

Segurança da Informação e Forense Digital: Uma abordagem holística

Marcelo Caiado, M.Sc., CISSP, GCFA, EnCE, GCIH
Chefe da Divisão de Segurança da Informação
Procuradoria Geral da República
marcelobc@mpf.mp.br



Disclosure

**Todas as opiniões aqui apresentadas
são exclusivas do palestrante, apenas
de caráter ilustrativo e não possuem
nenhum vínculo o MPF**



“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”

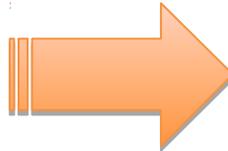
Thomas Welch



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



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.





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

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

Permalink.

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

from the *because-that's-how-this-works* dept

Over a decade ago, I pointed out that every single time there were a major data breach, a few weeks after the initial report, we would find out that the breach was much worse than originally reported. That maxim has held true over and over and over and over and over and over. Last week, we noted that the US government's Office of Personnel Management had been hacked, likely by Chinese hackers. And, now, it has come out that the hack was much worse than originally reported.

The President of the union that represents federal government workers, the American Federation of Government Employees (AFGE) sent a letter to the director of the FBI, saying that the hackers got away with the Central Personnel Data File, which included information about everything about that employee -- including (get this) unencrypted Social Security numbers.

Based on the sketchy information OPM has provided, we believe that the Central Personnel Data File was the targeted database, and that the possession of all personnel data for every federal employee, including up to one million former federal employees. We believe that the affected person's Social Security number(s), military records and other identifying information, address, birth date, job and pay history, health insurance, and pension information; age, gender, race, union membership, and other identifying information.

Oh, and then there's this:

Worst, we believe that Social Security numbers were not encrypted, a major cybersecurity failure that is absolutely indefensible and outrageous.

The letter further points out -- as we did last week -- that the 18 million federal government employees that the government has offered everyone is a complete joke. It's unlikely that anyone would do identity fraud for financial gain -- and quite likely this is for espionage.

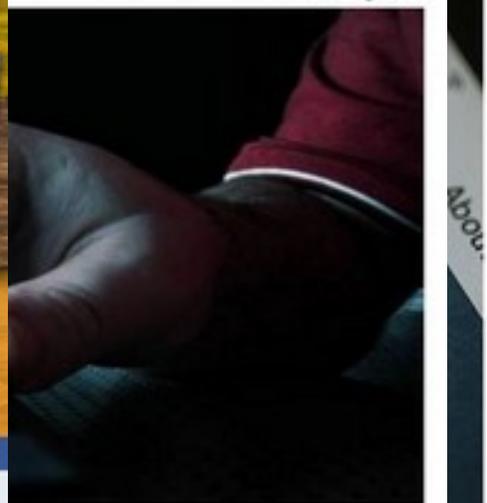
But, let's go back to the Social Security numbers being unencrypted. The fact that the Social Security numbers being unencrypted is already being used by intelligence system defenders to argue for "cybersecurity" laws that will give the NSA and FBI much greater access to our data.

And, yes, this would be the very same FBI that has actively argued that encryption is bad. The NSA has always hated encryption and insists it needs backdoors into our data.

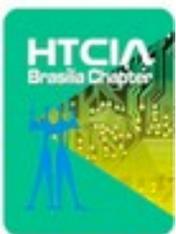
Both of these organizations strongly support "cybersecurity" legislation, claiming that it's necessary to protect our data. The NSA has always argued that encryption is bad, and the FBI has always argued that encryption is bad.

10 WhatsApp usa McDonald's dados

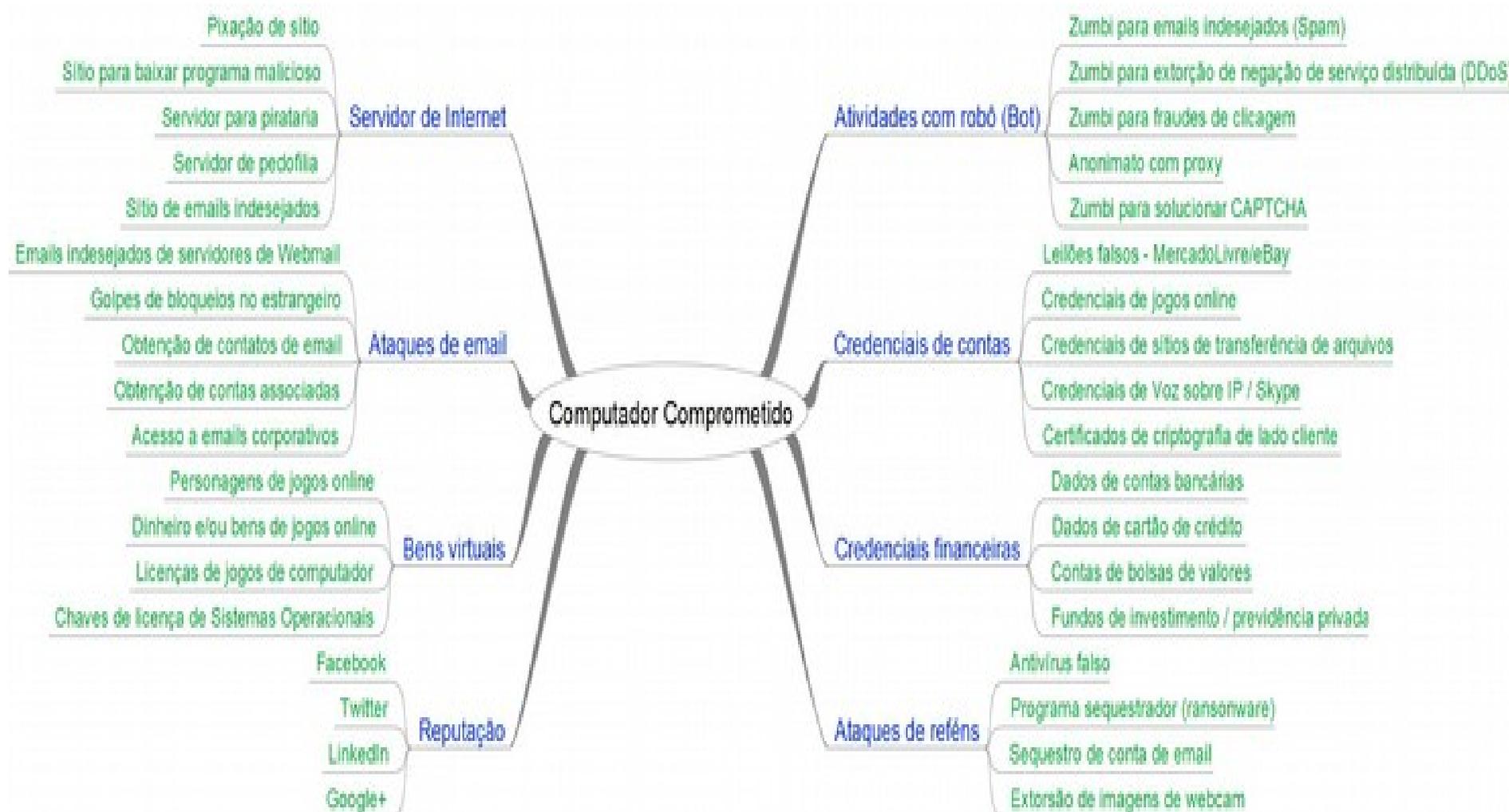
luz usando um
27.181 views
Salvar notícia



mente destrutivo
blecaute que atingiu metade da cidade
3 de dezembro.
o colocado em três centros de
centenas de milhares de pessoas sem
ight Partners afirmaram que
que causou o blecaute na Ucrânia.
ues com eventos destrutivos no setor
a - empresas de óleo, por exemplo -, mas nunca tínhamos visto um
ue tenha causado um blecaute", afirmou John Hulquist, chefe de
inteligência de ciberespionagem na iSight, em entrevista ao Ars Technica.



Crimes Digitais





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

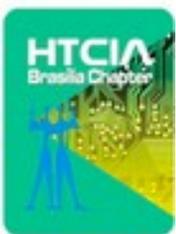


Forense Digital



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

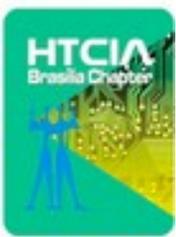
- Casos emblemáticos
 - Procurador “ameaçado de morte”
 - Empresa varejista Target (US\$ 148 milhões de prejuízo)
 - Compra e venda de acessos a sites (governamentais)
 - Vazamentos de dados do Ministério Público (?!?)
 - Emails institucionais (Ashley Madison, DLH.net, mSpy, Pastebin, etc)
 - Dossier do Iraque
 - Colin Powell / Tony Blair



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.





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 detectado, 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.

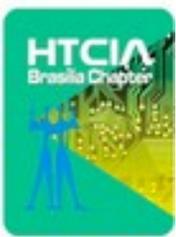
O OPM não tinha comentários adicionais a fazer imediatamente sobre o assunto nesta terça-feira, ou sobre seu esperado cronograma de notificações.

Autoridades culpam a China pelo vazamento do OPM.



Resposta a Incidentes





Resposta a Incidentes





Resposta a Incidentes

- 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





Abordagem Holística

- 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)

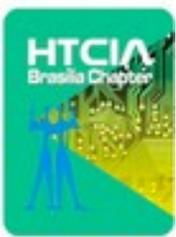




Abordagem Holística

- 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





Abordagem Holística

• Conscientize e eduque seus usuários

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: iStockphoto.

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 o 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 cabe ao usuário não é permitido a instalação de aplicativos na rede sem a devida autorização.

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: iStockphoto.

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 [link](#) 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. 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



Abordagem Holística



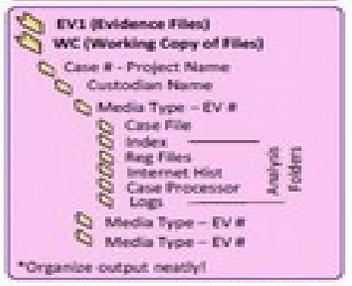
1. ADMINISTRATIVE STUFF

- 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
 - Deliverables
- Create Analysis Work Plan
- Create Investigative Plan

3. SETUP CASE FOLDER (example)



4. CONFIRM IMAGE INTEGRITY

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

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 NILES (12/26/2011)
TWITTER: @DAVIDNILES
BLOG: DAVIDNILES.BLOGSPOT.COM
EMAIL: DAVID@KPMG.COM
CREDITS TO: ED GOINGS, BOB LEE & SANS
QUESTION/FEEDBACK-CONTACT US!



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, identify "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 AMBR)
- 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/status

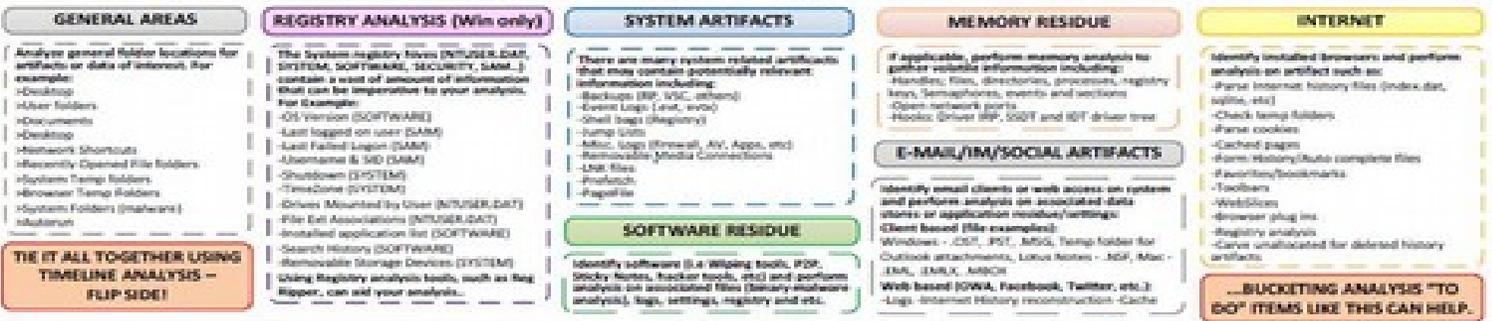
FILTERING

- Filter data based on meta data and extended 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: MemoryDump, Baseline, Volatility (SIFT), Passwords, AD-PSK, Password, Cyberback, Shellbags, Shellbags.py (SIFT), Internet History, Web historian, LNK Files, TweakUI, LnkB (SIFT), Event Logs LnkB & .evtx, TweakUI, GunkEVT, MFT, AnalyzeMFT, Network (SIFT), Index/PSB, SIDX/Forensic (SIFT), GFT Workstation (a great resource for lots of tools!), Email, NUSK, Clearwell, Recover My Email, Bulk extractor (SIFT), Image Mounting, FTK, Imager, InDisk, Live View, ODFMount, Virtual Box, Stego, Outguess, Hashing, MD5deep (SIFT), Shu2Md5deep (SIFT), Hashdeep (SIFT), Registry, Reg Ripper (SIFT), Registry Decoder, AD Registry Viewer, Reglookng (SIFT), vncui (SIFT), Windows Journal, Power, TweakUI

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



THE IT ALL TOGETHER USING TIMELINE ANALYSIS - FLIP SIDE!

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



Have more? Let me know!

8. REPORTING

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

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



Concluindo

“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 Brasilia

<http://www.facebook.com/HTCIABrasilia>

CERT.br

<http://www.cert.br/docs/whitepapers/notificacoes>

SANS Institute Blogs

<http://www.sans.org/security-resources/blogs>



Obrigado!