sobre o assunto nesta terça-feira, ou sobre seu esperado cronograma de notificações.

Autoridades culparam a China pelo vazamento do OPM.

Resposta a Incidentes

Resposta a Incidentes

Open Incidents by Phase

Priority	Engage	Detect/Analyze	Respond	Post-Incident	Total
Low	2	0	0	0	2
Medium	7	0	0	0	7
High	3	0	0	0	3
Breach	2	0	0	0	2
Criminal Activity	1	0	0	0	1

Resposta a Incidentes

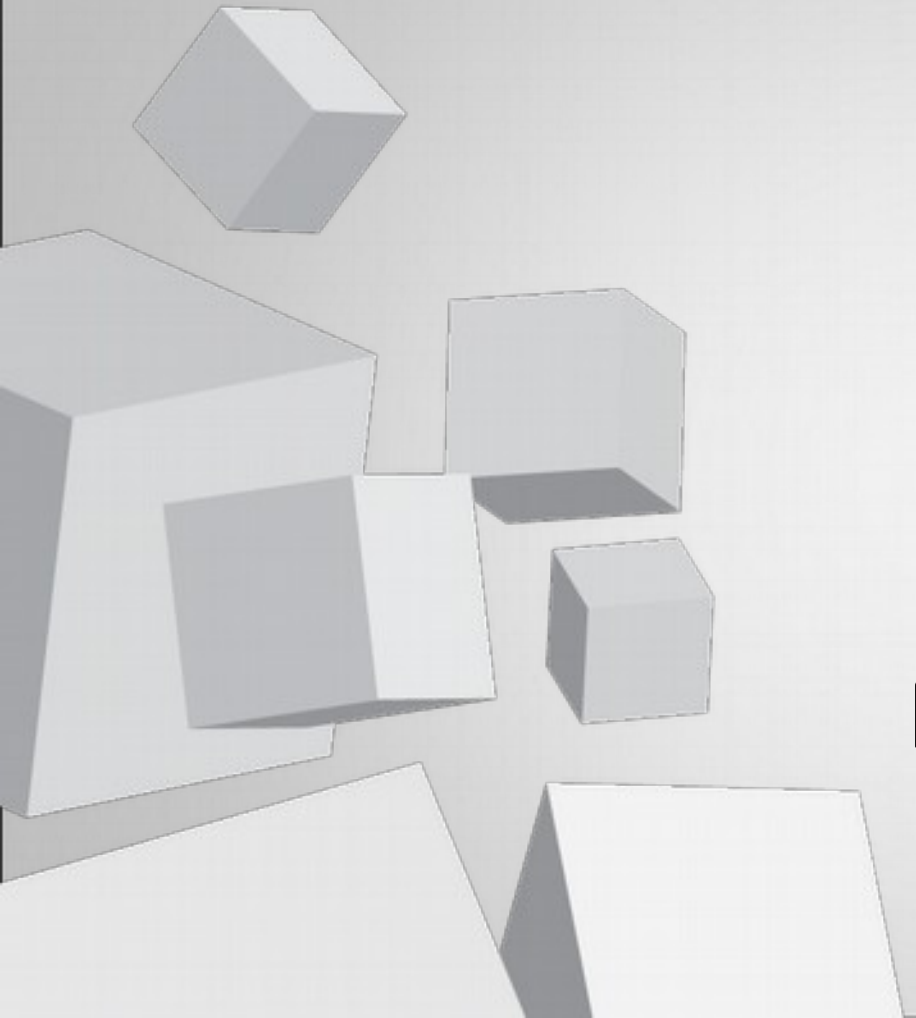
"Sed quis custodiet ipsos custodes?"

Decimus Iunius Iuvenalis (Juvenal)

Resposta a Incidentes

- Saiba onde sua informação está, e quem pode acessá-la
- Compartilhe conhecimento com seus competidores

- Monitore a segurança de sua rede e aplicações
- Segurança física e de pessoal



04.

NOVO PARADIGMA

Novo Paradigma

- Criminosos expandindo atividades

HOSPEDAGEM R50.00$

Local perfeito para colocar sua FAKE ou VIRUS ou SCRIPT MALICIOSO!

- Hospedagem Rapida
- Ilimitados Mysql
- Dominio Incluso

Viral Facebook R70.00$

Novo Viral Facebook o mais versatil sistema de CURTI + COMPARTILHAR. Espalhe um INFECT rapidamente, com apenas poucas shares seu Viral se propaga rapidamente.

Testador de CC R400.00$

Contratar agora »

Serviço de programador R500.00$

do papel! Traga sua ideia, seu plicação, que programaremos Trabalhamos com

os os OS
os os Browsers

Contratar agora »

FÊNIX BUSCAS

Fenix Jose Dos
(Fenix Buscas)

Linha do Tempo

Moc Consultas

Linha do Tempo Sobre Amigos Fotos Mais

FRAUDE GARANTIDA OU SEU DINHEIRO DE VOLTA

Naturalmente, no meio de uma negociação que envolve dados sigilosos, a desconfiança é mútua entre vendedor e comprador. O cliente está quase sempre com medo de pagar e não receber, mas, em nossa experiência, os comerciantes se mostraram bastante receptivos e generosos, oferecendo períodos de teste para os sistemas ofertados. Um deles chegou a prometer "total suporte" ao consumidor, garantindo um login novo caso a credencial comprada pare de funcionar.

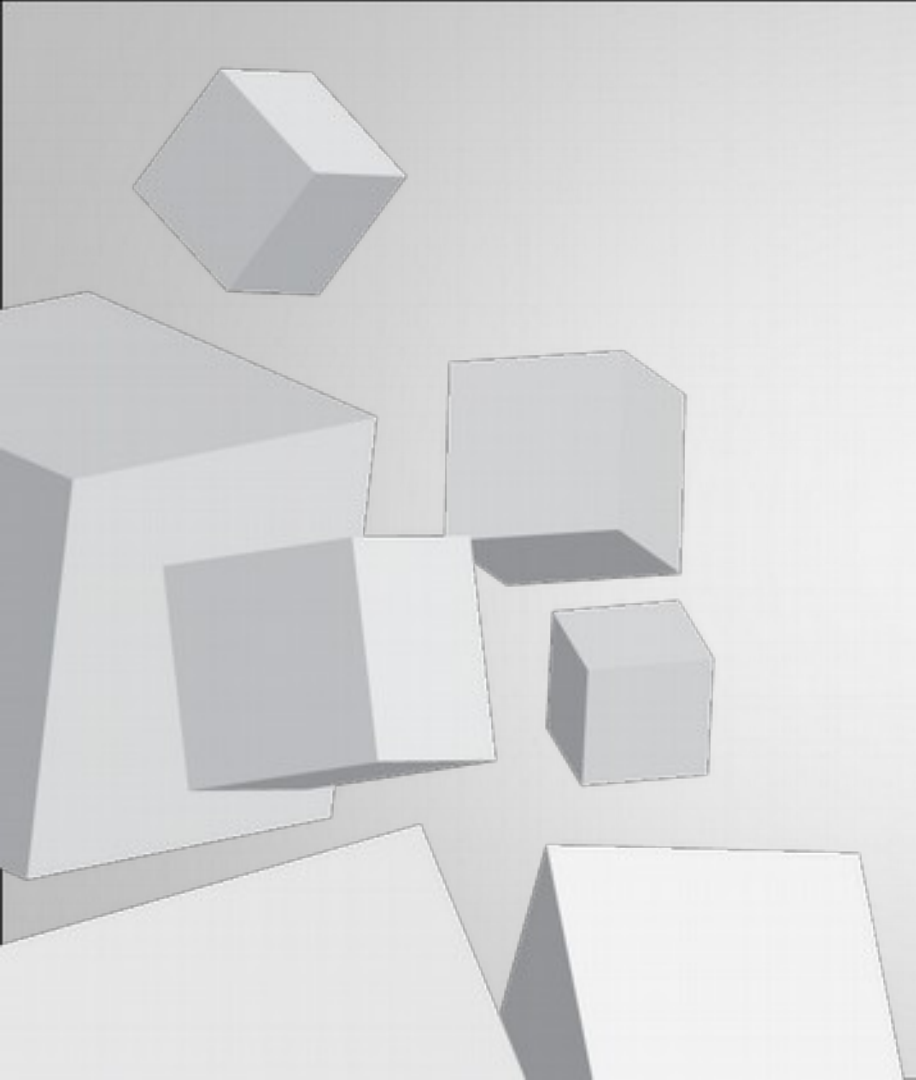
Existe todo um submundo da delinquência eletrônica, uma comunidade espalhada por todos os cantos do país, que se ajuda e se completa com um único objetivo em comum: cometer fraudes e causar danos a terceiros.

Novo Paradigma

- Maior integração das áreas de suporte técnico, SOC, NOC e DFIR (e Jurídico e RH)
- Investimentos em certificações correlatas
- Adequação das ferramentas forenses

Novo Paradigma

- Internet das Coisas (IoT) => incremento do MMO (Motivação, Meio e Oportunidade)
- Legislação específica e cooperação internacional
- Maior preocupação com privacidade de dados
- Regulamentação da profissão de Perito Digital



05.

CONCLUSÕES

(ISC)²
SECURITY CONGRESS | LATIN AMERICA 2015

Conclusões (1)

"Temos de identificar e deter as pessoas por trás desses teclados de computador e uma vez que identificá-las (…) devemos elaborar uma resposta que seja eficiente não apenas contra o que ataque específico, mas para toda a atividade ilegal semelhante ."

Robert Mueller, Diretor do FBI

Conclusões (2)

"Mesmo a melhor infra-estrutura de segurança da informação não pode garantir que intrusões ou outras ações maliciosas não ocorrerão. Quando um incidente de segurança ocorre, torna-se crítico para a organização ter uma maneira eficaz de responder a este incidente."

Tradução: CERT/CC CSIRT FAQ – http://www.cert.br/certcc/csirts/csirt_faq-br.html

Para refletir

"Eduquem as crianças e não será necessário castigar os homens"

Perguntas

http://dfir.com.br