Número 109 | Dezembro 2025

NTT DATA

Radar

A revista de cibersegurança

Quando o hacking evolui mais rápido que o código

Por Jose Carlos Moral

O desenvolvimento de software deixou de ser uma corrida por agilidade e passou a ser uma corrida por segurança. Nesse novo paradigma de melhoria contínua, a segurança deixou de ser o último controle antes da implantação e passou a estar presente em todas as etapas do desenvolvimento.

Vivemos em um ecossistema onde os ataques evoluem tão rapidamente quanto o próprio código que tenta detê-los.

Hoje, os cibercriminosos já não estão escondidos em porões escuros — eles atuam a partir de laboratórios de IA, fóruns privados e, muitas vezes, de dentro das próprias empresas que usam para se proteger.

Novas técnicas de hacking — como phishing com IA, injeções de comandos, exploração da cadeia de suprimentos e deepfakes operacionais — estão mudando as regras do jogo.

Já não basta contar apenas com firewalls e antivírus. O verdadeiro desafio é antecipar-se e desenvolver soluções que pensem como um invasor, antes que ele ataque de fato.

Shift Left: segurança desde a primeira linha de código

No universo do desenvolvimento seguro, "Shift Left" já não é somente um conceito — é uma necessidade. Incorporar segurança em cada fase do ciclo de vida do desenvolvimento de software (SDLC, na sigla em inglês) não apenas reduz os custos com correções, mas também diminui a superfície de ataque antes mesmo que o produto seja lançado.

Automatizar auditorias, utilizar ferramentas de análise estática e dinâmica (SAST e DAST), adotar modelagem de ameaças e revisar dependências de terceiros deve ser tão comum quanto registrar alterações no repositório (commit).

Afinal, uma falha em uma dependência pode abrir caminho para a próxima grande violação de segurança. Casos como SolarWinds, Log4Shell e XZ Utils estão aí para lembrar que a cadeia de suprimentos digital é tão forte quanto seu elo mais fraco.

O fator humano: do elo mais fraco ao escudo inteligente

Por mais avançadas que sejam as técnicas de detecção, a engenharia social continua sendo a forma mais eficaz de ataque.

E é justamente aí que está a mudança de mentalidade desta nova era: na educação do usuário. Não se trata de transformar todos em especialistas em cibersegurança, mas de mudar a cultura digital.

O objetivo deve ser fazer com que um desenvolvedor saiba reconhecer quando um código pode ser vulnerável, e que desconfie antes de clicar em um link que pareça suspeito.

O futuro do hacking é colaborativo

Hacking ético, programas de recompensa por bugs (bug bounty programs) e a colaboração entre comunidades de especialistas (white hats) e empresas estão impulsionando uma nova mentalidade: a defesa compartilhada.

Em um mundo em que os ciberataques já funcionam como uma indústria, apenas uma resposta coletiva pode fazer frente à ameaça. A segurança já não é uma camada adicional. Tornou-se uma postura.

E, como toda postura, ela se consolida desde a concepção do software, no modo como projetamos cada linha com segurança em mente.

Jose Carlos Moral
Cybersecurity Manager Architecture

Encerramento de 2025

Cibercrônica por Joel Perez

No segundo semestre de 2025, o cenário da cibersegurança entrou em uma fase de transformação acelerada. Táticas clássicas, como phishing em massa e ransomware genérico, já não são suficientes. Os hackers vêm aprimorando técnicas de ataque mais sofisticadas, integradas e perigosas — exigindo respostas igualmente robustas e imediatas.

IA, automação e deepfakes: a arma silenciosa

Relatórios recentes indicam que ataques impulsionados por inteligência artificial (IA) deixaram de ser uma especulação do futuro, sendo aplicados em larga escala. Segundo a Check Point Software, em 2025, tanto estados quanto organizações criminosas "vêm empregando IA em campanhas de desinformação e na disseminação de malware disruptivo". Por exemplo:

- Modelos generativos que criam e-mails de phishing quase idênticos aos legítimos.
- Deepfakes com voz ou vídeo para imitar executivos ou funcionários e obter acessos privilegiados.
- Automação do processo de invasão, acelerando o intervalo entre a identificação de vulnerabilidades e sua exploração.

Essas técnicas estão transformando o "hacker tradicional" em algo mais parecido com um "orquestrador digital": em vez de lançar cinco e-mails genéricos, são gerados dezenas de ataques personalizados, desenvolvidos por IA e adaptados ao alvo específico.

Multiplataforma, cadeia de suprimentos e ataques sem malware clássico

As táticas também estão se diversificando para vetores mais complexos em comparação com as táticas do passado. Por exemplo, segundo a revista especializada, essa tendência engloba:

- Ataques à cadeia de suprimentos: comprometem um terceiro elemento para alcançar o alvo final.
- Ataques multiplataforma: têm como alvo diferentes sistemas operacionais (como Windows, Linux, dispositivos móveis e até mesmo ambientes em nuvem) dentro de uma mesma ofensiva.
- Técnicas sem malware visível (fileless): exploram processos legítimos do sistema, memória RAM ou serviços em nuvem para se movimentar sem deixar rastros tradicionais.

Isso significa que muitas defesas tradicionais — antivírus, firewalls, assinaturas de malware — não são mais suficientes individualmente.

Extorsão tripla, infostealers e ataques ao perímetro da nuvem

A evolução do ransomware também sustenta essa nova era do hacking: não se trata apenas de criptografar discos, mas de roubar dados, publicá-los, exercer pressão social e aplicar múltiplas formas de extorsão. Uma das técnicas-chave para 2025 é a chamada "extorsão tripla" (roubo + criptografia + exposição pública), combinada ao uso de deepfakes e ataques direcionados.

Além disso, os chamados infostealers — programas voltados ao roubo de informações sensíveis — se multiplicaram e atuam como ponto de partida para o ciclo completo do ataque.

Por outro lado, a ampliação dos ambientes em nuvem, dispositivos IoT e edge computing escancarou novas brechas de entrada: os invasores já não entram apenas pela rede corporativa tradicional, mas por dispositivos periféricos, serviços SaaS, contêineres e microsserviços vulneráveis.

Ameaça persistente, colaboração entre atores e reutilização acelerada

Os invasores — sejam grupos criminosos, hacktivistas ou estados-nação — também vêm apresentando uma evolução estrutural:

- Colaboração entre APTs (grupos de ameaças persistentes avançadas) e redes criminosas, combinando espionagem com objetivos financeiros.
- Ciclos de reutilização de ferramentas, kits modulares prontos para uso e rápidas adaptações permitem que uma técnica descoberta hoje seja disseminada em poucas semanas.
- O fator surpresa tornou-se cotidiano: menos ataques "ruidosos" e mais operações sigilosas, que são distribuídas ao longo do tempo e exigem detecção proativa, ao invés de uma detecção reativa.

O que fazer? Medidas de resposta para não ficar para trás

Diante desse cenário, a estratégia de defesa precisa evoluir:

- Adotar monitoramento contínuo e análise de comportamento, não apenas amostras;
- Integrar IA e automação à ciberdefesa: se os criminosos recorrem à inteligência artificial, a defesa também deve incorporar recursos inteligentes e adaptativos;
- Segmentar ambientes, reforçar o perímetro, mas também blindar o interior — incluindo cloud, endpoints e serviços de terceiros;
- Realizar simulações avançadas, exercícios de resposta rápida e operar com a premissa de que um “incidente” tende a ser uma campanha prolongada;
- Capacitar as equipes para identificar deepfakes, spear phishing hiperpersonalizado e ofensivas que se manifestam fora dos canais tradicionais, como o e-mail corporativo.

Conclusão

Entramos em uma nova era do hacking, marcada por velocidade, automação, uso da inteligência artificial e vetores cada vez mais complexos — um cenário que exige repensar radicalmente tanto os métodos ofensivos quanto as práticas de defesa cibernética.

As técnicas mencionadas não são mais uma "previsão do que pode surgir": elas já estão em campo. Cabe aos profissionais de cibersegurança enfrentá-las em um ambiente dinâmico, multidimensional e cada vez mais exigente.

Mic-E-Mouse: quando o mouse vira microfone

Artigo de Rodrigo Rey e Alberto Agra

Em um cenário em que a inteligência artificial (IA) avança mais rápido que os mecanismos de proteção, cada nova descoberta em cibersegurança desafia os limites da tecnologia. A mais recente delas, batizada de Mic-E-Mouse, revela uma vulnerabilidade inesperada: os sensores de movimento dos mouses de computador podem ser explorados para captar sons do ambiente, transformando-se, na prática, em microfones improvisados. Essa revelação não apenas representa um desafio técnico, mas também levanta um debate ético sobre os riscos associados à engenhosidade humana na era da IA.

A pesquisa, publicada em meados de setembro de 2025 por um grupo de especialistas em cibersegurança de diversas universidades, tinha um objetivo simples, porém alarmante: explorar se os sensores ópticos e de movimento presentes em mouses comuns seriam capazes de registrar vibrações mínimas provocadas por ondas sonoras.

Esses sensores, projetados originalmente para detectar deslocamentos sobre superfícies, registram variações de luz em alta velocidade — em alguns modelos, até 30 mil vezes por segundo. Os pesquisadores perceberam que essas oscilações poderiam, em determinadas condições, refletir vibrações geradas por vozes ou sons próximos.

A descoberta se espalhou rapidamente por veículos especializados como TechSpot, Kaspersky, GBHackers e The Indian Express, surpreendendo a comunidade tecnológica e lembrando que as ameaças cibernéticas nem sempre vêm de softwares maliciosos — às vezes, vêm dos próprios dispositivos físicos.

O ataque descrito pelos pesquisadores se baseia em um princípio físico. Todo som gera uma vibração mecânica nas superfícies próximas. Quando um mouse com sensor óptico de alta resolução está sobre uma mesa, essas vibrações microscópicas podem interferir no reflexo de luz usado pelo sensor para calcular o movimento.

Os cientistas desenvolveram um modelo de IA capaz de analisar os sinais captados pelo sensor — aparentemente apenas coordenadas de movimento — e filtrá-los para reconstruir padrões de frequência associados a sons humanos. Com treinamento suficiente, a rede neural conseguiu identificar trechos de fala e reconhecer palavras específicas com precisão surpreendente em ambientes controlados.

O ataque, conhecido como Mic-E-Mouse, não exige acesso físico ao microfone do computador, nem a componentes de áudio. Bastaria comprometer o firmware do mouse ou interceptar os dados de movimento transmitidos ao equipamento. Embora o processo ainda seja experimental e sua execução prática seja complexa, demonstra que mesmo os periféricos mais comuns podem se transformar em ferramentas de espionagem.

O experimento Mic-E-Mouse não é apenas uma demonstração técnica, mas sim um alerta sobre o futuro da privacidade digital. A capacidade de transformar um mouse em um dispositivo de escuta mostra até que ponto a IA pode reinterpretar os limites físicos da tecnologia.

Embora o ataque não represente, por enquanto, uma ameaça em larga escala, sua existência nos lembra que a segurança deve ser pensada como um sistema integrado — em que cada componente, por mais trivial que pareça, pode se tornar uma porta aberta ao risco.

Portanto, este estudo nos convida a refletir sobre nossa relação com a tecnologia. Mais do que desenvolver máquinas inteligentes, é essencial garantir que essa inteligência permaneça a serviço do ser humano — e não contra ele.

Rodrigo Rey
Cybersecurity Lead Architect

Alberto Agra
Cybersecurity Expert Architect

Consciência quântica

Espaço quântico por María Gutiérrez

Encerramos este ano de 2025, marcado pela ciência e pelas tecnologias quânticas, com a convicção de que o universo quântico já é uma realidade. Recentemente, vimos aplicações concretas nas áreas da saúde, energia, logística, finanças, comunicações... A física quântica deixou de habitar apenas as fórmulas, os laboratórios ou os centros de pesquisa, e começa a fazer parte do nosso cotidiano. Mais do que isso, talvez ela sempre tenha estado presente em nossas vidas — especialmente no nosso cérebro. Fenômenos como superposição, entrelaçamento quântico e coerência quântica podem desempenhar um papel essencial nos processos que dão origem à experiência subjetiva, essa misteriosa qualidade que nos faz “ser” e “sentir”. A discussão vai além da informação ou do processamento neural, trata-se da base fundamental que sustenta a mente consciente. Será que isso é o que chamamos de consciência?

Durante muito tempo, acreditou-se que o cérebro humano, por operar em temperatura corporal, seria um ambiente quente e ruidoso demais para manter a coerência quântica. No entanto, nos últimos anos, surgiram evidências experimentais que reabrem esse debate. No campo da biologia quântica, já foi comprovada a existência de coerência em sistemas vivos, como na fotossíntese e na navegação de certas aves – o que demonstra que a vida é capaz de explorar fenômenos quânticos mesmo em condições "não ideais".

Essa ideia ganhou corpo nos anos 1990, quando o físico Roger Penrose e o anestesista Stuart Hameroff propuseram a teoria redução objetiva orquestrada (Orch-OR). Segundo essa hipótese, a consciência emergiria de processos quânticos nos microtúbulos – estruturas do citoesqueleto celular – que permitiriam estados de superposição no cérebro. Esses estados colapsariam de forma orquestrada, gerando momentos discretos de consciência.

Essa teoria impulsionou uma nova linha de pesquisa, que alguns chamam de neurobiologia quântica, voltada a explorar os limites da decoerência em estruturas neurais e a possível interação entre processos quânticos e cognição. Embora estejamos longe de uma demonstração real, a simples possibilidade está modificando nossa forma de conceber a mente.

Essas ideias tocam o campo da metafísica, mas também lançam um desafio empírico: é possível criar experimentos que diferenciem um cérebro clássico de um "quântico"? Alguns projetos, ainda em fase conceitual, tentam detectar assinaturas de entrelaçamento em redes neuronais ou correlações não clássicas na atividade cerebral.

A dificuldade técnica é enorme, mas o impacto potencial seria revolucionário. Em um momento em que a inteligência parece não ser mais o que nos define como humanos – já que a IA supera nossa memória, capacidade e velocidade, embora exija muito mais energia para aprender –, a busca pelo que nos torna verdadeiramente únicos e diferentes nos conduz à consciência.

Será que a consciência é mesmo o nosso diferencial? E se, na verdade, estiver ligada à complexidade e ao colapso de estados quânticos? Seria possível que a computação quântica – concebida para resolver problemas complexos – possa algum dia dotar a IA de consciência? Então, não é isso que nos torna "únicos" e "diferentes".

A consciência quântica ainda não é uma teoria comprovada, mas é um convite ao pensamento. E esse pensamento, situado na fronteira entre a física, a biologia e a filosofia, deve se consolidar como um dos grandes temas do debate científico nas próximas décadas. O ano de 2025 chega ao fim, mas o debate quântico está apenas começando.

Evasão de EDR: a nova fronteira da segurança ofensiva

Tendências por Jesús Murciano

Ao longo de 2025, uma tendência tem chamado a atenção dos especialistas em cibersegurança: a evasão de detecção e resposta de endpoint (EDR). Essas plataformas, que representam a linha de frente contra ameaças avançadas, têm sido alvo de estudos tanto por pesquisadores quanto por cibercriminosos que buscam burlar seus mecanismos de detecção e resposta. O surgimento de ferramentas como a EDRFreeze simboliza o início de uma nova fase na corrida armamentista entre ataque e defesa. A tática já não se limita à ocultação de malwares: seu foco agora é desativar temporariamente os mecanismos que garantem a proteção do sistema.

Como funciona essa técnica?

Até recentemente, as estratégias mais comuns para evitar a detecção por EDR envolviam o uso de drivers vulneráveis (conhecidos como BYOVD, Bring Your Own Vulnerable Driver), que concediam privilégios de kernel para desativar serviços de segurança. No entanto, esse método exigia acesso avançado e deixava rastros detectáveis.

A mudança de paradigma vem com técnicas como a EDRFreeze, que operam totalmente em modo usuário. Ao explorar mecanismos legítimos do sistema operacional, como o serviço Windows Error Reporting (WER), essas ferramentas podem suspender ou “congelar” os processos de segurança sem precisar explorar vulnerabilidades do kernel ou carregar drivers assinados.

Na prática, isso permite que um invasor interrompa a atuação do EDR pelo tempo necessário para executar códigos maliciosos, movimentar-se lateralmente ou exfiltrar dados, sem gerar alertas imediatos.

Por que essa técnica é tão eficaz?

A eficácia dessa técnica está justamente em sua atuação discreta e no uso de componentes legítimos do próprio sistema operacional. Ao utilizar processos nativos do Windows e ser executado com permissões padrão, o invasor reduz significativamente as chances de ser detectado pelas defesas tradicionais.

Esse tipo de tática, alinhada à filosofia "living off the land (LotL)" (viver da terra, em tradução literal), representa uma evolução natural das técnicas de evasão, priorizando o uso silencioso de recursos internos do próprio sistema ao invés de ferramentas externas.

Além disso, essas ferramentas dispensam conhecimento técnico aprofundado sobre o kernel, ampliando seu uso entre agentes menos experientes. Ao mesmo tempo, o avanço das pesquisas em comunidades ofensivas tem acelerado a divulgação de provas de conceito e scripts que replicam o comportamento de suspensão de processos, indicando que mesmo atores com baixo nível técnico poderão executar ataques mais sofisticados.

Conclusão

A evasão do EDR representa uma evolução significativa nas táticas dos invasores e obriga os defensores a se adaptarem rapidamente. Proteger os próprios mecanismos de defesa torna-se uma prioridade estratégica. As organizações devem reforçar os controles de integridade de processos, aplicar listas de bloqueio de drivers vulneráveis, monitorar o uso anômalo de serviços do sistema e, sobretudo, interpretar os “silêncios do EDR” – períodos em que a telemetria deixa de ser reportada – como possíveis indicadores de um ataque.

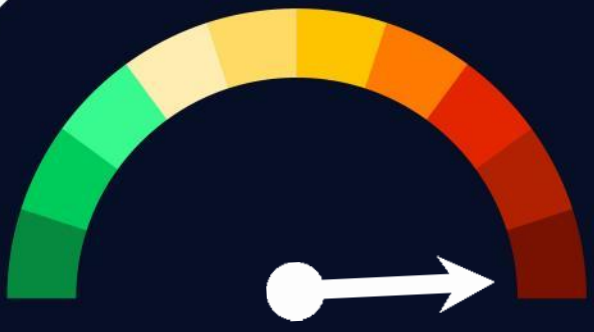
Em um ambiente cada vez mais sofisticado, onde o objetivo não é mais apenas comprometer o sistema, mas desativar aqueles que protegem esse sistema, a resiliência dos sistemas de defesa será o verdadeiro fator diferenciador. A corrida para “congelar o EDR” está apenas começando.

Jesús Murciano
Cybersecurity Analist

Vulnerabilidades

Vulnerabilidade crítica no React Native Metro CLI

Data: 3 de novembro de 2025
CVE: CVE-2025-11953



CVSS: 9.8
CRÍTICA

Descrição

A vulnerabilidade **CVE-2025-11953**, classificada como crítica, permite que invasores remotos executem código arbitrário nas máquinas dos desenvolvedores que utilizam o servidor de desenvolvimento Metro do React Native.

A origem da vulnerabilidade ocorre porque o servidor não valida corretamente os parâmetros *lineNumber* e *file*. Em ambientes Windows, o servidor aciona o editor por meio do módulo *child_process.spawn* do Node.js e transmite o arquivo e a linha como argumentos. Se o parâmetro lineNumber contiver metacaracteres de *shell*, o *cmd.exe* pode interpretá-los e permitir a execução de comandos arbitrários. Não é necessária autenticação, e é possível explorar a falha remotamente caso haja acesso à porta padrão do servidor (8081).

Solução

Para mitigar a vulnerabilidade CVE-2025-11953, execute as seguintes etapas:

- Atualize o @react-native-community/cli-server-api para a versão 20.0.0 ou superior, que inclui a correção para essa vulnerabilidade.
- Para melhorar a segurança, ou caso não seja possível atualizar, configure o servidor de desenvolvimento para se conectar de modo explícito à interface localhost, incluindo a opção --host 127.0.0.1

Produtos afetados

Esta vulnerabilidade crítica afeta todas as versões anteriores do commit que resolve a falta de validação dos parâmetros de entrada, corrigida no React Native CLI, especificamente no componente Metro Development Server versões anteriores à 20.0.0. A exploração da vulnerabilidade é mais severa em sistemas Windows.

Referências

- nvd.nist.gov
- jfrog.com

Vulnerabilidades

Vulnerabilidades Críticas no Cisco Unified Contact Center Express (UCCX)

Data: 5 de novembro de 2025
CVE: CVE-2025-20354 e mais 1

CVSS: 9.8
CRÍTICA

Descrição

A Cisco divulgou vulnerabilidades críticas que afetam o seu produto Unified Contact Center Express (UCCX).

A vulnerabilidade CVE-2025-20354 permite que um invasor remoto, mesmo sem permissões, envie arquivos maliciosos e execute código com privilégios administrativos. A falha está relacionada a um erro no mecanismo de autenticação do UCCX.

Já a vulnerabilidade CVE-2025-20358 permite que um hacker contorne a autenticação (bypass) e obtenha permissões administrativas. Essa vulnerabilidade decorre de um problema na autenticação entre o componente CCX Editor e o servidor UCCX.

Solução

A Cisco disponibilizou um patch para mitigar as falhas. Recomenda-se a atualização imediata para uma das versões abaixo:

- 12.5 SU3 ES07.
- 15.0 ES01.

Produtos afetados

A vulnerabilidade afeta todas as instalações do UCCX, independentemente da configuração utilizada.

Referências

- sec.cloudapps.cisco.com

ShopLentor para WordPress corrige uma vulnerabilidade crítica

Data: 4 de novembro de 2025
CVE: CVE-2025-12493

Crítica

Descrição

ShopLentor (anteriormente conhecido como WooLentor) é um **complemento de destaque do WordPress** que integra o WooCommerce com os editores de páginas Elementor e Gutenberg. Com milhões de downloads e uma ampla base de usuários ativos, é um componente fundamental no ecossistema de comércio eletrônico do WordPress.

Recentemente, foi identificada a vulnerabilidade **CVE-2025-12493**, uma falha de **inclusão de arquivos locais (LFI)** que afeta todas as **versões até a 3.2.5**. O problema tem origem na função load_template, que não valida corretamente os caminhos de arquivos fornecidos pelo usuário, permitindo o uso de sequências como ../ para acessar arquivos internos do servidor, como o wp-config.php.

Classificada como **CWE-22**, essa vulnerabilidade pode permitir a **exposição de informações sensíveis** ou até a **execução remota de código**, mesmo sem autenticação — o que eleva sua gravidade. Até o momento, não foram divulgadas provas de conceito nem códigos de exploração, embora a atualização imediata do plugin para uma versão corrigida seja fortemente recomendada.

Produtos afetados

O complemento afetado é o **ShopLentor – WooCommerce Builder** para Elementor e Gutenberg. A vulnerabilidade impacta **todas as versões até a 3.2.5 (inclusive)** e pode ser explorada em qualquer site WordPress que utilize uma versão vulnerável do plugin.

Solução

Atualize o plugin ShopLentor do WordPress para a versão mais recente (3.2.6 ou superior). Caso não seja possível realizar a atualização de imediato, recomenda-se desativar o plugin temporariamente e implementar regras específicas de WAF para bloquear possíveis vetores de exploração.

Referências

- nvd.nist.gov
- wordfence.com

Google corrige vulnerabilidades no Chrome

Data: 5 de novembro de 2025
CVE: CVE-2025-12725, CVE-2025-12727 e mais 3

Alta

Descrição

O Google publicou recentemente um patch de segurança que corrige 5 vulnerabilidades que afetam diferentes componentes do navegador, incluindo WebGPU, JavaScript V8 e Omnibox. Essas vulnerabilidades podem permitir a execução remota de código.

As vulnerabilidades corrigidas mais relevantes são:

- CVE-2025-12725 (CVSS 8.8): vulnerabilidade que permitiria a um invasor executar código remotamente devido a uma falha de script que permite escrever além dos limites definidos (Out of Bounds).
- CVE-2025-12727 (CVSS 8.8): vulnerabilidade que permitiria a um invasor executar um código remotamente devido a uma falha no motor Javascript V8.

Produtos afetados

As versões impactadas do produto são:

- Versões anteriores à 142.0.7444.134/.135 (Windows)
- Versões anteriores à 142.0.7444.135 (macOS)
- Versões anteriores à 142.0.7444.134 (Linux)

Solução

O fabricante recomenda atualizar para as seguintes versões:

- 142.0.7444.134/.135 (Windows)
- 142.0.7444.135 (macOS)
- 142.0.7444.134 (Linux)

Referências

- chromereleases.googleblog.com
- cybersecuritynews.com

Eventos

SANS CyberThreat Summit 2025
3 a 4 de dezembro

O emblemático estádio Stamford Bridge será palco de um congresso de dois dias voltado a profissionais de cibersegurança ofensiva e defensiva. Organizado pelo SANS Institute, o evento oferece uma imersão técnica profunda, com foco em táticas, ferramentas e estudos de caso reais de ataque e defesa em um ambiente de alto nível de conhecimento. Uma chance única para profissionais que desejam avançar para cargos de liderança em cibersegurança: dois dias com conteúdo técnico aprofundado, networking estratégico e a reconhecida excelência do SANS como selo de qualidade.

Link

Black Hat Europe 2025
8 a 11 de dezembro

Londres volta a ser o epicentro europeu da cibersegurança com um dos eventos mais relevantes do setor. Além de treinamentos especializados de dois e quatro dias, o evento inclui as conferências principais (briefings) nos dias 10 e 11, onde são reveladas pesquisas inovadoras, demonstrações de ferramentas open-source ("Arsenal"), exposição de soluções e amplas oportunidades de conexão profissional.

Link

León Cybersecurity Conference
20 de dezembro

Realizada em Cafiada de Mariches #3435, a conferência de um dia coloca o Bajío no mapa da segurança digital.

Reunindo especialistas nacionais e internacionais, o evento tem como foco capacitar pessoas e organizações para enfrentar os desafios do ambiente digital, com uma proposta clara de formação, atualização e inspiração.

Link

Recursos

➢ AdaptixC2

Adaptix é um framework extensível de pós-exploração e emulação adversária desenvolvido para profissionais de pentest. O servidor é escrito em Golang, oferecendo maior flexibilidade para o operador. A interface gráfica (GUI), desenvolvida em C++ QT, é compatível com Linux, Windows e macOS.

Link

➢ LLM Red Teaming Framework

O DeepTeam incorpora as pesquisas mais recentes para simular ataques adversários utilizando técnicas de ponta (SOTA), como jailbreaking e injeções de comandos, com o objetivo de detectar vulnerabilidades como vieses e vazamentos de informações de identificação pessoal, que de outra forma poderiam passar despercebidas. Após a descoberta das vulnerabilidades, a DeepTeam oferece medidas de proteção para evitar problemas na produção.

Link

➢ DumpGuard

A Darktrace desenvolveu sua plataforma para detectar ameaças através do aprendizado do comportamento normal da rede, sem depender de sinais de ataques conhecidos. Sua capacidade de resposta autônoma Antigena pode conter ataques de maneira direcionada, sem interromper as operações comerciais.

A plataforma utiliza análise comportamental para identificar anomalias de alto risco, incluindo ameaças sofisticadas impulsionadas por IA, e estabelece modelos únicos para cada ambiente digital empresarial.

Link1

Link2

Inscreva-se na RADAR
up.nttdata.com/suscribetearadar

Powered by the Cybersecurity NTT DATA Team

br.nttdata.com