



Home ■ Segurança ■ Hacker

Deus do Cibercrime: a ascensão e a queda do maior defacer do Brasil

Por Redação | 07 de Agosto de 2020 às 20h00

Canaltech

Era manhã do dia 18 de abril de 2019 — véspera de feriado de Paixão de Cristo. A Polícia Federal, obedecendo mandados de busca e apreensão expedidos pela 3ª Vara da Justiça Federal da Seção Judiciária de Sergipe, bateu na casa de seis indivíduos nas cidades de Belo Horizonte (MG), Brasília (DF) e Novo Hamburgo (RS). O objetivo era coletar computadores, notebooks e smartphones que poderiam ser usados como prova para identificar e responsabilizar os autores de invasões ao site da autoridade sergipana.

- [Protestos na Internet: Conheça 7 casos recentes de ativismo hacker](#)
- [Site de governo dos EUA é invadido e mostra Trump ensanguentado](#)
- [Polícia prende grupo que aplicou golpe em 55 mil brasileiros usando criptomoedas](#)

Um desses indivíduos era o programador Rodrigo Zanatta. Lá em 2016, estando desempregado, resolveu se aliar a alguns membros do submundo cibernético com a esperança de fazer algum dinheiro e acabou participando de tais invasões, aproveitando-se de seu talento natural para encontrar falhas em ambientes web e explorá-las ao seu bel prazer. A jornada, obviamente, não terminou do jeito que o brasiliense esperava.

“Algo muito divertido para sua vida, devo lhe dizer”, brinca Zanatta, relembrando a visita dos federais à sua residência. Embora atualmente trabalhe no setor de segurança da informação de um respeitado órgão público, ele ainda responde crime de invasão de dispositivo informático, previsto no art. 154-A do Código



O art. 154-A foi criado pela lei 12.737 de 30 de novembro de 2012. Ele tipifica como crime o ato de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. A pena é de três meses a dois anos.



Reprodução/DataBreachToday

O arrependimento pelos seus atos acabou fazendo com que Rodrigo se tornasse obcecado em estudar sobre todas as infrações registradas desde a criação de tal artigo, e, ao mesmo tempo, resolveu que passaria a ajudar as autoridades a identificar outros criminosos especializados em invadir websites. Após mirar em alvos “pequenos”, ele naturalmente acabou se centrando em um peixe grande: VandaTheGod, o maior *defacer* brasileiro e um dos mais renomados do mundo inteiro.

Afinal, o que é defacement?

Defacement — ou simplesmente *deface*, como é popularmente conhecido — é ato de desfigurar a aparência de um website, geralmente com o objetivo de transmitir uma mensagem de cunho ativista. Comumente considerada uma



nasceu (e tampouco quando o termo foi cunhado).

Na maioria das vezes, um *deface* não culmina no roubo de informações sensíveis e tampouco causa disruptões graves no sistema afetado: o responsável pela página vitimizada consegue reverter as alterações em poucos minutos. Para efetuar a desfiguração, os criminosos costumam explorar brechas na codificação do site, se aproveitar de vulnerabilidades no servidor web em que ele está hospedado ou até mesmo roubar senhas de sistemas como Wordpress para editar a “home” manualmente.

Podemos dividir os *defacers* — hackers especializados na prática — em dois grandes grupos: os vândalos, que simplesmente o fazem por pura diversão ou para deixar sua marca em um website de alto tráfego; e os hacktivistas, que o fazem com o objetivo de protestar contra políticas governamentais ou demonstrar apoio por alguma causa social bem específica. De qualquer forma, ambos se enquadram no art. 154-A.



(Imagem: Reprodução/Marcelo Camargo/Agência Brasil)

A prática do *deface* é tão comum ao redor do globo que existe até mesmo um website dedicado a guardar *mirrors* (cópias offline) de sites desfigurados. Trata-se do Zone-H, criado em 2002 na Estônia e que compila defaces pelo apelido do [hacker](#) responsável pela pichação. Todos os feitos submetidos à plataforma são

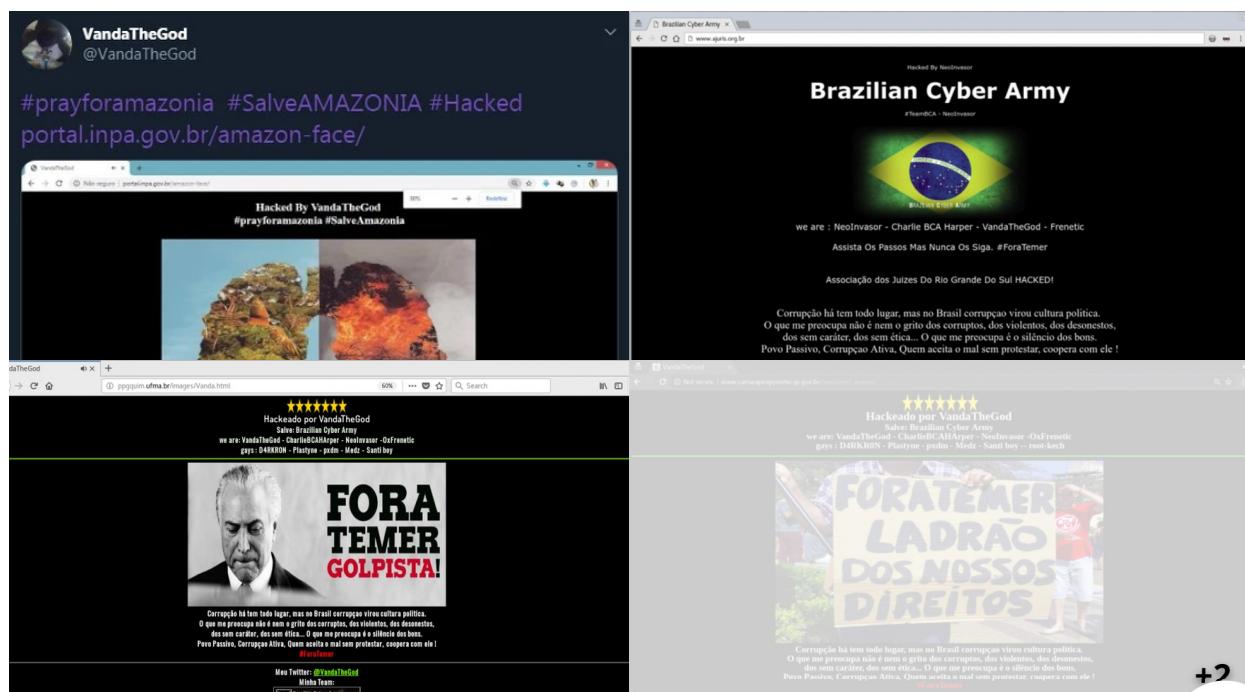


Um currículo memorável

É normal encontrar, após algumas horas navegando pelo Zone-H, hackers que acumularam 100, 200 ou até 500 sites desfigurados. Trata-se de uma marca capaz de impressionar qualquer iniciante no mundo do crime cibernético. Há, porém, um indivíduo em específico que ostenta quase 5 mil *defaces* em nada menos do que 42 países diferentes. Este indivíduo é brasileiro, e é conhecido no universo do [cibercrime](#) pelo apelido de VandaTheGod.

Os primeiros rastros de atividade de tal nickname remontam o ano de 2013. Naquela época, Vanda começou sua “carreira” de forma tímida: no Brasil, desfigurou sites de pequenas empresas (como um lava rápido de São Bernardo do Campo, em São Paulo) e de algumas entidades governamentais do Equador, da Argentina e da Filipinas. Os sites foram modificados simplesmente para exibir a mensagem “Deface By @VandatheGod or @CosmoTheGod”, fazendo propaganda de sua equipe de criminosos UGNazi.

Ao longo dos próximos seis anos, Vanda atacaria diversos outros sites governamentais — na maioria das vezes, com o objetivo de disseminar mensagens de protesto político ou para demonstrar sua aparente associação com o nazismo.



Na lista de vítimas brasileiras, podemos destacar diversas prefeituras (como



o Serviço Brasileiro de Apoio as Micro e Pequenas Empresas (SEBRAE). Internacionalmente falando, Vanda mirou em uma série de sites locais de estados dos EUA e até mesmo alguns domínios gerenciados pela União Europeia.

É difícil obter um cálculo preciso sobre a quantidade de páginas desfiguradas pelo hacker. O Zone-H lista apenas as invasões registradas a partir de setembro de 2016; ademais, é necessário levar em conta que a contabilidade de defaces inclui também subdomínios presentes no mesmo IP. Também existem *defaces* verificáveis (que podem ser conferidos através de *mirrors*) e os não verificáveis (que não possuem uma cópia disponível).

Número de sites hackeados





Arte/Canaltech

Um trabalho de investigação do **Canaltech** contabilizou, em 21 de novembro de 2019, que Vanda havia realizado um total de 4,743 defaces em 919 IPs diferentes. Desse total, os defaces verificáveis, em ordem decrescente, foram feitos nos EUA (522), Brasil (236), Austrália (80), Países Baixos (56), Itália (57), Alemanha (38), África do Sul (34), Canadá (33) e assim por diante; os países menos afetados foram Romênia, Trindade e Tobago, Guatemala, Cabo Verde, Cingapura, Islândia e Índia, com um deface cada um.

Quando os deuses caem

Tal currículo, por si só, seria mais do que o suficiente para colocar VandaTheGod na história do crime cibernético. Porém, o criminoso fez muito mais do que simplesmente desfigurar sites: ele também possui uma lista extensa de outras contravenções, e a maioria delas sempre foi ostentada em seu próprio perfil no [Twitter](#). Usando a rede social, o cracker publicava anúncios de cartões de crédito clonados, armas de fogo, cédulas falsas, apologias ao nazismo e compras realizadas com informações pessoais de terceiros.

Em outubro do ano passado — pouco antes da nossa conversa com Zanatta —, o *defacer* atingiu um novo patamar ao anunciar, aos quatro ventos, ter obtido detalhes médicos de pelo menos 1 milhão de cidadãos da Nova Zelândia. O banco de dados teria sido extraído através de uma vulnerabilidade nos sistemas do Ministério da Saúde do país em questão, e Vanda parecia disposto a comercializar tal pacote por quantias generosas de dinheiro.



Yes I`m Have 1 million datas PHO Zealand I sell vs
200 dolar in btc contact

11:00 PM · Oct 4, 2019 · Twitter Web App

Reprodução/VandaTheGod/Twitter

A venda, porém, nunca chegou a ser concretizada. Aos 23 anos de idade, VandaTheGod foi preso em sua residência na cidade de Uberlândia, no Triângulo Mineiro, no fim de novembro.

Seguindo o rastro de migalhas

Ao que tudo indica, a gota d'água para as autoridades foi uma série de invasões cometidas pelo defacer nos meses anteriores à sua detenção: ele desfigurou o site da Polícia Civil de Minas Gerais, do Ministério Público de Minas Gerais, do Tribunal de Justiça do Estado de Goiás e — pasmem — do Exército Brasileiro. O que Vanda não sabia é que, enquanto ele se divertia com tais desfigurações, existiam duas investigações ocorrendo simultaneamente e que culminaram em sua prisão.

A primeira delas partiu do próprio Rodrigo Zanatta, que passou meses estudando as redes sociais do criminoso e as fotografias que o próprio disponibilizava em tais plataformas. Antes mesmo da prisão de Vanda, o **Canaltech** já tinha acesso ao relatório de Zanatta e possuía conhecimento de seu endereço.

“Antes de discutir sobre o hacker, esclareço que nunca o conheci na vida real nem mesmo troquei mensagens com ele. Foquei nele por seu elevado número de invasões e o longo período que vem praticando seus defaces”, explica Zanatta, em um detalhado report compartilhado com a redação. “Ele é apenas alguém que se acha no direito de cometer esses crimes e arrogante para achar que não irão atrás dele”, aponta.

O ponto de partida do brasiliense foi o email utilizado por VandaTheGod: “fathernazi@gmail.com”. Pesquisando tal endereço, Zanatta encontrou um *doxxing* (dossiê contendo informações pessoais de um cidadão) realizado por outro hacker contrário às ações de Vanda. Tal documento revelaria o endereço e nome real do criminoso, mas o próprio defacer negou, em uma mensagem publicada no Tw em outubro de 2016, que aqueles dados seriam os seus.



registrante de sites administrados pelo criminoso e ao observar capturas de tela que mostram a caixa de emails aberta), o pesquisador decidiu conferir o endereço informado no *doxxing* no Google Maps. Uma casa simples, no bairro Laranjeiras, em Uberlândia.

A comprovação de que o endereço era realmente a casa de Vanda veio através de comparações de fotografias registradas pelo próprio hacker no interior de sua residência. Detalhes como frestas no portão da garagem e caixa de correspondências na entrada social combinam perfeitamente com o exterior vislumbrado através do Street View.



Como se isso não fosse o suficiente, Vanda também cometeu um deslize ao publicar, em abril de 2019, um tweet se gabando de ter pedido uma pizza no [iFood](#) com cartões clonados. O hacker borrou o nome da pizzaria, mas, ao analisar os estabelecimentos em Uberlândia com caracteres similares aos borrados, Zanatta conseguiu confirmar que o pedido foi feito na Rafa Pizza Delivery, localizada a apenas 15 quilômetros da casa do criminoso cibernético.

A linha do tempo das provas que ajudaram na identificação é a seguinte:

- Em 28 de maio de 2013, ele menciona seu email pessoal;
- Em 15 de setembro de 2015, ele publica uma captura de tela com o mesmo email aberto em uma guia do navegador;



pessoais;

- Em 08 de outubro de 2016, ele toma conhecimento do *doxxing* e nega sua veracidade;
- Em 20 de abril de 2018, ele publica a primeira foto de sua garagem, mostrando o portão deslizante;
- Em 27 de abril de 2018, ele publica a segunda foto, mostrando o portão social;
- Em 13 de março de 2019, ele divulga uma captura de tela de um pedido no iFood, mostrando estar morando na mesma cidade.

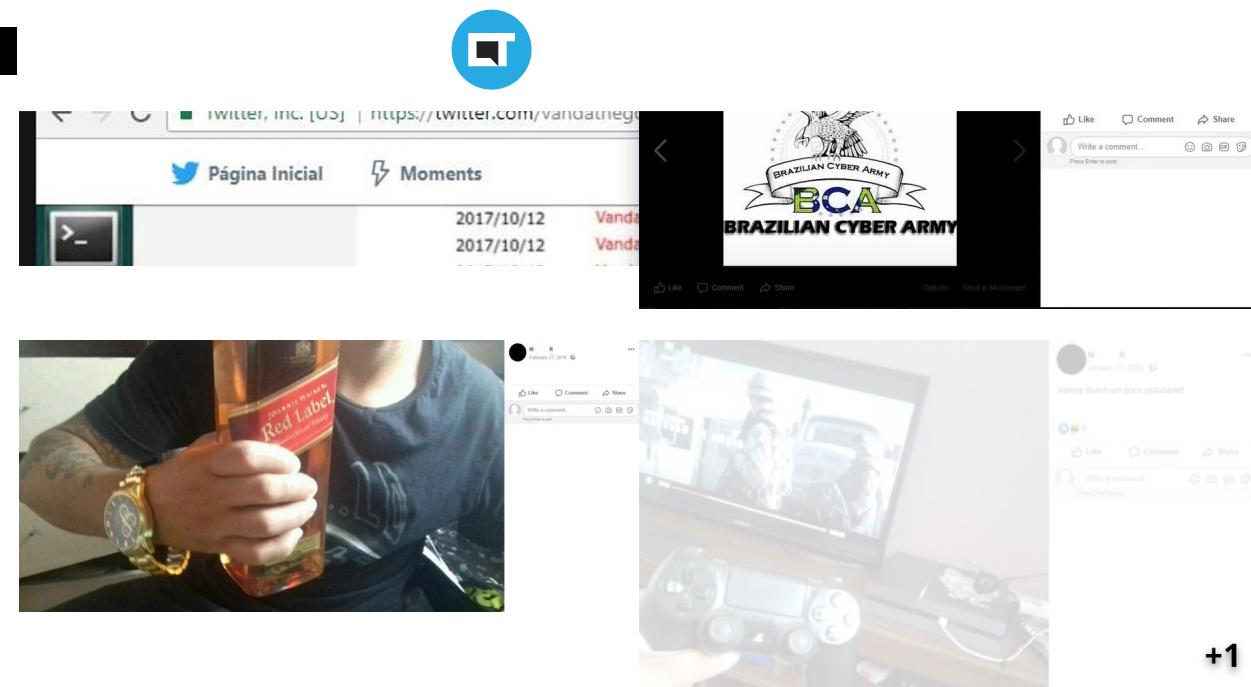
“Não foi preciso fazer perícia dos locais invadidos por ele. Mesmo se ele for extremamente cuidadoso quando realiza uma invasão, conseguiu ser extremamente descuidado em se esconder”, explica Zanatta. “Isso prova que não é apenas pelo IP que se identifica uma pessoa”.

Enquanto isso, do outro lado...

Simultaneamente, lá em Israel, outra investigação estava em andamento com o objetivo de descobrir a identidade de VandaTheGod. Pesquisadores da Check Point, empresa provedora de soluções de segurança, também analisavam as redes sociais do criminoso — incluindo sua atividade com outros apelidos, incluindo “Vanda de Assis” e “SH1N1NG4M3” — na esperança de encontrar brechas que revelassem seu nome real.

O *modus operandi* dos israelenses, porém, foi muito mais simples em comparação com o de Zanatta. Algumas checagens de registros de domínios também indicaram o mesmo endereço de Uberlândia. Porém, foi uma screenshot em específico que chamou atenção dos especialistas: uma captura de tela que exibe, discretamente, o nome de usuário logado no computador. Por questões de privacidade, citaremos apenas as iniciais: M. R.

De posse de tal nome, não demorou muito para que a Check Point encontrasse o perfil pessoal de Vanda — que, embora não citasse qualquer tipo de atividade criminosa, estava repleto de fotos do mineiro ostentando garrafas de uísque e relógios de grife. Também foram feitas comparações com fotografias de uma sala de estar postada em perfis de Vanda com imagens publicadas no perfil de M. R.



+1

Em entrevista ao **Canaltech**, os pesquisadores israelenses afirmaram que começaram a investigação “após um pedido de uma entidade governamental latino-americana que foi vítima de numerosos ataques” de Vanda. “Eles nos pediram para dizer quem estava por trás desses ataques perturbadores em websites governamentais”, explica a companhia, sem citar nomes específicos por razões de segurança.

“Em termos de volume, o Vanda gerou um número consistentemente alto de desfigurações. Porém, enquanto outros *defacers* também são capazes de temperar dados e causar danos permanentes, o Vanda não o fez”, comenta a empresa. “Sua prisão ocorreu poucas semanas depois que reportamos as informações para as autoridades. Entregamos o relatório para entidades brasileiras”, conclui.

Atrás das grades

A detenção do meliante causou comoção e teve uma ampla cobertura da mídia tradicional. Na época, a delegada Danielle Aguiar Carvalho, da 1ª Delegacia Especializada em Investigação de Crimes Cibernéticos, realizou uma audiência com a imprensa local para comentar sobre os crimes de Vanda.

“O site da Polícia Civil foi invadido e nós começamos a investigação para descobrir a identidade desse *cracker*. Ele usou uma técnica como se fosse uma pichação no site, onde ele colocou mensagens de cunho político. Em geral é contra a política do Brasil, ele não tinha nenhuma bandeira e não apoiava nenhum partido. Ele queria



"Ele também invadiu sites de lojas varejistas e obteve acesso aos dados de cartões de crédito dos clientes. E, com esses dados, ele fazia compras. No momento não temos como falar o valor do prejuízo. Ele é de uma família humilde, não tem formação na área", conclui.

A prisão foi tão emblemática que mereceu um comentário público até mesmo de Romeu Zema (Novo), atual governador de Minas Gerais. Em seu perfil no Twitter, o político publicou um vídeo a respeito da detenção e comemorou: "Mais uma vitória das nossas Forças de Segurança!".

Mais uma vitória das nossas Forças de Segurança! A Polícia Civil de Minas Gerais (PCMG) prendeu, na última semana, o homem que invadiu os sites da própria polícia, do Ministério Público de Minas Gerais, do Tribunal de Justiça de Goiás e até o site do Exército Brasileiro. pic.twitter.com/xXPM33l0Et

— Romeu Zema (@RomeuZema) November 25, 2019

É impossível dizer com exatidão quem ajudou mais na prisão de VandaTheGod. O **Canaltech** entrou em contato com as forças policiais de Minas Gerais para obter mais informações sobre a detenção do *cracker*, mas as autoridades negaram entrevistas. Em uma rápida conversa por telefone, porém, um investigador da Delegacia de Crimes Cibernéticos da Polícia Civil de Minas Gerais envolvido no caso garantiu que o dossiê de Zanatta "ajudou bastante".

"Estamos fazendo uma avaliação sobre quais crimes ele responderá", informou o investigador. Analisando seu perfil no Twitter, é possível estimar que, além da invasão de dispositivo informático, Vanda também poderia ser indiciado por porte ilegal de arma de fogo, fraude eletrônica, falsificação de moeda, falsidade ideológica e apologia ao nazismo. "Tem muita coisa a mais, incluindo corrupção de menores", garante o policial.

Não durou muito

Infelizmente, como todos nós bem sabemos, o Brasil ainda engatinha em relação a uma legislação mais firme contra crimes cibernéticos. E talvez seja por conta disso que, após poucos meses na cadeia, VandaTheGod conseguiu reaver sua liberdade no final de julho, enquanto esta reportagem era elaborada. Em seu perfil no



VandaTheGod
@VandaTheGod

▼

#PJL #hacktivist canto liberdade

11:53 AM · 24 de jul de 2020 · Twitter Web App

7 Retweets 30 Curtidas



Reprodução: Twitter/VandaTheGod

Tal fato, porém, não espanta. Lembra-se das extensas pesquisas de Zanatta a respeito do art. 154-A? O brasiliense encontrou um total de 41 casos de indivíduos e grupos indiciados por tal crime, e apenas um caso — uma invasão a um site ocorrida em 2017 — resultou em uma pena de dez meses de prisão.

Questionada sobre a soltura precoce, a equipe da Check Point afirma não estar familiarizada com o sistema judiciário brasileiro, mas diz que, "no geral, nós vemos os países fazendo progresso neste domínio, com mais forças policiais, legislações e agências especializadas em delitos cibernéticos". Zanatta, por outro lado, é bem mais direto: "Não pense que isso é liberdade. Ele ainda tem um problemão para resolver", garante.

Veremos.

Gostou dessa matéria?

Inscreve seu email no Canaltech para receber atualizações diárias com as últimas notícias do mundo da tecnologia.

Email

INSCREVER





O Privacy Badger substituiu esse Disqus widget

[Permitir uma vez](#)

[Sempre permitir neste site](#)

Linha Galaxy S21

Ofertas Canaltech



a partir de

R\$134⁸⁹

COMPRE UM TÊNIS OLYMPIKUS E LEVE OUTRO POR + R\$ 5,00 - Netshoes

+ ofertas desse produto





R\$109⁰⁰

em 3x sem juros

Fones de ouvido Bluetooth Redmi Airdots NO BRASIL!



R\$788⁶⁰

em 6x sem juros

Placa de Vídeo AFOX Radeon RX 560, 4GB DDR5 128 Bits, HDMI/DVI/D [INTERNACIONAL]





Carregador Portátil Power Bank 10.000mah - Compatível com todos os celulares

Home ■ Segurança

Ransomware segue como a maior ameaça digital no mês de maio

Por Roseli Andrion | Editado por Claudio Yuge | 10 de Junho de 2021 às 23h40

Elements/tommyandone

Um novo [ransomware](#) (malware usado por criminosos para sequestrar dados) foi o destaque das principais vulnerabilidades de maio. A conclusão é da ISH Tecnologia, especialista nos segmentos de cibersegurança, infraestrutura crítica e nuvens blindadas.

- [O que é ransomware e como se livrar dele](#)
- [Vulnerabilidade com mais de dez anos de idade é finalmente corrigida no Linux](#)
- [Ransomware: brasileiros pagam resgate, mas poucos conseguem reaver arquivos](#)

O DarkSide Ransomware Group é responsável por ataques que, nos últimos nove meses, somaram cerca de US\$ 90 milhões em Bitcoins. Foram eles que invadiram os sistemas do maior oleoduto dos EUA em maio. Em abril, aqui no Brasil, o Grup^o Moura foi vítima do mesmo ransomware.





[LER MAIS](#)

Home ■ Segurança

Falha de dia zero do Chrome é corrigida em pacote de atualização do Google

Por Roseli Andrion | Editado por Claudio Yuge | 10 de Junho de 2021 às 19h30

Divulgação/Google

Uma das vulnerabilidades mais conhecidas do Chrome foi contemplada na nova atualização de segurança da empresa. É uma falha do tipo dia zero (ou *zero day*) usada em diferentes ataques nas versões do navegador para Windows, MacOS e Linux.

- [Pesquisadores descobrem graves vulnerabilidades em conversores digitais](#)
- [Vulnerabilidade inédita é encontrada no Desktop Window Manager do Windows 10](#)
- [Como usar o Google Chrome](#)

Ela vem de um erro de digitação no motor [JavaScript](#) usado no Chrome e em outros navegadores baseados no Chromium. Com classificação de alta severidade, a vulnerabilidade foi descoberta por Sergei Glazunov, da equipe do Project Zero



STRESSED

[LER MAIS](#)

Home ■ Segurança

Alto volume de ciberataques tem levado equipes à sobrecarga emocional

Por Roseli Andrion | Editado por Claudio Yuge | 10 de Junho de 2021 às 17h30

Elements/wutzkoh

Com ataques cibernéticos cada vez mais frequentes, os profissionais de segurança da informação têm ficado emocionalmente sobrecarregados. É o que mostra um estudo da Trend Micro: o levantamento detectou que as equipes de Centros Operacionais de Segurança e de Tecnologia da Informação têm enfrentado níveis altos de estresse em razão do excesso de alertas.

- [Voilá AI Artist | Será que o app que transforma selfie em desenho é seguro?](#)
- [Ciberataque à JBS: dados de operações brasileiras podem ter sido comprometidos](#)
- [Atenção: estes são os 6 principais golpes envolvendo o Pix](#)





Segundo a pesquisa, 70% deles são afetados emocionalmente no trabalho em razão do gerenciamento de ameaças.

A maioria (51%) sente que a equipe está sobrecarregada, enquanto 55% admitem que não têm confiança em sua capacidade de priorizar e responder aos alertas. Nesse cenário, as equipes gastam até 27% do tempo lidando com falsos positivos.

Um estudo recente da Forrester chegou à mesma conclusão. Segundo o documento, "as equipes de segurança têm pessoal insuficiente para responder a incidentes, mesmo quando enfrentam um aumento no número de ataques".

[LER MAIS](#)

[Home](#) ■ [Produtos](#) ■ [Notebook](#)

Notebooks perfeitos para trabalhar em home office

Por Redação | 03 de Junho de 2021 às 09h00

Rafael Damini/Canaltech

PUBLIEDITORIAL



[Tudo sobre Intel](#)

[VER MAIS](#)

A pandemia do novo coronavírus (SARS-CoV-2) pegou muitas pessoas desprevenidas, principalmente por elas se verem tendo de trabalhar de casa co-



produtividade vai por agua abaixo.

Se você está passando por esse sufoco e está há algum tempo buscando qual máquina comprar, certamente é porque está em dúvida sobre quais os melhores notebooks para trabalhar em home office. As opções são diversas, isso é verdade, mas apenas laptops equipados com os processadores Intel Core de 11ª geração vão atender todas as suas necessidades.

Não importa se o trabalho é básico ou complexo, existe um notebook equipado com Intel Core de 11ª geração perfeito para você fazer coisas incríveis. Ao todo, são mais de 150 modelos de laptops diferentes que atendem desde professores e estudantes até criadores de conteúdo e designers onde quer que eles queiram trabalhar. Ainda assim, fica a dúvida: qual exatamente é o modelo feito para você?

[LER MAIS](#)













