Segurança da Informação e Perícia Digital onde estamos e para aonde vamos?

Prof. M.Sc. Marcelo Caiado

Disclosure

Todas as opiniões aqui apresentadas são exclusivas do palestrante, apenas de caráter ilustrativo e não possuem nenhum vínculo o MPF, o SANS Institute, ou qualquer outra instutição

“As mesmas novas tecnologias que permitiram o avanço e a automação de processos de negócio, também abriram as portas para muitas novas formas de uso indevido de computadores”

Thomas Welch

Apresentação

- Graduado em Processamento de Dados / UCB 1994
- Graduado em Sistemas de Informações / UNEB 1997
- Mestre em Ciência da Computação / UnB 2001
- Analista do MPU / Perícia / TIC – Abril 1997, até a presente data
- CyberForensics Analyst / Research In Motion – 2008 a 2010
- Especialista em Gestão Pública / FGV 2016
- Certificado CISSP, GCFA, GCIH, EnCE
- Mentor de cursos do SANS Institute

Apresentação

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

Malware rouba mais de 225 mil credenciais Apple

Pedófilos assediam
participante de

Hacker deixa cidade sem luz usando um
do Office

Autor: Redação

27.181 views · Salvar notícia

Freeimages.com

Hack Of Federal Gov't Employee Info Is Much, Much Worse Than Originally Stated: Unencrypted Social Security Numbers Leak

Failures
by Mike Masnick
Fri, Jun 12th 2015
7:43am

Filed Under: cybersecurity, federal government, leaks, opm, social security numbers, unencrypted

Permalink.

from the *because-that*

Over a decade ago, I p
hacking, a few weeks a
than originally reporte
Last week, we noted th
likely by Chinese hacke
worse than originally

The President of the un
of Government Employ
hackers got away with
about everything about

> *Based on the ske*
> *Personnel Data*
> *possession of all*
> *up to one millio*
> *affected person's*
> *information, ad*
> *insurance, and p*

Oh, and then there's th

> *Worst, we belie*
> *cybersecurity fai*

metade da cidade

centros de
s de pessoas sem

da empresa de segurança iSight Partners afirmaram que
nostras do código malicioso que causou o blecaute na Ucrânia.

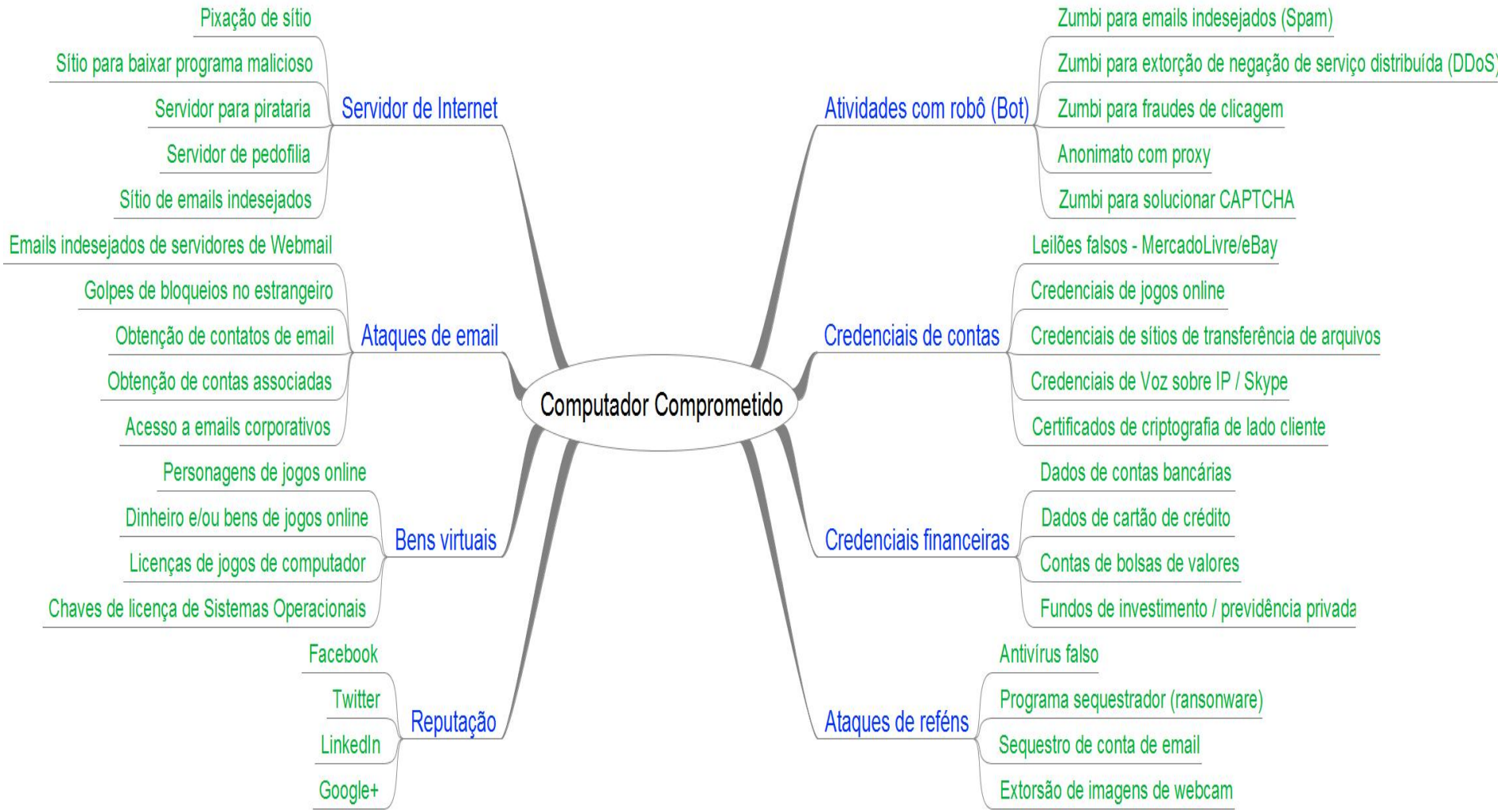
co porque nós já vimos ataques com eventos destrutivos no setor
presas de óleo, por exemplo –, mas nunca tínhamos visto um
ha causado um blecaute", afirmou John Hulquist, chefe de
ciberespionagem na iSight, em entrevista ao *Ars Technica*.

The letter further points out -- as we did last week -- that the 18 months of credit monitoring the government has offered everyone is a complete joke. It's unlikely that the hackers are looking to do identity fraud for financial gain -- and quite likely this is for espionage purposes.

But, let's go back to the Social Security numbers being unencrypted for a second. Remember, this hack is *already* **being used** by intelligence system defenders to argue for why we need stronger "cybersecurity" laws that will give the NSA and FBI **much greater** access to Americans' data.

And, yes, this would be the very same FBI that has **actively** argued **against** encryption. And the NSA has **always** hated encryption and insists it **needs backdoors** into any encryption.

Crimes Digitais



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

Crimes Digitais

- **Estratégias dos criminosos**
  - Fazem forte uso da Engenharia Social
  - Criam oportunidades a partir de notícias: Natal, imposto de renda, olimpíadas, escândalo no Vaticano, etc
  - Exploram vulnerabilidades muitas vezes já conhecidas (e que possuem correções) => WannaCry
  - O crime é organizado
  - Transnacional: ShadowCrew, Russian Business Network, Superzonda (América do Sul), Yakuza

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Dark-Web Drug Dealer Arrested After He Travelled US for World Beard Championships

Thursday, September 28, 2017 Mohit Kumar

United States authorities arrested suspected dark web drug kingpin late last month while he was travelling from his base in France to the United States of America for this year's annual World Beard and Mustache Championships.

Gal Vallerius, a 38-year-old French national, was travelling to Austin, Texas, for the competition but was caught by U.S. authorities on August 31 upon landing at Atlanta International Airport on a distribution complaint filed in Miami federal court, The Miami Herald reported Tuesday.

Authorities confirmed Vallerius' identity to the online moniker "**OxyMonster**," which was previously used to sell drugs on an illegal underground dark web marketplace called Dream Market by searching his laptop that the brown-beard contestant carried with him.

EMPTYAGE

Mat Honan's Tumblr

HOME

ARCHIVE

ASK ME, ASK ME, ASK ME

Yes, I was hacked. Hard.

So maybe you saw my Twitter going nuts tonight. Or you saw Gizmodo's Twitter account blow up. Or you saw this in AllThingsD. Or this in the DailyDot. Although embarrassing, Twitter was the least of it. In short, someone gained entry to my iCloud account, used it to remote wipe all of my devices, and get entry into other accounts too.

Here's what happened:

At 4:50 PM, someone got into my iCloud account, reset the password and sent the confirmation message about the reset to the trash. My password was a 7 digit alphanumeric that I didn't use elsewhere. When I set it up, **years and years** ago, that seemed pretty secure at the time. But it's not. Especially given that I've been using it for, well, years and years. My ~~guess is they used brute force to get the password~~ (see update) and then reset it to do the damage to my devices.

The backup email address on my Gmail account is that same .mac email address. At 4:52 PM, they sent a Gmail password recovery email to the .mac account. Two minutes later, an email arrived notifying me that my Google Account password had changed.

At 5:00 PM, they remote wiped my iPhone.

At 5:01 PM, they remote wiped my iPad.

At 5:05, they remote wiped my MacBook Air.

A few minutes after that, they took over my Twitter. Because, a long time ago, I had linked my Twitter to Gizmodo's they were then able to gain entry to that as well.

Here's how I experienced it:

I was playing with my daughter, when my phone went dead. It then rebooted to the setup screen. This was irritating, but I wasn't concerned. I assumed it was a software

Login de usuários

ASHL
MAD

A vida é

Para começar, diga o stat

Selecione

Veja seu

Mais de 45.025.000

Ransom notes sent by blackmailers to wives of Ashley Madison hack victims

Share this content:

Blackmailers have begun sending ransom letters to the wives of alleged users of the extramarital website Ashley Madison.

Blackmailers sent ransom notes demanding Bitcoin from the wives of Ashley Madison hack victims.

The threatening letters demand that the women pay $2,500 in Bitcoin or the blackmailer will tell the woman's friends, family and colleagues that her husband used the site, security blogger Graham Cluley said in a Wednesday post.

The letters also stated the husband was contacted previously via other means but didn't pay the ransom.

Cluley advised recipients not to pay and speculated that the most recent wave of blackmail letters indicated that the threat actors have become desperate after previous attempts failed to persuade the alleged users themselves through blackmail demands sent via email.

So far, only Americans have been targeted and the letters were postmarked from the state of Virginia, according to *The Telegraph*.

Cluley also said the letters are addressed only as "Mrs.," followed by the husband's last name.

"They don't know anything about the wives of the Ashley Madison members so this could be quite a lot of effort involved if the blackmailer actually did want to go through with their scheme," Cluley said.

He advised anyone who has received a letter to contact the proper authorities.

The most recent string of threats comes roughly eight months after hackers, calling themselves The Impact Team, hacked into the Ashley Madison database and leaked "customers' secret sexual fantasies and matching credit card transactions," along with other data belonging to the website's operators.

★★★★ 100% Gente que pensa igual a você

Falan
Com G
Robert
Pânico

SSL Site Seguro

Registre-se no Ashley Madiso

cidade Fale conosco

País: Brasil Idioma: Português (Brasil)

Google

intitle:index.of "cpf" "rg" "jpg"

Todas | Imagens | Notícias | Vídeos | Shopping | Mais | Configurações | Ferramentas

Aproximadamente 436 resultados (0,46 segundos)

Index of /uploads/docs - Marcos Bossolani
www.marcosbossolani.com.br/uploads/docs/
2014-05-30 15:04, 60K. comprovante-pagament..> 2014-05-30 15:04, 91K. comprovante-residenc..> 2014-05-30 15:04, 614K. rg-e-cpf.jpg, 2014-05-30 15:04 ...

Index of /site/assets/socios - Circuito EcoBike
www.circuitoecobikepe.esp.br/site/assets/socios/
... 00b37-1487336251639-1558283866.jpg · 029e5-img-20170313-wa0120.jpg · 02ee8-img-20170314-wa0019.jpg · 032ab-rg-e-cpf-emerson.jpg ...

Index of /images - misodor
www.misodor.com/images/
... 23:17, 322K. 028ec50885.jpg, 2010-08-12 00:40, 17K ... 08-01-17_money8.jpg, 2010-03-08 14:59, 13K ..... CPF E RG FRENTE.jpg, 2010-09-30 13:40, 625K.

Imagens de intitle:index.of "cpf" "rg" "jpg"

→ Mais imagens para intitle:index.of "cpf" "rg" "jpg" Denunciar imagens

Index of /wp-content/uploads/cache/formidable/rg-cpf
www.fluxexperiences.com.br/wp-content/uploads/cache/.../rg-cpf... ▾ Traduzir esta página
Index of /wp-content/uploads/cache/formidable/rg-cpf. Parent Directory · 3409230202.jpg. Apache/2.4.18 (Unix) mod_hive/6.6 OpenSSL/1.0.1e-fips ...

Index of /wp-content/uploads/profiles/5136 - CREAjr-SC
www.creajr-sc.org.br/wp-content/uploads/profiles/5136/
Index of /wp-content/uploads/profiles/5136. Parent Directory · RG-CPF-Camila.jpg.

Index of /imagens - Achar Pessoas

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.

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.
Oferecemos o pacote completo, com viral + dominio + host

Contratar agora »

Cybersecurity Incident & Important Consumer Information

We are currently experiencing difficulties with our TrustedID website. As a result, the site may be unavailable periodically, and we are working hard to help reduce interruptions.

We apologize for any inconvenience and appreciate your patience.

Recent Updates

WSJ Opinion: On Behalf of Equifax, I'm Sorry

September 28, 2017

On September 28, Interim CEO Paulino do Rogos Barros Jr., published an opinion piece in the Wall Street Journal. In it, he discusses moving the organization forward and earning back trust. Click the image below to read the opinion piece:

THE WALL STREET JOURNAL.
WebReprint

WSJ Opinion: On Behalf of Equifax, I'm Sorry

September 28, 2017

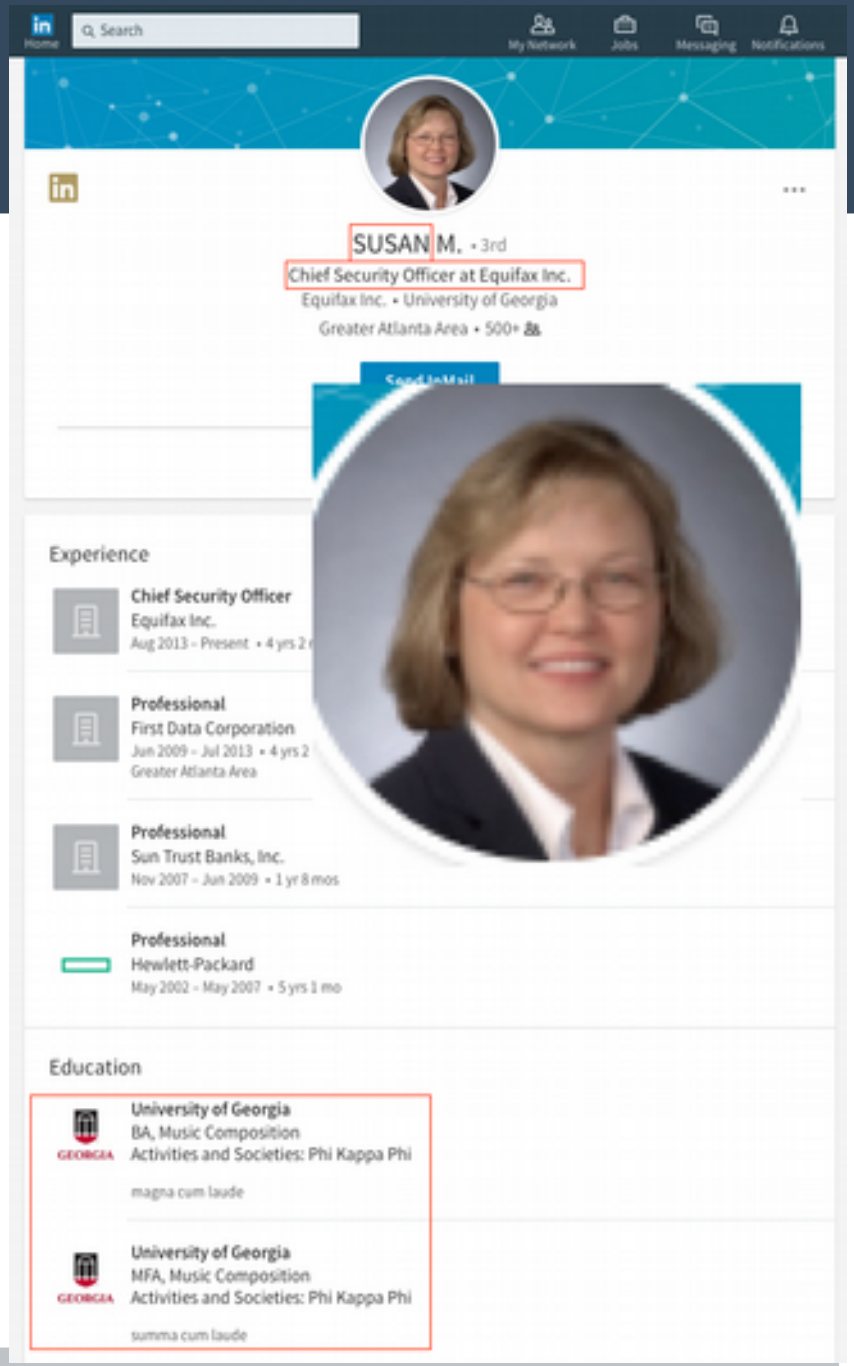
Equifax Chairman, CEO, Richard Smith Retires; Board of Directors Appoints Current Board Member Mark Feidler Chairman; Paulino do Rego Barros, Jr. Appointed Interim CEO; Company to Initiate CEO Search

September 26, 2017

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

September 15, 2017

Crimes Digitais



25 SEP 17

Source: Deloitte Breach Affected All Company Email, Admin Accounts

Deloitte, one of the world's "big four" accounting firms, has acknowledged a breach of its internal email systems, British news outlet *The Guardian* revealed today. Deloitte has sought to downplay the incident, saying it impacted "very few" clients. But according to a source close to the investigation, the breach dates back to at least the fall of 2016, and involves the compromise of all administrator accounts at the company as well as Deloitte's entire internal email system.

Seguro | https://pastebin.com/raw/ARN7yjSe

3389
tcp
rdp

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            17:02:6b:b1:d2:88:38:a2:4a:79:68:1a:99:7a:59:20
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Deloitte-AD-02.Deloitte.local
        Validity
            Not Before: May 18 10:35:01 2017 GMT
            Not After : Nov 17 10:35:01 2017 GMT
        Subject: CN=Deloitte-AD-02.Deloitte.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
```

date
nstall
hem.

Windows Server 2012 R2

ENG

P@$$word
//build forge

Indeed, it appears that Deloitte has known something was not right for some time. According to this source, the company sent out a "mandatory password reset" email on Oct. 13, 2016 to all Deloitte employees in the United States. The notice stated that employee passwords and personal identification numbers (PINs) needed to be changed by Oct. 17, 2016, and that employees who failed to do so would be unable to access email or other Deloitte applications. The message also included advice on how to pick complex passwords:

2016
GLOBAL SECURITY AWARENESS WEEK

Mandatory password reset
Action required today—don't get locked out!

Our firm is deeply committed to protecting our confidential information and that of our clients. To launch Global Security Awareness week and meet this shared commitment, please take 5 minutes to update your Deloitte password and pin.

Your password will expire on Monday, October 17.

If your password is not changed by then, you will not be able to access email or other Deloitte applications until it is reset.
To reset your password, connect to DeloitteNet VPN or from a Deloitte office.

Strong password guidelines

- ***Really* change your password.** Don't reuse or slightly change old passwords. Come up with something completely new.
- **Make your password longer.** Go for 10 characters, or even 12 or 16. Phrases can be helpful to remember and can combine numbers, letters, and characters to meet password guidelines.
  - The phrase: "to lock it is good" as a password: 2lockIT15:)

A screen shot of the mandatory password reset message Deloitte sent to all U.S. employees in Oct. 2016, around the time sources say the breach was first discovered.

Crimes Digitais

Europol: Ransomware top threat in 2017 cybercrime 'epidemic'

Toby Sterling

2 MIN READ

THE HAGUE (Reuters) - Ransomware eclipsed most other forms of cybercrime as on-line crime surged in 2017, European policing agency Europol said on Wednesday, citing high-profile attacks such as "WannaCry" that reached millions of computers.

Europol coordinated several successful cross-border operations against cybercriminals last year. But national authorities urgently need to devote more resources to targeting the developers of hacking tools, the agency's head said.

"The last year has been exceptional, given the size and the type and the range of the attacks that we've seen," Europol director Rob Wainwright said, detailing an annual review of Internet crime threats.

"Growing sophistication in the cybercrime community", where criminal groups band together to deliver "cybercrime services", is becoming the major engine of growth in online crime undertaken for illegal profit, he said.

Ransomware "has eclipsed most other cyber-threats. ..indiscriminately affecting victims across multiple industries in both the public and private sectors," the report said.

The 80-page report also named data breaches, darknet markets, extortion of youth for child pornography and payment fraud as growing threat areas.

Crimes Digitais

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

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

Summary of findings
"Nossos resultados nos levam a crer que informação incorreta foi fornecida no tribunal. Além disso, estamos preocupados quanto à possível falta de um exame forense aprofundado sobre as provas físicas, tanto pela defesa quanto pela acusação."

Forense Digital

Casos emblemáticos

- Invasão da RSA e Lockheed Martin
- Empresa varejista Target (US$ 148 milhões de prejuízo)
- Compra e venda de acessos a sites (governamentais)
- Vazamentos de dados do Ministério Público (?!?)
- Emails institucionais (Ashley Madison, DLH.net, mSpy, Pastebin, etc)
- Operação Darknet
- Dossier do Iraque => Colin Powell / Tony Blair

GeoHack (-15.817725; -47.867508)

WGS84	15° 49' 3.81" S, 47° 52' 3.03" W -15.817725, -47.867508		
UTM	23L 192814 8249130		
Zoom	8	Scale	± 1:10000
Region	BR	Type	
Title			

Contents Global and Local services · Wikipedia articles · Photos · Other · Report

Views
- Template
- Talk
- View source
- History

Languages
- Afrikaans
- Alemannisch
- العربية
- Aragonés
- Asturianu
- বাংলা
- Беларуская
- Беларуская (тарашкевіца)
- Brezhoneg
- Български
- Català
- Česky
- Dansk
- Deutsch
- Diné bizaad
- Dolnoserbski
- Eesti
- Ελληνικά
- Español
- Esperanto
- Euskara
- فارسی
- Føroyskt
- Français
- Frysk
- Galego
- ગુજરાતી
- 한국어
- Հայերեն
- Hornjoserbsce
- বিষ্ণুপ্রিয়া মণিপুরী
- Bahasa Indonesia
- Íslenska
- Italiano

*View this location in **Google Maps**, in **OpenStreetMap**, with **Dual view**, or select one of the services listed below:*

Global services

Service	Map	Satellite	Topo	Other
ACME Mapper	Map	Satellite	Topo	Terrain, Magnifier
Arctic.io				Daily Satellite
Ayna	Maps	Satellite		
Bing Maps Popular	Maps	Satellite		Bird's eye
Blue Marble Navigator		Satellite		
Flash Earth		Satellite		
Fourmilab		Satellite		
GeaBios		Satellite		
GeoNames		Satellite		Text (XML)
Google Earth note				w/ meta data

Brazil

Service	Map
MSN Maps Brazil	Map

View all regional services

Filename - P1000328.JPG
Make - Panasonic
Model - DMC-TZ7
DateTime - 2010:07:09 19:01:30
ExifOffset - 654
ExposureTime - 1/15 seconds
FNumber - 3.30
ExposureProgram - Normal program
ISOSpeedRatings - 1600
DateTimeOriginal - 2010:07:09 19:01:30
(...)
not fitted, compulsory flash
4.0 mm
FileSource - DSC - Digital still camera
SceneType - directly photographed image
ExposureMode - Auto
White Balance - Manual
atio - 3.0000 x
35 mm - 25 mm
c - Standard
on: -
- 2.2.0.0
ef - S
15 49 3.81 (15.817725)
eRef - W
- 47 52 3.03 (47.867508)
pa 21 58 50
p - 2010:07:09
Vendor): -
High
Focus Mode - Auto

Google -15.817725,-47.867508 Marcelo Caiado 0 + Comp.

Como chegar | Meus lugares

Sces Trecho 2, 2 - Brasília
DF, 70200-002, República Federativa do Brasil 40 m L

Rota Nesta área, pesquisar por Salvar em... mais

Labs do Google Maps - Ajuda
Google Maps - ©2012 Google - Termos de Uso - Privacidade

Satélite
Trânsito

Av. das Nações
Via L Quatro Sul
Sces Trecho 2
Sces Trecho 3
Safs
Ses
Pte Costa E Silva
Av. Costa E Silva
Embaixada Chile
Embaixada Uruguai
Embaixada Sérvia
Embaixada do Canadá
Tribunal Superior do Trabalho
TRIBUNAL DE JUSTIÇA
Safs Quadra 8
Mangai
Clube Naval de Brasília
AABB
Clube do Exército
AABB-Associação Atlética Banco do Brasil
Porto Vittoria Espaço de Eventos
ASCADE-Associação dos Servidores da Câmara dos Deputados
Associação Médica de Brasília
Churrascaria Porcão
Cinemark Pier 21
Pier 21 Cultura e Lazer Ltda-Administração
Restaurante Coco Bambu Frutos do Mar
Dom Francisco
Bierfass
Devassa do Pontão
Pontão do Lago Sul
500 pés
Dados cartográficos ©2012 Google, MapLink

Forense Digital

Oops! Did Vice Just Give Away John McAfee's Location With Photo Metadata?

BY MAT HONAN 12.03.12 5:02 PM

Follow @mat

Share 294 Tweet 196 +1 22 Share 13

John McAfee, the millionaire software executive turned semi-fugitive, was falsely reported captured over the weekend. Now, in a new post on his blog, he claims that he's left Belize for another country in the company of two Vice journalists and his longtime female companion, Sam. He also noted that Vice would be publishing a story today that would end all the speculation as to whether or not he is a "drug-crazed madman."

In fact, Vice did publish a story today, titled "We Are With John McAfee Right Now, Suckers," complete with a photo of McAfee and Vice editor-in-chief Rocco Castoro taken with an iPhone 4S. And location information embedded in the photo indicates the foursome is in Guatemala, specifically along the Rio Dulce in the Parque Nacional Rio Dulce. Near the Ranchon Mary restaurant. By a swimming pool.

Presumivelmente, quem tirou a foto em seu iPhone 4S tinha esquecido de desligar os serviços de localização ..

```
exif:GPSImgDirection: 54424/255
exif:GPSImgDirectionRef: T
exif:GPSLatitude: 15,39.49N
exif:GPSLongitude: 88,59.53W
exif:GPSTimeStamp: 2012-12-03T18:25:26Z
```

Essas coordenadas sugerem que John McAfee foi fotografada na Guatemala, depois de ter atravessado a fronteira de Belize.

Eu não sei o que - se houver - envolvimento de John McAfee teve com a morte de seu vizinho Gregory Faull, e nós temos que assumir que ele é inocente, a menos que se prove a culpa de um crime.

Mas seria realmente irônico se John McAfee, um homem que foi um dos líderes na indústria de anti-vírus 20-25 anos atrás, foi desfeito pela segurança de TI desleixado. A lição que todos nós devemos aprender é ter

Fontes: http://www.wired.com/gadgetlab/2012/12/oops-did-vice-just-give-away-john-mcafees-location-with-this-photo/ e http://nakedsecurity.sophos.com/pt/2012/12/03/john-mcafee-location-exif/

Forense Digital

A perícia de TIC do MPF atua investigando as violações aos direitos humanos identificadas na internet, além de fraudes bancárias

As principais violações atualmente envolvem:

- apologia, incitação ou crime de ódio (racismo e xenofobia)
- pornografia infantil e juvenil
- crimes contra o sentimento religioso
- incitação ao genocídio

Forense Digital

Além disso, a perícia de TIC do MPF atua na elaboração de Laudos e Relatórios Técnicos, que podem estar relacionados a questões cíveis, do consumidor, de corrupção:

- Suposto uso indevido de verba pública na implementação de WiFi gratuito
- Licitação de equipamentos de órgão público
- Contratação de software por empresa pública
- Velocidade de acesso à Internet e sinal de telefonia celular
- Acessibilidade digital
- etc

LEI Nº 13.441, DE 8 DE MAIO DE 2017.

Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º O Capítulo III do Título VI da Parte Especial da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), passa a vigorar acrescido da seguinte Seção V-A:

"Seção V-A

Da Infiltração de Agentes de Polícia para a Investigação de Crimes contra a Dignidade Sexual de Criança e de Adolescente"

"Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras:

I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público;

II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas;

III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.

§ 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo.

§ 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se:

I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão;

II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.

§ 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios."

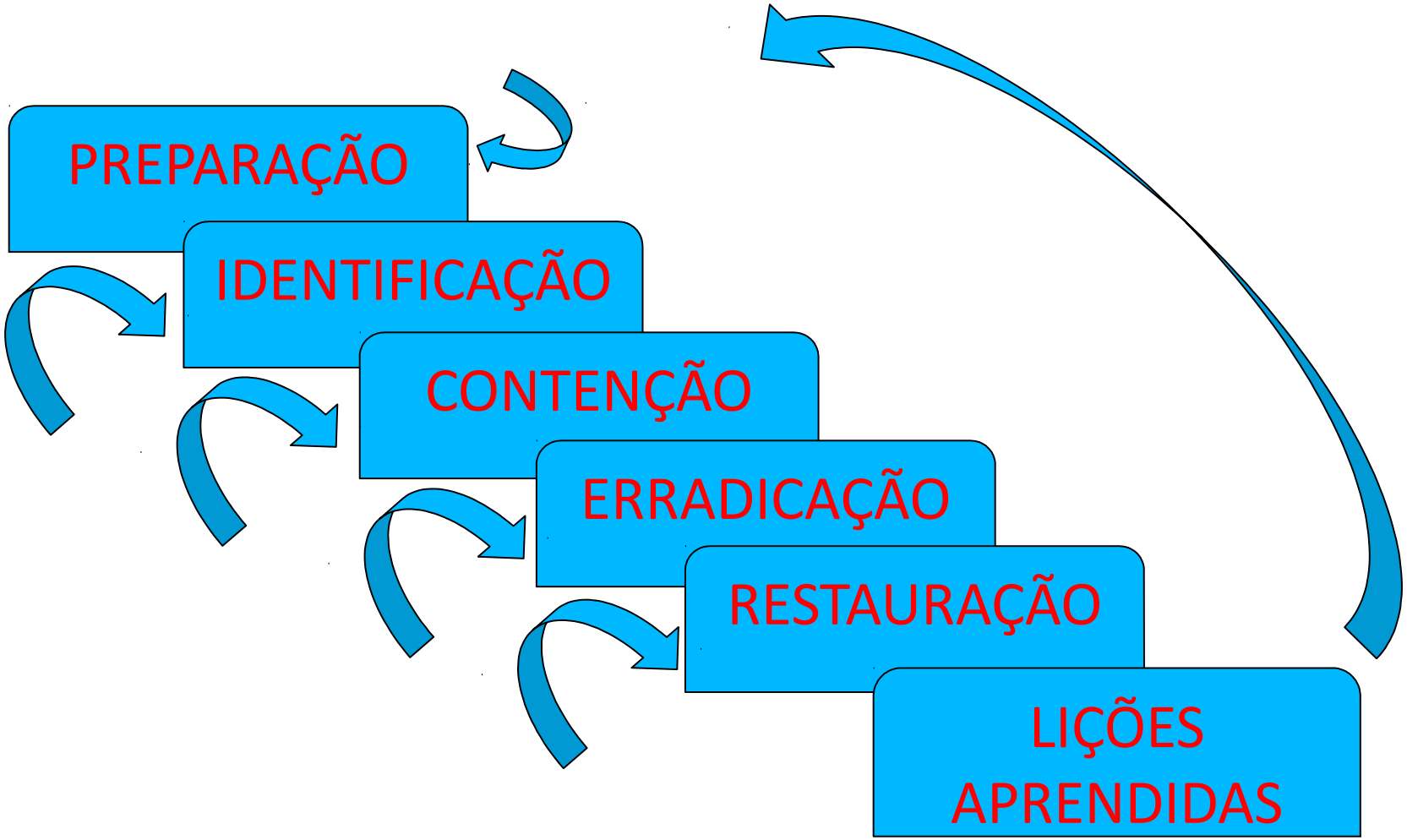
"Art. 190-B. As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo.

Parágrafo único. Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações."

"Art. 190-C. Não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

Segurança da Informação

DFIR – Digital Forensics & Incident Response



Fonte: SANS Institute

DIGITAL EVIDENCE COLLECTION → ADMINISTRATIVE → WORK PLAN → CASE SETUP → IMAGE INTEGRITY → ANALYSIS PREP → ANALYSIS → INTERPRETATION- REVIEW → REPORTING

1. ADMINISTRATIVE STUFF

- Review Policies and Laws
- Chain of Custody form
- Digital Evidence Collection Form
- Consent form (if needed)
- ✓ Evidence Tracked and Stored

2. WORK PLAN (docs)

- Review Policies and Laws (if needed)
- Gain understanding of:
  - -Background
  - -If applicable, previous work
  - - Requirements/Goal of analysis
  - - Deliverable
- Create Analysis Work Plan
- Create Investigative Plan

3. SETUP CASE FOLDER (example)

- EV1 (Evidence Files)
- WC (Working Copy of Files)
  - Case # - Project Name
    - Custodian Name
      - Media Type – EV #
        - Case File
        - Index
        - Reg Files
        - Internet Hist
        - Case Processor
        - Logs

        (Analysis Folders)
      - Media Type – EV #
      - Media Type – EV #

*Organize output neatly!

4. CONFIRM IMAGE INTEGRITY

- ✓ Compare Acquisition and Verification Hash values (MD5, SHA)
- Save Verification Reports

5. BEFORE YOU GET STARTED..

- ✓ Check physical size of drive and compare to physical label accounting for all drive space (Check for DCA/ HPA).
- ✓ Identify & compare logical partition size(s) to physical drive size to identify any deleted partitions or unused disk space
- ✓ Retrieve time zone settings for each disk and apply correct time zone, if applicable
- ✓ Rename hard disk volumes as necessary to "Recovery", "C", etc.

GATHER SYSTEM INFORMATION

- ✓ Determine OS, service pack, OS install date, application list, owner, machine name, and other basic information.
- ✓ Retrieve user profile information (names, SIDs, create and last logon dates)

PRE-PROCESSING ANALYTICS

- ✓ Conduct hash analysis, indentify "known" and/or "notable" files.
- ✓ Conduct file signature analysis, review renamed files.
- ✓ Identify encrypted files (entropy)
- ✓ Mount ALL compound files (VHD, VMDK, ZIP,RAR, Email containers, Reg Files, etc
- ✓ Index Case (DT Search, WDS, Encase, AD..)
- ✓ Generate metadata (and extended) listings/ reports

RP / VSC

- ✓ Identify if services turned on/used
- ✓ Extract or make available accordingly for analysis

MOUNTING / VIRTUAL EMULATE

- ✓ Mount - Malware/Virus Scan (Don't forget about MBR)
- ✓ Mount - Stego Scan
- ✓ Virtually Emulate – conduct behavior and live analysis

KEYWORD SEARCHING

- ✓ Create keyword list & QC syntax formatting/code page usage (may be iterative process)
- ✓ Perform targeted or full disk search including unallocated and slack areas.
- ✓ Create hit report/stats

FILTERING

- ✓ Filter data based on meta data and exteneded meta data such as Date and Time values, File Extension, and etc.

EXPORT

Export files from case for independent analysis with specialty tools. For example:

Memory
Memorize
Redline
Volatility (SIFT)
Passwords
AD PRTK
Passware
Ophcrack
Shellbags
Shellbags.py (SIFT)
Internet History
WebHistorian
LNK Files
Tzworks
Lslnk (SIFT)
Event Logs (.evt & .evtx)
Tzworks
GrokEVT
MFT
AnalyzeMFT
Ntfswalk (SIFT)
index/$I30
INDXParse.py (SIFT)
SIFT Workstation is a great resource for tons of tools!

Email
NUIX
Clearwell
Recover My Email
Bulk extractor (SIFT)
Image Mounting
FTK Imager
ImDisk
Live View
OSFMount
Virtual Box
Stego
Outguess
Hashing
Md5deep (SIFT)
Sha256deep (SIFT)
Hashdeep (SIFT)
Registry
Reg Ripper (SIFT)
Registry Decoder
AD Registry Viewer
Reglookup (SIFT)
YARU (SIFT)
Windows Journal Parser
Tzworks

6. EQUATION FOR SUCCESSFUL ANALYSIS: (TIMELINES + MANUAL ANALYSIS) x (PASSION + TIME + RESEARCH + RESOURCES) = "WINNING"

GENERAL AREAS

Analyze general folder locations for artifacts or data of interest. For example:
>Desktop
>User folders
>Documents
>Desktop
>Network Shortcuts
>Recently Opened File folders
>System Temp folders
>Browser Temp Folders
>System Folders (malware)
>Autorun

TIE IT ALL TOGETHER USING TIMELINE ANALYSIS – FLIP SIDE!

REGISTRY ANALYSIS (Win only)

The System registry hives (NTUSER.DAT, SYSTEM, SOFTWARE, SECURITY, SAM..) contain a vast of amount of information that can be imperative to your analysis. For Example:
-OS Version (SOFTWARE)
-Last logged on user (SAM)
-Last Failed Logon (SAM)
-Username & SID (SAM)
-Shutdown (SYSTEM)
-TimeZone (SYSTEM)
-Drives Mounted by User (NTUSER.DAT)
-File Ext Associations (NTUSER.DAT)
-Installed application list (SOFTWARE)
-Search History (SOFTWARE)
-Removable Storage Devices (SYSTEM)
Using Registry analysis tools, such as Reg Ripper, can aid your analysis..

SYSTEM ARTIFACTS

There are many system related artificacts that may contain potentially relevant information including:
-Backups (RP, VSC, others)
-Event Logs (.evt, evtx)
-Shell bags (Registry)
-Jump Lists
-Misc. Logs (firewall, AV, Apps, etc)
-Removable Media Connections
-LNK files
-Prefetch
-PageFile

SOFTWARE RESIDUE

Identify software (i.e Wiping tools, P2P, Sticky Notes, hacker tools, etc) and perform analysis on associated files (binary-malware analysis), logs, settings, registry and etc.

MEMORY RESIDUE

If applicable, perform memory analysis to gather volatile information including:
-Handles; files, directories, processes, registry keys, Semaphores, events and sections
-Open network ports
-Hooks: Driver IRP, SSDT and IDT driver tree

E-MAIL/IM/SOCIAL ARTIFACTS

Identify email clients or web access on system and perform analysis on associated data stores or application residue/settings:
Client based (file examples):
Windows - .OST, .PST, .MSG, Temp folder for Outlook attachments, Lotus Notes - .NSF, Mac - .EML, .EMLX, .MBOX
Web based (OWA, Facebook, Twitter, etc.):
-Logs -Internet History reconstruction -Cache

INTERNET

Identify installed browsers and perform analysis on artifact such as:
-Parse Internet history files (index.dat, sqlite, etc)
-Check temp folders
-Parse cookies
-Cached pages
-Form History/Auto complete files
-Favorites/bookmarks
-Toolbars
-WebSlices
-Browser plug ins
-Registry analysis
-Carve unallocated for deleted history artifacts

...BUCKETING ANALYSIS "TO DO" ITEMS LIKE THIS CAN HELP.

7. INTERPRETATION/REVIEW OF ARTIFACTS (examples) ..

- File Download: Open/Save MRU → Open/Run MRU → Email → Skype History → Index.dat / places.sqlite → downloads.sqlite → P2P Logs
- File Opening/ Creation: MACB → MRU by ext → MS Office MRU → LNK Files → Index.dat file:// → JumpLists → Shellbags → Prefetch
- File Knowledge: XP Search ACMRU → Win7 Search WordWheelQuery → Thumbs.db → Win7 Thumbnails → Recycle Bin → Browser Artifacts → Last visited MRU
- USB Usage: Identification → First & Last Insert Times → User Identification → Volume Name → Drive Letter → LNK Files → Event Logs → Mount Point
- Program Execution: User Assist → LastVisited MRU → Run MRU (Start->Run) → Prefetch → MUI Cache → Jump Lists → Event Logs
- Physical Location: Time Zone → Wireless SSID → Vista/W7 Network History → Cookies → Search Terms → IP → Image exif
- Account Usage: Last Password Change → Group Membership → Success/Fail Logons → Logon Types → RDP Usage → Account Logon/ Authentication → SID Attributes
- Browser Usage: History → Search Box Terms → Cache → Session Restore → Flash & Super Cookies → Suggested Sites → Memory Fragments of Private Browsing → AJAX Transactions → Typed URLS

Have more? Let me know!

8.REPORTNG

- ✓ Document findings comprehensively
- ✓ Fact based Interpretation
- ✓ Remember who the audience is
- ✓ Remember requirements/expectations

GENERAL FORENSIC ANALYSIS CHECKLIST V.1.1

THE PURPOSE OF THIS REFERENCE GUIDE IS TO PROVIDE AN OVERVIEW AND OUTLINE OF COMMON PROCESSES, SOFTWARE, AND BEST PRACTICES FOLLOWED BY PROFESSIONALS CONDUCTING COMPUTER FORENSIC ANALYSIS

BY DAVID NIDES (12/16/2011)
TWITTER: @DAVNADS
BLOG: DAVNADS.BLOGSPOT.COM
EMAIL: DNIDES@KPMG.COM

CREDITS TO: ED GOINGS, ROB LEE & SANS

QUESTIONS/FEEDBACK–CONTACT US!

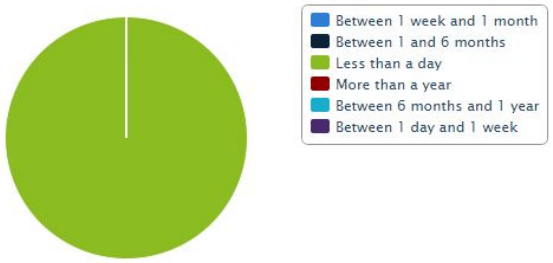
SANS COMPUTER FORENSICS and INCIDENT RESPONSE

DFIR – Digital Forensics & Incident Response

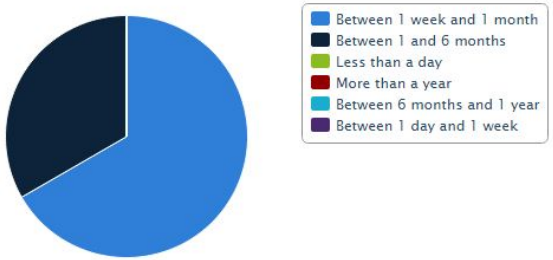
Open Incidents by Phase

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

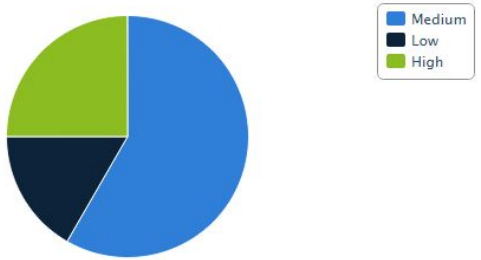
Closed Incidents by Duration Last 30 Days (Aug 13, 2014 - Sep 12, 2014)



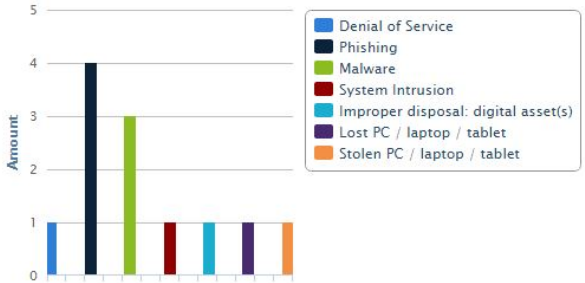
Open Incidents by Duration



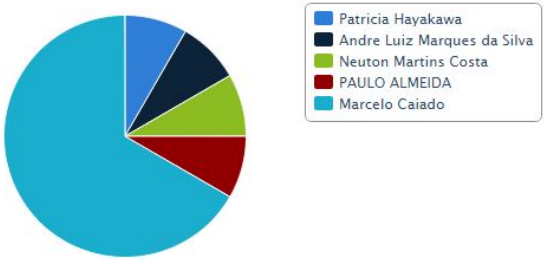
Open Incidents by Severity



Open Incidents by Type



Open Incidents by Owner



DFIR – Digital Forensics & Incident Response

- ✓Saiba onde sua informação está, e quem pode acessá-la
- ✓Compartilhe conhecimento com órgãos públicos e seus competidores (que passam pelos mesmos problemas)
- ✓Monitore a segurança de sua rede e aplicações
- ✓Cuide da segurança ambiental, física e de pessoal
- ✓Implemente autenticação multifator
- ✓Gerencie a aplicação de patches

DFIR – Digital Forensics & Incident Response

- ✓Maior integração das áreas de suporte técnico, SOC, NOC e DFIR (e Jurídico e RH)
- ✓Investimentos em certificações correlatas
- ✓Adequação das ferramentas forenses
- ✓Possua um time ou equipe de Resposta a Incidentes (treinado e equipado)
- ✓Observe a “Teoria do pato”
- ✓Proporcione canais fáceis de notificação de incidentes (RFC 2142 => Mailbox Names)

DFIR – Digital Forensics & Incident Response

- Internet das Coisas (IoT) => incremento do MMO (Motivação, Meio e Oportunidade)
- Legislação específica e cooperação internacional
- Maior preocupação com privacidade de dados
- Mantenha sua segurança compatível com a tecnologia atual
- Enfatize a importância de boas práticas para desenvolvimento de código seguro

Segurança da Informação

À Divisão de Segurança da Informação compete:

I - administrar e manter atualizados os recursos de segurança da informação (...)

II - zelar pelo bom funcionamento dos recursos de segurança das redes metropolitanas (...)

III - atuar no tratamento e na resposta a incidentes de segurança de redes de computadores;

IV - acompanhar e realizar testes de vulnerabilidade nos ambientes operacionais do Ministério Público Federal;

PORTARIA SG/MPF Nº 382, DE 5 DE MAIO DE 2015

Segurança da Informação

À Divisão de Segurança da Informação compete: (cont.)

V - estimular as demais áreas de tecnologia da informação do Ministério Público Federal a manter os equipamentos e serviços sob sua responsabilidade atualizados e livres de vulnerabilidades conhecidas;

VI - promover a cultura da segurança da informação entre a equipe técnica e os usuários de recursos de tecnologia da informação;

VII - zelar pelo cumprimento das políticas e normas institucionais relativas à segurança da informação; e

VIII - assistir às áreas do Ministério Público Federal nas análises de dispositivos computacionais utilizados em incidentes relacionados a segurança da informação.

PORTARIA SG/MPF Nº 382, DE 5 DE MAIO DE 2015

Segurança da Informação

Os 10 Mandamentos

- ✓Participarás junto com sua equipe em atividades de prospecção de tecnologias;
- ✓Implementarás demandas de segurança com requisitos de conformidade, privacidade e corporativos;
- ✓Monitorarás todos seus ativos de segurança, como NGFW, IDS/IPS, SIEM, DLP, antivírus, etc;
- ✓Estarás atento aos desafios diários como sites maliciosos, vulnerabilidades, zero days, espionagem, crime organizado, funcionários insatisfeitos, script kiddies, hacktivistas, etc;

Segurança da Informação

Os 10 Mandamentos

- ✓Trabalharás ativamente para que a cultura seja da resposta a incidentes, e não da resposta após incidentes;
- ✓Engajarás a alta administração;
- ✓Indicarás as tecnologias de segurança adequadas e aplicarás os devidos processos;
- ✓Não descuidarás da capacitação de sua equipe;
- ✓Protegerás seus ambientes físico, móvel e virtual;
- ✓Atuarás sempre de forma ética.

“Sed quis custodiet ipsos custodes?”

Decimus Iunius Iuvenalis (Juvenal)

"Mas quem guardará os guardiões?"

Segurança da Informação

Cânones do Código de Ética do (ISC)[2]

- ✓Proteger a sociedade, o bem comum, necessária confiança mútua e confiança do público, e a infra-estrutura.
- ✓Agir honradamente, honestamente, de forma justa, com responsabilidade e dentro da lei.
- ✓Fornecer serviço diligente e competente para a alta administração.
- ✓Avançar e proteger a profissão.

Confira dicas para cuidar da sua estação de trabalho

Publicado em: 26/04/2016

Na segunda matéria sobre segurança da informação, você entende como pequenas mudanças de hábitos pessoais e funcionais podem contribuir para a implantação de uma nova cultura relacionada à segurança da informação e comunicação no âmbito do MPF

Foto: Istockphotos.

Talvez você não saiba, mas apenas em março, a área de tecnologia do MPF bloqueou em média 42 mil tentativas de ataques diários à rede da instituição, tais como investidas para obter acesso de administrador. A Secretaria de Tecnologia da Informação e da Comunicação (STIC) trabalha para garantir a segurança da informação, mas é fundamental que todos estejam atentos para que as informações não sejam alteradas sem autorização ou que pessoas mal-intencionadas tenham acesso a dados ou informações da instituição.

"Todo servidor público tem um compromisso com a integridade, a confidencialidade, a autenticidade e a disponibilidade da informação institucional, a partir da adoção de condutas pessoais e procedimentos padrões de segurança. É uma questão de conscientização, destaca do secretário da STIC, Mauro Sobrinho.

O coordenador de Atendimento e Relacionamento da STIC, Guilherme Freitas, lembra que é comum as pessoas se preocuparem com a segurança da casa, da carteira, do carro e do celular, mas têm a falsa sensação de que estão seguros no ambiente online, especialmente o corporativo. "Por vezes o usuário supõe que ninguém tem interesse em utilizar o seu computador ou que, entre tantos computadores conectados, o seu dificilmente será atacado", destaca. Por isso, o coordenador reitera a importância de possuir uma senha forte, estar atento aos sites visitados e de realizar backups dos documentos importantes instalados nas máquinas.

Também é preciso ter atenção ao uso do "Drive T", utilizado para compartilhamento de arquivos na rede. "O ideal é que não seja utilizado como repositório, nem para o compartilhamento de informações sensíveis e de arquivos pessoais". Guilherme alerta que, basta uma busca rápida na rede para encontrar músicas e fotos pessoais. "O usuário nem sempre tem a dimensão de que esse arquivo pessoal pode ser aberto e visto por qualquer pessoa e que músicas e filmes podem ser protegidos por direitos autorais e não deveriam ser utilizados no ambiente corporativo", finaliza.

Plano de Segurança- Segundo o Plano de Segurança Institucional, os procedimentos e as operações realizados por intermédio das estações de trabalho conectadas à rede são sempre de responsabilidade dos usuários que nelas estiverem autenticados.

Também segundo o texto, não é permitida a instalação e/ou execução de qualquer outro programa ou

Saiba como utilizar redes wi-fi com segurança

Publicado em: 02/05/2016

No terceiro texto da série sobre segurança da informação, conheça os riscos em acessar sistemas e ferramentas do MPF fora da rede institucional

Foto: Istockphotos.

Na última matéria da série sobre segurança da informação, a Secretaria Tecnologia da Informação e Comunicação (STIC) deu dicas sobre como garantir a segurança da sua estação de trabalho. Mas quais são os riscos em acessar sistemas e ferramentas do MPF fora da rede institucional, a exemplo de viagens?

"O MPF, nos últimos anos, avançou significativamente no sentido de desenvolver ferramentas e sistemas que possam ser acessados pelos usuários onde quer que eles estejam. O Único é um excelente exemplo. Os gerenciadores se adaptam aos diferentes tamanhos de telas ou de resolução, o que torna possível acessá-lo independentemente dos dispositivos. Mas esse tipo de acesso requer cuidados", lembra o secretário de Tecnologia da Informação e Comunicação, Mauro Sobrinho.

Uma importante dica é ter atenção ao conectar seu dispositivo a uma wi-fi pública utilizando a senha de rede do MPF. "Quem chega a um bar, a um restaurante ou a um estabelecimento e se conecta à rede wi-fi do local? Todo mundo! As pessoas nem sempre param para pensar se aquela wi-fi realmente é segura", alerta coordenador de Atendimento e Relacionamento da STIC, Guilherme Freitas.

O chefe da Divisão de Segurança da Informação, Marcelo Calado, destaca que um dos principais problemas ao acessar uma rede insegura é a interceptação de dados. "Cibercriminosos costumam aproveitar falhas de segurança para bisbilhotar as atividades online dos usuários. E é importante notar que interceptação de dados nem requer muito conhecimento de computação", pontua.

Por isso, configurar a rede wi-fi da forma adequada é um dos meios de assegurar a segurança do seu dispositivo. Segundo Marcelo, além da necessidade de senha, o usuário deve informar ao sistema operacional que a conexão é pública e que não deseja compartilhar arquivos com outras pessoas. O usuário deve, ainda, atentar-se sobre as informações que possuem em seus dispositivos, como fotos íntimas e informações institucionais, e ter em mente o que pode acontecer se essas informações caírem em mãos erradas.

"Precisamos entender que a responsabilidade com as informações da instituição extrapola os limites do local de trabalho e que somos responsáveis por esse cuidado. Se houver a subtração e o vazamento de uma informação sensível do MPF, quem paga por isso? Quanto custa para a imagem da instituição?" provoca Marcelo.

Senha forte - O uso de credenciais do usuário e a utilização de senha são condições indispensáveis

Segurança da Informação

Segurança da Informação

Experiência internacional

Experiência internacional

SANS FOR508 Mentor Brasília – Outubro de 2017

14 de julho de 2017 Análise, Aquisição, Browser, Cookies, E-mail, Hacking, Imagens, Imagens forenses, Incident Response, Log, Metadados, Resposta a incidentes, SANS, USB Crimes Cibernéticos, DFIR, Perícia Digital, Threat Hunting

Estão abertas as inscrições para o curso SANS FOR508 Mentor – Advanced Digital Forensics, Incident Response, and Threat Hunting, a ser realizado em Brasília nos dias 18, 19, 20 e 21 de outubro de 2017 (4 dias, formato mentor, em 20 horas).
Este é um curso avançado de resposta a incidentes e threat hunting, fornecendo aos responders e às equipes de threat hunting habilidades avançadas para caçar, identificar, contornar e recuperar de uma ampla gama de ameaças nas redes corporativas, incluindo APTs de adversários nação-estado, sindicatos do crime organizado, e hacktivismo.

Constantemente atualizado, o FOR508 Resposta a Incidentes Avançados e Threat Hunting aborda os incidentes de hoje, fornecendo respostas a incidentes práticas, além de táticas e técnicas de threat hunting que os responders e os hunters de elite estão usando com sucesso para detectar, contornar e responder a casos de violação do mundo real. É um curso

BlackBerry
3:27
vr-zone.com
alt
option
command
command
alt
option

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US $3 TRILLION TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

7½ MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *2014 Internet Security Threat Report, Volume 19*, Symantec, April 2014; **2.** *M-Trends 2014: Attack the Security Gap*, Mandiant, April 2014; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *An Executive's Guide to 2013 Data Breach Trends*, Risk Based Security/Open Security Foundation, February 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2014; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*, Cisco, January 2014;

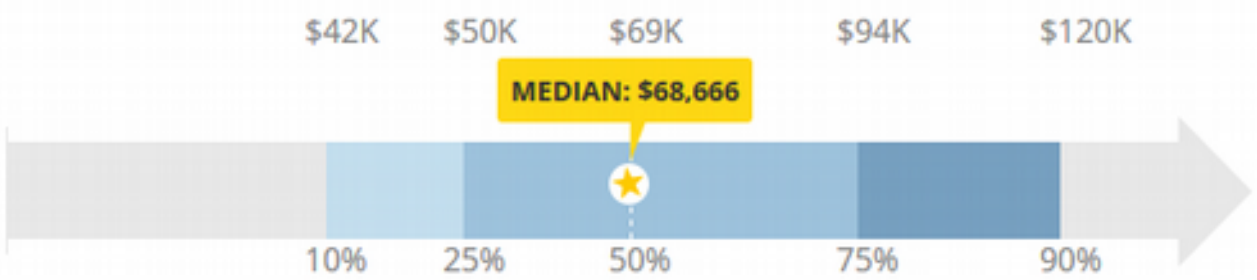
CSX CYBERSECURITY NEXUS

ISACA Trust in, and value from, information systems

Experi

Forensic Computer Analyst Salary (United States)

A Forensic Computer Analyst earns an average salary of $68,667 per year. A skill in Computer Security is associated with high pay for this job. Experience has a moderate effect on income for this job. Most people with this job move on to other positions after 20 years in this career.



Add this chart to your site: 640px 300px

Show Hourly Rate

+ experience + skill job

National Salary Data (?)	$0 $50K $100K $150K
Salary	$41,703 - $115,992
Bonus	$1,231 - $24,658
Total Pay (?)	**$40,895 - $119,492**

Country: United States | Currency: USD | Updated: 28 Oct 2016 | Individuals Reporting: 232

© Payscale, Inc. @ www.payscale.com

National Hourly Rate Data (?)	$0 $25 $50 $75
Hourly Rate	**$16.00 - $52.15**
Overtime	$34.01 - $73.97

National Annualized Data (?) $0 $50K $100K $150K

12
1
TIMEX
2
3
4
QUARTZ
5

S.i.Systems

Dear Marcelo,

I hope you had a great weekend! I am reaching out regarding a 1 year Bilingual IT Security Analyst contract starting September 18th.

This contract can be worked from either Montreal or Ottawa. Below is the job description for your reference, if you are interested please g respond to this email with your resume attached.

Our valued client in the private sector is seeking an Intermediate/Senior Security Analyst for an initial 1 year contract in either Ottawa or Montreal, with a possibility of extension. The security specialist must work within and have an appreciation for the clients security operating environments.

The specific focus of the position requires knowledge for the management of all operational applications, processes and technological capabilities required to support the managed security deliverables within all secure operating centers. The incumbent is required to understand each of the managed customer contracted requirements as it relates to operational performance and deliverables, the respective internal infrastructure and inter-networking relationships as well as the required security operating practices as defined by the contracts.

Responsibilities Include:

- Manage the daily customer requests for changes to their security infrastructure.
- Prepare changes for security devices such as firewalls, intrusion detection and prevention systems, identity access management etc.
- Participate in new customer integration projects and services and prepare implementations.
- Reviews and interprets security alerts and provide diagnostics in the management of incidents to support clients.
- Depending on the nature of the security threat, assess and develop mitigation measures to ensure that appropriate treatment is applied, and ensure that customers are informed.
- Take proactive measures to manage all perimeter security equipment or associated components which may be interrupted or affected as a result of threats or vulnerabilities.
- Configure, install, manage and maintain security devices and provide general information and recommendations on security best practices.
- Develop documentation associated with maintenance releases and keep them updated.
- Observe security management best practices.

Must Have Skills:

- Completion of University or College program in Computer Science; or 5 years of equivalent industry experience in the information systems field.
- Demonstrated experience designing, implementing, and troubleshooting security solutions including authentication, authorization, encryption and audit capabilities as part of an overall system design.
- Thorough knowledge of devices and network security infrastructure (hands-on).
- Practical experience recognized in the implementation, daily management and troubleshooting firewalls from multiple vendors.
- Proven experience in the daily management and troubleshooting of intrusion detection and prevention systems (IPS).
- Experience in troubleshooting security solutions including authentication capabilities, authorization, and encryption as well as securing devices access.
- Experience translating complex and ambiguous problems into actionable components. Ability to work on multiple clients and multiple technologies.
- Be able to work under pressure (required during incidents). Good communication skills, writing and presentations.Self starter with excellent organization and interpersonal skills.
- Excellent communication skills in both English and French (written and spoken).

Nice to Have Skills:

- Hands-on security certifications from major vendors
- Experience working with the following security management consoles of Checkpoint, Juniper, Cisco, Tufin, Fortinet, Mc Afee, Arcsight etc.
- Knowledge of offensive and defensive security operational tactics.
- Understanding of NIST, ISO 27001, ITIL, SAS70 (or 5970) and/or other compliance frameworks.
- Knowledge of security information events management (SIEM).

Para refletir...

“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

Links Úteis

- DFIR - http://dfir.com.br
- HTCIA Brazil - http://www.facebook.com/HTCIABrazil
- CERT.br - http://www.cert.br/docs/whitepapers/notificacoes
- SANS Institute Blogs - http://www.sans.org/security-resources/blogs