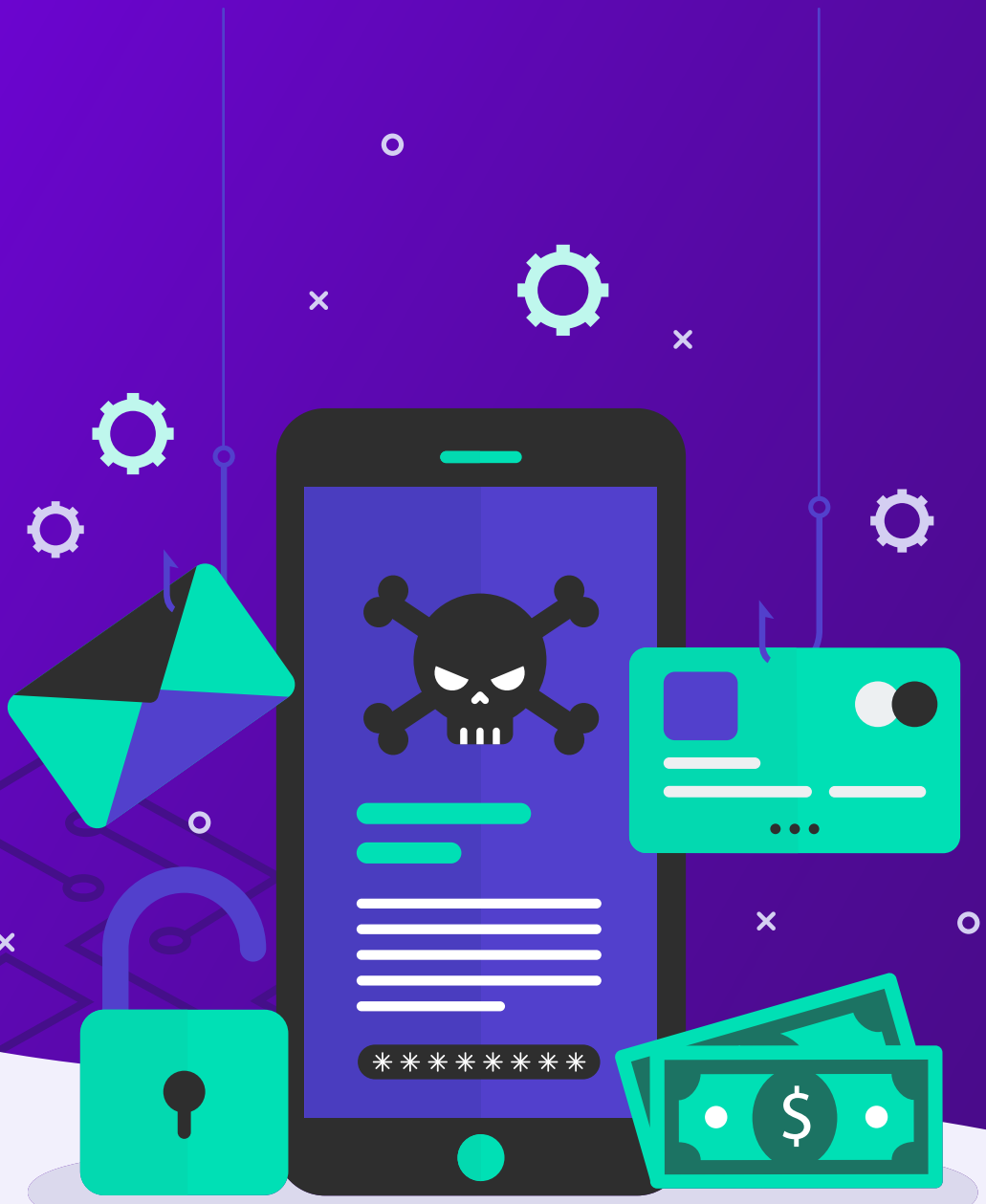
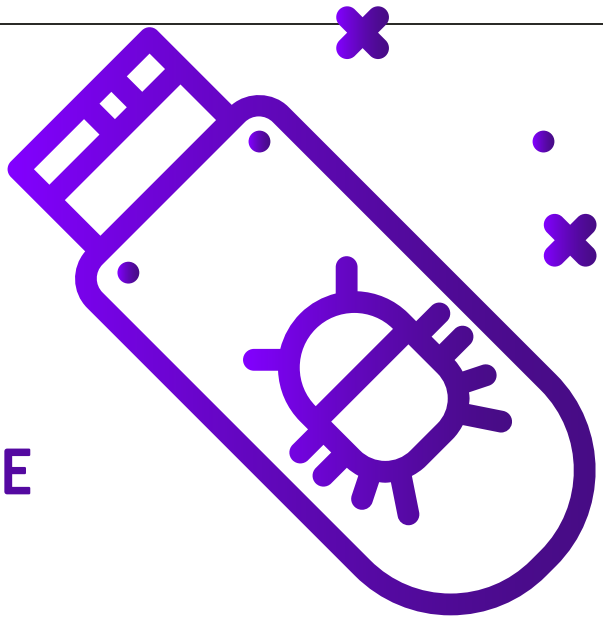
WALLINSON OLIVEIRA SCHUTTE

HISTÓRIA COMPLETA VÍRUS DE COMPUTADOR



SUMÁRIO



O QUE É UM VÍRUS DE COMPUTADOR?

As pessoas gastam grande parte do tempo online, seja na sua vida pessoal ou profissional. **Mas o mundo online está cheio de ameaças cibernéticas que podem causar problemas irreparáveis a usuários desprotegidos.** Não apenas financeiramente, mas pessoalmente. É por isso que começamos nossa jornada pela história dos vírus de PCs entendendo, primeiramente, o que é uma das maiores ameaças cibernéticas da atualidade.

Apesar de serem muito conhecidos, existem usuários da internet que ainda não sabem como funciona exatamente o grande problema dos vírus de computador que afeta milhões.

Eles são softwares extremamente peculiares que possuem comportamentos que se assemelham aos vírus biológicos. Esse, inclusive, era um dos preceitos desenvolvidos pelos seus criadores: apresentar condutas similares aos dos vírus biológicos. Basicamente, eles buscam se aproveitar das fragilidades dos sistemas de computador e de celular para extorquir as vítimas de alguma forma. E tudo isso, logicamente, violando as leis e termos de serviços dos provedores do mundo todo.

Existem diversas formas de ataque por vírus. Um exemplo são os Worms. Os tipos mais novos desse vírus incluem um backdoor (uma porta que libera o acesso para o vírus propriamente dito). Mais tarde, quando o número de pessoas infectadas com ele é grande, você nota um tráfego estranho indo até ele. Esse tráfego, na verdade, são comandos para enviar SPAM ou derrubar um site específico.

A MAIORIA DAS AMEAÇAS AO COMPUTADOR INCLUI MALWARE, SPYWARE, ADWARE, PHISHING, VÍRUS, CAVALOS DE TRÓIA, WORMS, ROOTKITS, RANSOMWARE E SEQUESTRADORES DE NAVEGADOR. COM ESSAS ARMAS, HACKERS PODEM ACESSAR SUAS SENHAS E INFORMAÇÃO DE CARTÃO DE CRÉDITO, TRAVAR COMPUTADORES E EXIGIR RESGATE PARA LIBERÁ-LOS, DELETAR DADOS PESSOAIS, DEIXAR O PC LENTO E MUITO MAIS.

A PERGUNTA SEGUINTE É:

VOCÊ **ESTÁ MESMO PROTEGIDO CONTRA ESSA GRANDE QUANTIDADE DE AMEAÇAS**?

SABE COMO PODE SER INFECTADO E COMO SE PROTEGER? COMO ESCOLHER UM BOM ANTIVÍRUS?

Se a sua resposta for não, ou pior, que para escolher um antivírus basta baixar qualquer um.... Sinto em lhe dizer que você pode ser infectado a qualquer momento. Os vírus de computador podem se infiltrar não apenas em e-mails e spam, mas também em arquivos Word, links de WhatsApp e downloads que você faz na internet.

Preocupante, certo?

Neste ebook em específico vamos tratar de como esses vírus evoluíram com o passar do tempo. Mas caso você deseje saber um pouco mais a fundo sobre quais os tipos de ameaças mais comuns hoje em dia, temos uma ótima solução para você.

Imagine um manual que te dá os nomes dos principais tipos de vírus da atualidade e uma forma de lidar com eles? **Esse é o Manual Completo do Vírus de Computador!**

Você pode resolver de forma simples até ameaças que parecem não ter solução (como é o caso do vírus Ransomware que criptografa todos os seus arquivos). Além disso, te damos um panorama importante de como escolher um bom antivírus (sim, não é só baixar qualquer um.) Após a leitura do manual, você terá todas as ferramentas possíveis para combater ativamente qualquer vírus que entre em contato com o seu computador!

CLIQUE E DESCUBRA!

HTTPS://WWW.DOUTORPW.COM

#1 HISTÓRIA DOS VÍRUS DE COMPUTADOR

AGORA, **VAMOS ENTRAR NUMA VERDADEIRA MÁQUINA DO TEMPO** E PROCURAR OS PRIMEIROS VESTÍGIOS DO QUE SE TORNARIA HOJE O VÍRUS DE COMPUTADOR MODERNO.

1949

Começamos nossa jornada em 1949, quando o matemático John Von Neuman publicou seu artigo Theory and Organization of Complicated Automata. Nele, o cientista falava sobre "um código capaz de reproduzir a si mesmo". Como sabemos hoje, essa é uma das características do vírus: a sua capacidade de reprodução autônoma. O artigo, na verdade, foi uma experiência teórica sobre a possibilidade de um organismo "mecânico", como um código de computador, danificar máquinas, se copiar e infectar novos hospedeiros da mesma forma que um vírus biológico.

1950

Após essa primeira citação, em 1950 começam as guerras de núcleo (Core Wars 4). Os investigadores de inteligência artificial dos laboratórios Bell, H. Douglas Mcllroy, Victor Vysottsky e Robert Morris Jr. descobrem programas hostis chamados RedCode que poderiam crescer na memória da máquina e lutar entre si.

1970 - 1980

Já no ano de 1970, Bob Thomas criou um programa denominado Creeper, que foi usado pelos controladores de tráfego aéreo para acessar e ceder o controle de uma aeronave entre os terminais. Neste mesmo estilo, para ter controle da troca de mensagens em tarefas automáticas durante o período noturno da empresa Xerox, os investigadores John Shock e Jon Hupp espalharam um tipo de programa worm em 1980. O programa acabou agindo de forma descontrolada e foi eliminado pelos seus criadores.

1982-1984

Passados 2 anos, em 1982, um programador de apenas 15 anos chamado Ricj Skrenta criou o primeiro código "malicioso" para Apple 2 em DOS. Colocamos aspas no malicioso porque, no fim, o código não fazia mal algum. Ele apenas exibia uma poesia do autor caso executadas algumas funções.

Além disso, as primeiras menções acadêmicas ao nome vírus de computador aconteceram em 1983, quando o pesquisador Fred Cohen nomeou esses programas maliciosos de "Vírus de Computador", por sugestão do seu orientador de TCC. Por fim, o termo é aceito em 1984 na 7th Annual Information Security Conference para programas que infectam outros sistemas e produzem cópias de si mesmos.

1986-1987

MAS FOI EM 1986 QUE SURGE, DE FATO, O PRIMEIRO VÍRUS DA HISTÓRIA.

O Brain, que era um vírus de boot, danificava o setor de inicialização do disco rígido e se propagava através de disquetes contaminados.

No ano seguinte foi criado o vírus Vienna. A cada execução ele infectava arquivos com extensão COM. Ele aumentava o tamanho do executável em 684 bytes. Os programas infectados não tinham uma cópia do vírus e só tinham suas funções alteradas. Na mesma época foi criado o ThusFix que neutralizava o Vienna, porém ele não foi considerado um antivírus e sim somente uma correção.

1992

Na época dos primeiros malwares, ainda não exitiam muitas menções na mídia sobre esse novo tipo de ameaça. Porém, em 1992, o vírus Michelangelo mudou este cenário. Ele sobrepunha partes do disco e criava diretórios e arquivos falsos no dia 6 de março. Essa, para os leigos, é a data do aniversário do artista renascentista Michelangelo. Esse vírus começou a preocupar muitos grandes escritórios que precisavam proteger os seus arquivos do ataque. Assim, houve uma explosão na venda e divulgação dos antivírus.

1995-1998

Apesar de ataques grandes já terem acontecido, foi apenas em 1995 que uma prisão para este tipo de crime aconteceu. Rastreado pela Scotland Yard, o criminoso cibernético Cristopher Pile, conhecido como Barão Negro, foi condenado a 18 meses de prisão pela criação do vírus Pathogen. Mais do que merecido, já que o estrago que o vírus provocou foi de quase 2 milhões de dólares e meio. As acusações iam desde invasão a computadores até modificações não autorizadas de software e uma acusação de incitação a propagar seu vírus.

Juntamente com a primeira prisão, novos vírus estavam sendo criados e assim surgiu o Concept, primeiro do tipo de vírus de macro, escrito para afetar o Word em Basic.

Três anos depois, em 1998, o vírus "Chernobyl" é criado e pode paralisar o hardware do computador atacando o BIOS (necessário para inicializar um PC). O primeiro vírus deste tipo a ser desenvolvido.

2003

Já em 2003 é criado o "Cabir", o primeiro vírus para telefone. Desenvolvido para infectar celulares rodando o sistema operacional Symbian, este malware pode se espalhar para outros telefones via Bluetooth.

2007

Com o passar do tempo e a evolução da tecnologia, novos tipos de vírus começaram a se desenvolver. Além disso, os códigos maliciosos que já tinham sido criados evoluíram para se tornarem ameaças piores.

Mas não só as formas de vírus evoluíram, as estratégias para convencer os internautas a baixarem arquivos maliciosos também se modificaram e se adaptaram a mentalidade dos novos tempos. Com isso, houve um aumento significativo dos vírus em redes sociais com chamadas que atraiam a vítima a clicar. O desenvolvimento de novas técnicas de engenharia social acabava por fazer o usuário se infectar e enviar mensagens contaminadas a todos os que estavam com ele nas redes sociais.

2010 - FUTURO

Desde o surgimento do primeiro vírus de computador em 1986 até o dia de hoje, calcula-se algo em torno de 100.000 a 150.000 vírus existentes, segundo os catálogos de produtos antivírus mais completos.

Além da quantidade, encontramos hoje em dia uma ameaça muito mais sofisticada. Devemos lembrar que a Internet das Coisas permite o controle de aparelhos reais, como carros e outros. Em 2010 surge o Stuxnet, que pode manipular máquinas de produção em linha e outros tantos aparelhos, como, por exemplo, brinquedos de parques de diversão e até mesmo uma centrifuga para separar material nuclear.

VOCÊ CONSEGUE IMAGINAR O TAMANHO DA AMEAÇA QUE UM VÍRUS DESSE PODE CAUSAR?

#2 POR QUE OS VÍRUS SURGIRAM?

Existem alguns fatores chaves que apontam para o surgimento dos vírus na década de 80. Vamos entender alguns deles abaixo.

1) AUMENTO DOS COMPUTADORES PESSOAIS

Antes da década de 80 as pessoas não tinham muitos computadores dentro de casa. Eles eram artigos raros e tinham o seu uso restrito aos profissionais da área. Foi apenas nos anos 80 que essas máquinas começaram a fazer parte da vida nos escritórios e nas casas devido à popularidade do IBM PC (lançado em 1982) e do Apple Macintosh (lançado em 1982 e 1984).

2) BULLETIN BOARDS

Os bulletin boards permitiam a discagem do modem e através dessa discagem, o download de programas de todos os tipos. Jogos eram muito populares, assim como processadores de textos, planilhas, etc. Os buletins boards conduziram ao precursor dos vírus conhecidos como cavalo de tróia.

3) DISCO FLEXÍVEL

Na década de 80, os programas eram pequenos e podiam ser armazenados em 1 ou 2 discos flexíveis. Muitos computadores não tinham discos rígidos e todo o processo desde a inicialização da máquina até a execução de programas era feito com discos flexíveis. Os criadores de vírus tiraram proveito desses três fatores para criar o primeiro programa de auto replicação.

#3 POR QUE CRIAR VÍRUS DE COMPUTADOR?

Neste ponto do ebook você deve estar se perguntando: Porque resolvemos criar uma ameaça do gênero? Por qual razão alguém se esforçaria tanto para invadir seu computador ou dispositivo móvel? Bem, pare e pense no tipo de gente que se torna criador de malware... e que vantagem eles levam com essa atividade. Hoje em dia fazemos praticamente tudo através da internet, dos nossos computadores e dos nossos celulares. Além disso, a venda de dados para empresas é um negócio extremamanete lucrativo.

A ERA ROMÂNTICA DOS CRACKERS QUE FAZIAM MANOBRAS PELO PURO PRAZER DE SE SUPERAR FICOU NO PASSADO. HOJE, A MAIOR PARTE DOS INVASORES TEM UM OBJETIVO DEFINIDO: ROUBAR DADOS.

Acrescentando ainda, conforme a Anti-Phishing Working Group, APWG, que 93,5% das instituições financeiras mundiais já foram atacadas. Os bancos só não divulgam isto individualmente para não alimentar vulnerabilidades e, também, para não enfraquecer sua competitividade mercadológica.

É triste a constatação de que, mais cedo ou mais tarde, indivíduos mal-intencionados descobrirão um jeito de explorar praticamente qualquer invenção ou nova tecnologia com a intenção de causar danos ou lucrar. O uso legítimo dos computadores, dispositivos móveis e da Internet cresceu na mesma proporção que as oportunidades que vândalos, trapaceiros, chantagistas e outros criminosos têm de tirar proveito da criação de vírus, worms, cavalos de Troia e outros tipos de malware.

#4 A CRIAÇÃO DOS ANTIVÍRUS

É CLARO QUE QUANDO AS AMEAÇAS COMEÇARAM A FICAR CADA VEZ MAIS COMUNS, OS PESQUISADORES DA ÁREA COMEÇARAM OS PREPARATIVOS PARA PROTEGER AS MÁQUINAS E REDES DOS VÍRUS DE COMPUTADOR.

Foi então que em 1988 o primeiro antivírus foi criado por Denny Yanuar Ramdhani. Especialmente feito para combater o Brain, ele removia as entradas do vírus e imunizava contra novos ataques. A forma de desinfetar era remover as entradas do vírus no PC e já bloquear as fraquezas para impedir um novo ataque.

Porém, apenas em dezembro de 1990 iniciou-se uma grande entrada das empresas de tecnologia no ramo de antivírus. Alguma das mais famosas eram: Symantec, McAfee, IBM e Kaspersky.

Após esse primeiro antivírus que atacava apenas ao Brain, surgiram os primeiros programas antivírus que possuíam uma base de dados, apoiado na ideia de que o os vírus eram muito simples e de código praticamente idêntico e que todos seguiam o mesmo ciclo de vida.

Com o passar do tempo, porém, os vírus foram se modificando e os antivírus precisaram se manter a altura deles. Surgiram então os primeiros antivírus que combatiam uma praga recente dessas ameaças digitais: o polimorfismo. Esses novos antivírus implementavam uma simples rotina de criptografia que decifrava o restante do corpo do vírus sempre que este fosse executado.

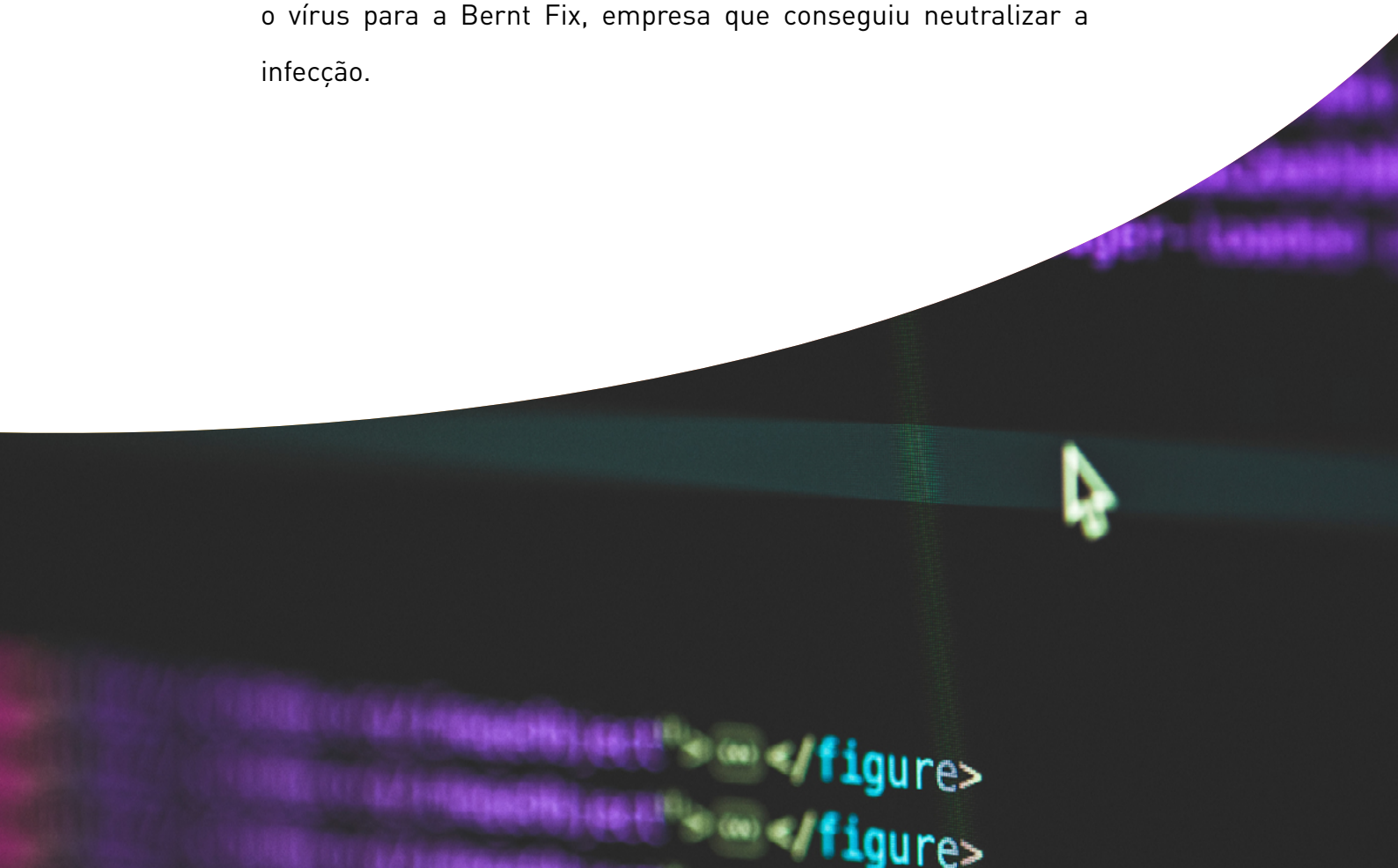
HOJE EM DIA, AS TÉCNICAS DE USO DE "ANÁLISE HEURÍSTICA" SÃO BASTANTE DIFUNDIDAS NOS ANTIVÍRUS DO MERCADO; POIS NÃO IMPORTA SE O CÓDIGO DO VÍRUS FOI MASCARADO OU CRIPTOGRAFADO, **PODE-SE DETECTAR UM VÍRUS POR SEU COMPORTAMENTO DANOSO, O QUE É MUITO MAIS EFICIENTE QUE A BUSCA POR SEQUÊNCIA DE INSTRUÇÕES.**

#5 OS PIORES VÍRUS DA HISTÓRIA

Agora que sabemos um pouco mais sobre a história dos vírus e antivírus, que tal darmos uma olhada em como eles foram evoluindo com alguns dos nomes mais comentados dessas ameaças cibernéticas? Vamos explorar agora os piores vírus de cada época!

VÍRUS VIENNA (1987):

Criado pelo estudante Rolf Burger da cidade de Viana, na Áustria, este vírus infectava programas cada vez que era executado. Os programas em si não possuíam o vírus, mas tinham seu código alterado por ele, o que fazia com que o computador começasse a se reiniciar continuamente até que todos os programas fossem substituídos por cópias não contaminadas. Rolf Burguer mandou o vírus para a Bernt Fix, empresa que conseguiu neutralizar a infecção.

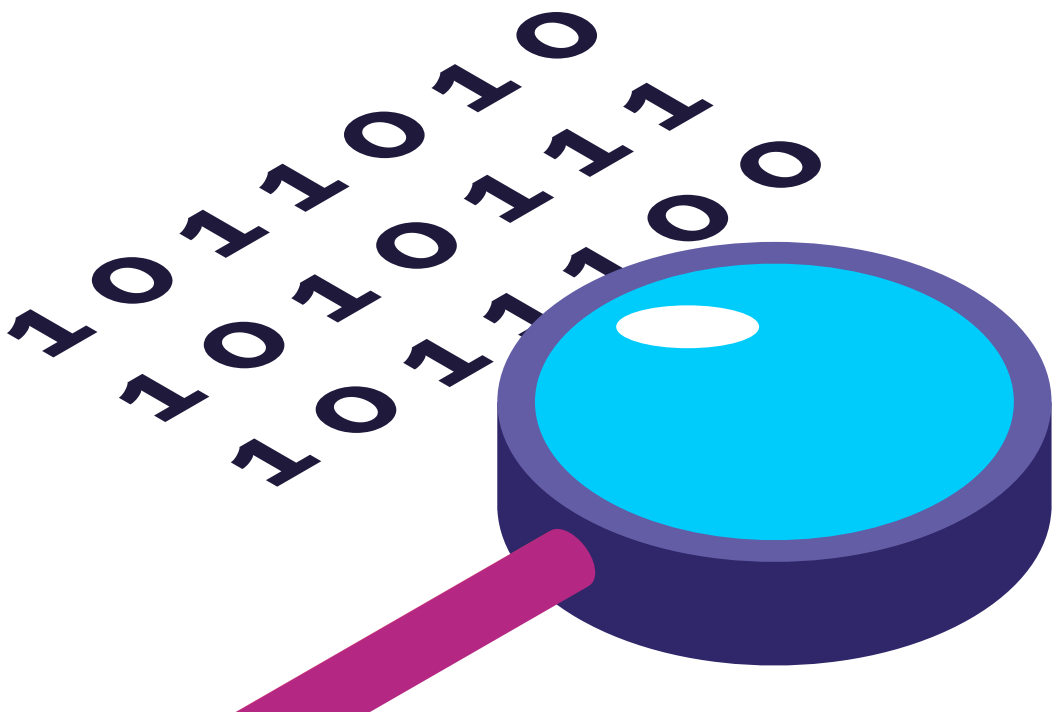


DARK AVENGER (1989)

Conhecido como Eddie (pseudônimo de um famoso escritor de vírus informático da Bulgária), o Dark Avenger foi o primeiro vírus a ter sido originado da Bulgária, no qual foi incorporado uma técnica nova conhecida como fast infector. Ele contaminava os programas rapidamente, mas o estrago subsequente acontecia bem devagar. A IBM foi a primeira a fornecer o antivírus comercial que protegia contra o Dark Avenger.

MICHELANGELO (1991)

O vírus Michelangelo infecta o setor de um disco rígido chamado Master boot Record e só entrava em atividade em 6 de março, no dia do aniversário do artista renascentista Michelangelo.



MORRIS (1988)

Um Worm lançado por Robert Morris que não tinha intenção maligna. Foi criado para tentar medir a extenção da internet, mas acabou causando um prejuízo entre 10 e 100 milhões de dólares. Sua falha era que ele infectava o mesmo computador diversas vezes, causando DOS (Denial of Service).

CIH/CHERNOBYL (1998)

Lançado em Taiwan em junho, o CIH infectava Windows 95, 98 e arquivos executáveis do ME. Se escondia na memória do computador e podia sobrescrever dados no HD, tornando-o inoperante. O vírus deixou de ser maligno depois da grande migração dos usuários para Windows 2000, XP e NT, que não são vulneráveis a ele. Os danos do Chernobyl foram estimados na casa dos 20 a 80 milhões de dólares, fora a perda massiva dos dados dos usuários.

MELISSA (1999)

Um vírus criado a partir do nome de uma dançarina, alvo da paixão do criador da ameaça, David L. Smith. O Melissa causou um prejuízo bilhonário e quando executado desligava todos os sistemas de e-mails por onde os e-mails infectados passassem.

CODERED (2001)

O CodeRed é um worm que utilizava uma vulnerabilidade dos servidores Microsoft IIS para se instalar e se replicar. Causou prejuízo de 2 bilhões de dólares e quando infectava a máquina desligava todos os sites armazenados no servidor e exibia a mensagem "Hacked by Chinese!".

SLAMMER (2003)

Este worm "desligou" a internet da Coreia do Sul por 12 horas. Utilizava um sistema de ataque que se aproveitava da mesma vulnerabilidade que o CodeRed, mas atacando agora o Microsoft SQL Server. Quando infectava algum sistema, causava Denial of Service fazendo com que o banco de dados não respondessem e causasse uma grande lentidão na internet.

NIMDA (2001)

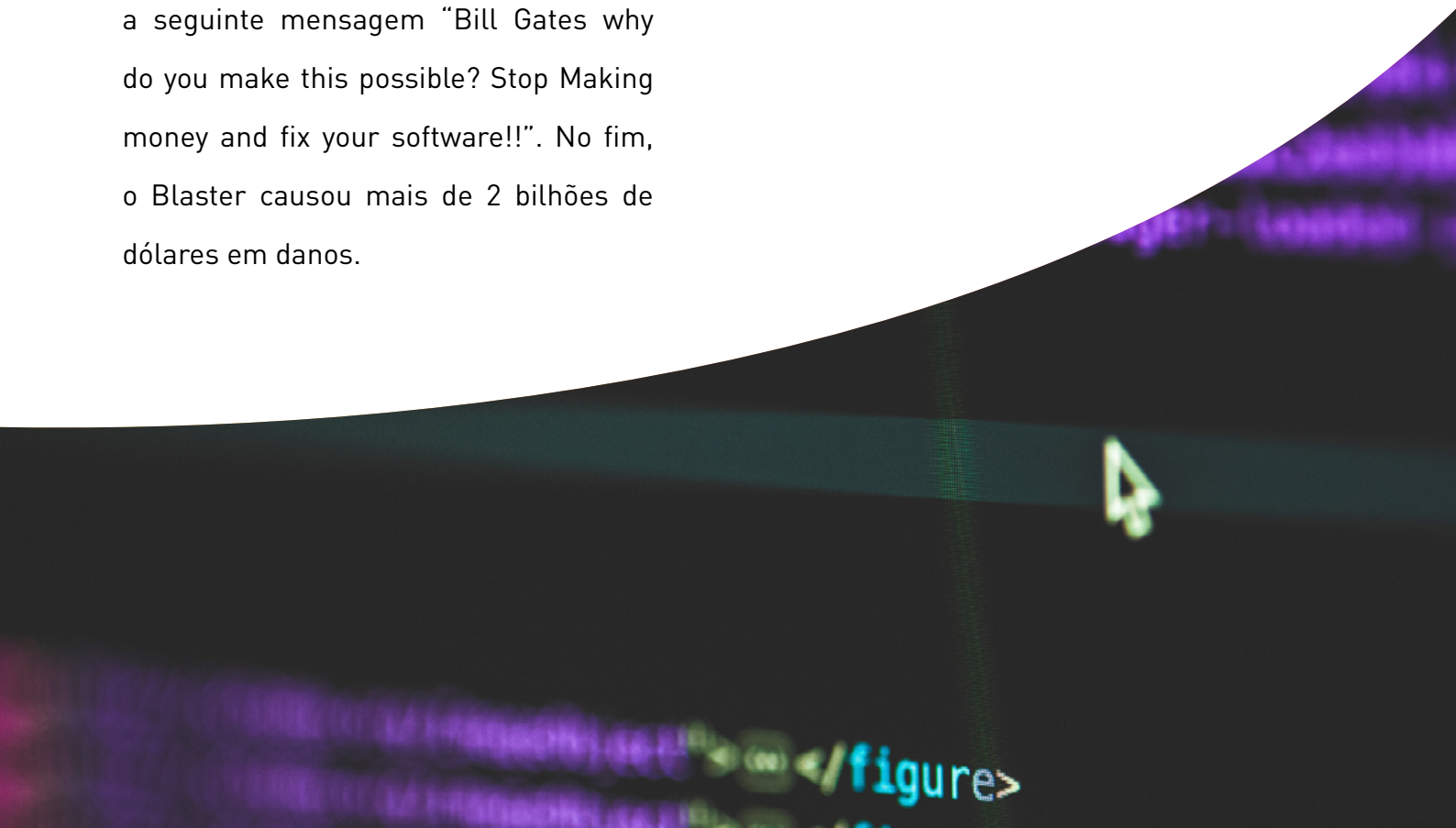
Não foi determinado qual o prejuízo causado por este worm. Haviam diversos métodos para espalhá-lo, por e-mail, rede, sites e backdoors feitos por outros vírus, causou muita lentidão na internet. Por conseguir se espalhar, ele foi considerado o worm mais rápido até o momento. Em apenas 22 minutos se tornou o vírus mais espalhado do mundo.

BLASTER (2003)

Foi criado pelo grupo hacker Xfocus com a intenção de atacar sistemas Microsoft Windows. Ele se espalhava com a seguinte mensagem "Bill Gates why do you make this possible? Stop Making money and fix your software!!". No fim, o Blaster causou mais de 2 bilhões de dólares em danos.

BAGLE (2004)

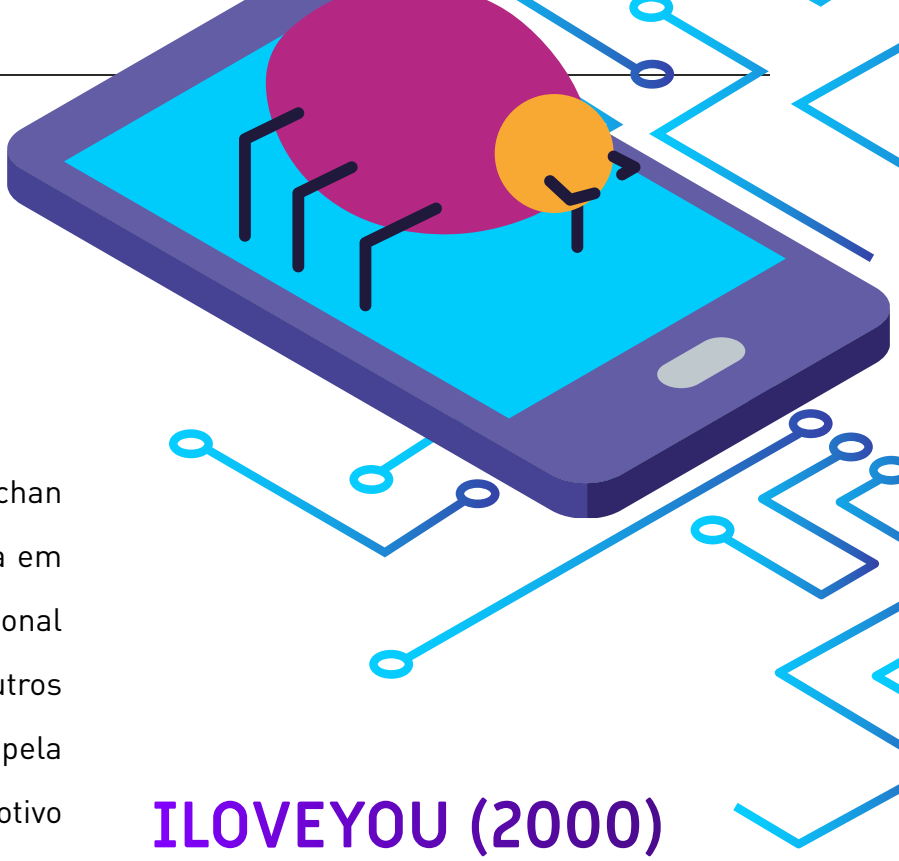
O Bagle é um worm mais sofisticado. Ele infectava os sistemas anexado a um e-mail e se propagava através de endereços de e-mail que pudesse utilizar para se replicar. O verdadeiro perigo é que, ao infectar o PC, ele abria uma porta que permitia o controle a distância do sistema. O Bagle parou de se espalhar depois de 28 de janeiro do mesmo ano, mas suas muitas variantes estão ativas até hoje. Isso acarretou em dezenas de milhões de dólares de prejuízo, um número que vem crescendo até hoje.



MYDOOM (2004)

Este worm é conhecido pela sua espantosa velocidade de propagação. Durante 4 horas no ano de 2004 ele se espalhou numa velocidade sem precedentes pela Internet. A praga, também conhecida como Norvarg, se espalhou em um arquivo anexado que parecia ser uma mensagem de erro com o texto "Mail transaction failed", e via compartilhamento de arquivos entre os usuários da rede P2P Kazaa. A sua autocópia era tão rápida que uma em cada dez mensagem de e-mail enviadas durante as primeiras horas da infecção continham o vírus. Essa ameaça cibernética foi tão letal que chegou a diminuir em 10% a performance global da Internet e aumentar o tempo de carregamento dos sites em 50%.

Após executado, o MyDoom destrói dados do HD.



SASSER (2004)

Um worm criado por Sven Jaschan atacou a vulnerabilidade de segurança em uma porta de rede do sistema operacional Windows que permitia a conexão com outros computadores. Assim, ele se espalhou pela internet. Porém, esse não foi o único motivo da sua grande fama. O Sasser acabou por infectar diversas empresas aéreas como a Delta Airlines, que por se infectar com o vírus teve que interromper os voos.

STORM (2007)

Mais um worm que dessa vez propagava notícias sensacionalistas , como, por exemplo, "Genocídio de muçulmanos britânicos" ou "Fidel Castro faleceu". O Storm construiu uma verdadeira "botnet", utilizava os computadores infectados para realizar ações programadas pelo worm, como ataques a sites específicos.

ILOVEYOU (2000)

O conhecidíssimo vírus ILOVEYOU trouxe problemas e prejuízos ao redor do mundo. Foi o responsável por 5,5 a 8,7 bilhões dólares de danos. O seu ataque é conhecido pela engenharia social envolvida. O vírus atacava os usuários mandando uma simples mensagem de uma confissão de amor. Os usuários curiosos clicavam e executavam o vírus. Em maio de 2000, por volta de 50 milhões de computadores foram infectados, incluindo órgãos dos governos de todo o mundo. Vários deles, como a CIA, tiveram que desligar o sistema de e-mails para diminuir a ameaça.

HEARTBLEED (2014)

Diferente dos outros vírus, o Heartbleed surgiu a partir de uma vulnerabilidade do OpenSSL, uma biblioteca criptográfica geral de código aberto usada por empresas do mundo todo. O OpenSSL envia "heartbeats" (pulsações) periodicamente para garantir que os endpoints seguros continuam conectados. Os usuários podem enviar ao OpenSSL uma quantidade específica de dados, depois solicitar o mesmo volume de volta. Por exemplo, um byte. Se os usuários alegarem que estão enviando o máximo permitido, 64 KB, mas enviarem somente um byte, o servidor responderá com os últimos 64 KB de dados armazenados na RAM, observa o tecnólogo de segurança Bruce Schneier, podendo incluir de tudo, desde nomes de usuários até senhas de chaves de criptografia.

WANNACRY (2017)

O ataque ao ransomware WannaCry se espalha globalmente. As explorações reveladas no vazamento do kit de ferramentas de hackers da NSA do final de 2016 foram usadas para permitir a propagação do malware. Logo após a notícia online das infecções, um pesquisador de segurança cibernética do Reino Unido, em colaboração com outras pessoas, encontrou e ativou um "interruptor" oculto no ransomware, interrompendo efetivamente a onda inicial de sua propagação global. No dia seguinte, os pesquisadores anunciaram que haviam encontrado novas variantes do malware.

As ameaças são muitas e entende-las a fundo é importantíssimo. Mas, mais do que isso, é preciso saber se defender contra todos esses tipos de vírus que podem estar em funcionamento até os dias atuais.

Além da grande variedade de vírus que atacam o seu PC, existem hoje em dia muitos casos de criptografia de arquivos, em que é solicitado uma quantia de dinheiro para a recuperação. Esse tipo de ataque geralmente é causado pelo vírus Ransomware e pode causar prejuízos milhonários. Nesse tipo de situação, há algumas ferramentas específicas para a descriptografia.

Existem inclusive diversos vírus que contaminam Pen Drives e outros dispositivos externos e que, mesmo com bons antivírus, são de difícil remoção. Eles acabam retornado por não serem removidos completamente. Nesses casos citados, um dos Softwares que recomendamos é o PW Clean.

O PW Clean é um antivírus com 5 anos de mercado. Dentre suas funções estão a remoção da maioria dos Vírus que criam atalhos e ocultam as pastas do seu dispositivo (Pen Drives, HD Externos, Cartões de Memória, etc.). Além de manter o seu computador protegido e desinfectado, ele impede que seu(s) dispositivo(s) sejam contaminados novamente e conta com diversas ferramentas para a manutenção saudável do seu computador (limpeza de arquivos temporários e finalização de processos.

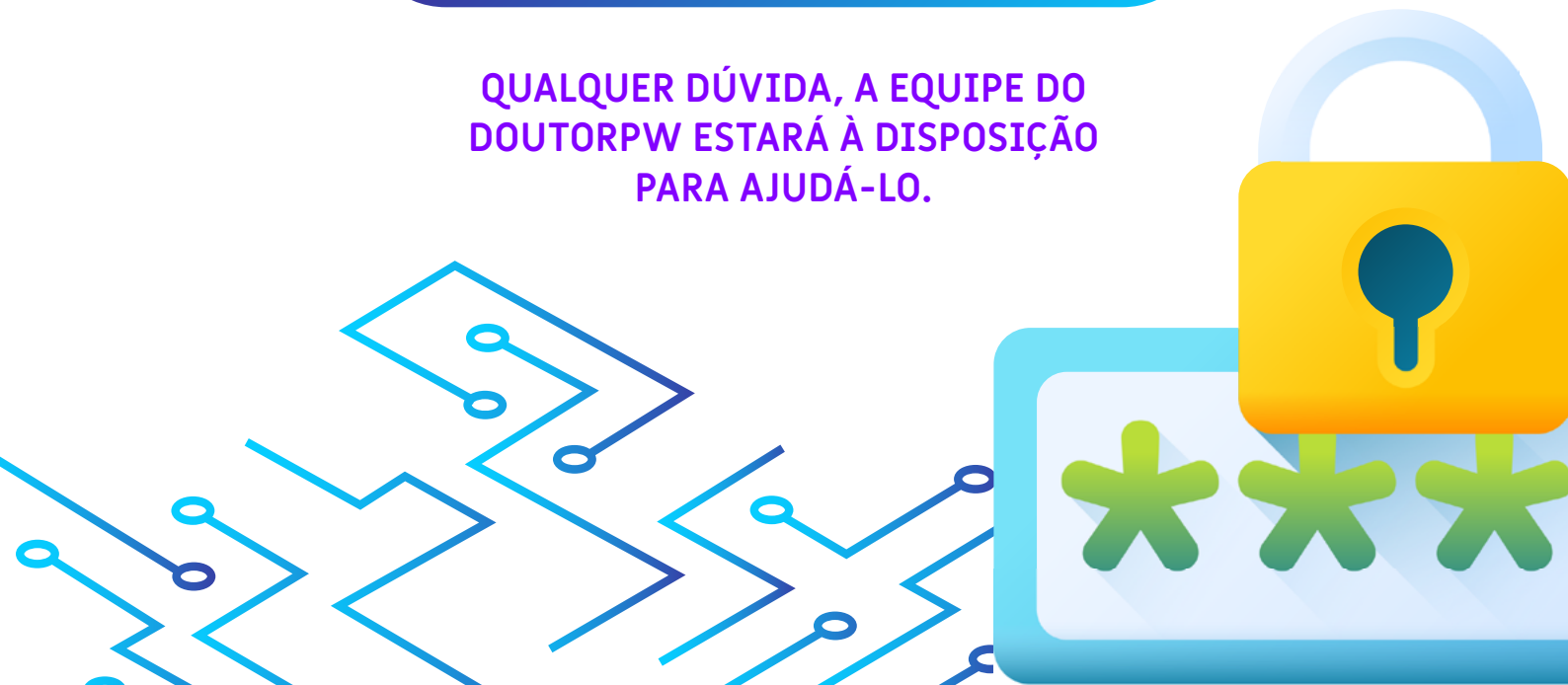
São diferentes funcionalidades, uma proteção eficaz e ativa contra vírus e uma interface de fácil utilização. Assim, você mesmo, com apenas alguns cliques, conseguirá livrar seu sistema e seus dispositivos desses terríveis malwares.

Para testar todas essas funcionalidades e muito mais, é possível baixar a versão limitada e fazer um teste gratuito.

Lembre-se que manter um antivírus de qualidade é uma segurança necessária para todos os seus documentos.

CLIQUE E DESCUBRA!
HTTPS://WWW.DOUTORPW.COM

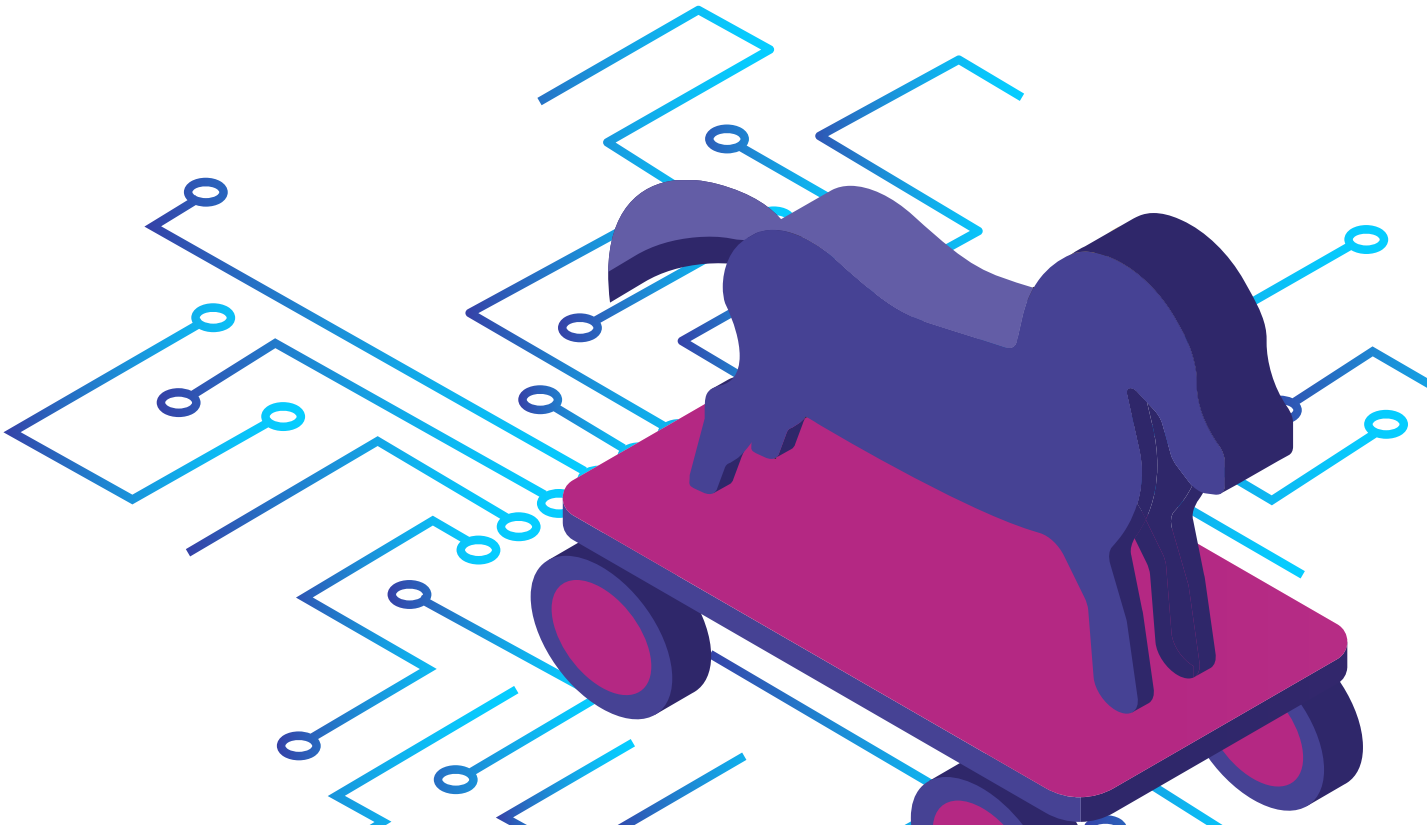
QUALQUER DÚVIDA, A EQUIPE DO DOUTORPW ESTARÁ À DISPOSIÇÃO PARA AJUDÁ-LO.



#6 CURIOSIDADES SOBRE OS VÍRUS

O PRIMEIRO CAVALO DE TROIA

O primeiro Cavalo de Tróia da história se chamava ANIMAL e foi desenvolvido pelo programador John Walker em 1975. Nessa época, estavam em alta os "programas de animais". Nele, o programa tentava adivinhar em qual animal o usuário está pensando em um jogo de 20 perguntas. A versão que Walker criou teve altíssima demanda e, para enviá-la aos amigos, era necessário gravar e transmitir fitas magnéticas. Para facilitar as coisas, Walker criou o PREVADE, que se instalava junto com o ANIMAL. Durante o jogo, o PREVADE examinava todos os diretórios do computador disponíveis ao usuário e depois fazia uma cópia do ANIMAL nos diretórios em que ele ainda não estava presente. Não havia um objetivo malicioso, mas o ANIMAL e o PREVADE se enquadravam na definição de cavalo de Troia: havia no ANIMAL um outro programa oculto que realizava ações sem a aprovação do usuário.



CASINO, UM JOGO EM QUE VOCÊ SÓ PODE PERDER

O vírus Casino copia o File Allocation Tables (FATs) para a memória RAM, deleta o FAT do disco rígido e força o usuário a jogar roleta para salvar seus arquivos. Independentemente do usuário ganhar ou perder, o computador desliga e o usuário é obrigado a reinstalar o DOS.

WALKER

Walker é um vírus benígno residente na memória que infecta arquivos COM e EXE quando eles são executados. O vírus Walker verifica as teclas e, às vezes, mostra um homem em movimento do vídeo game Bad Street Brawler. Em alguns casos, o vírus se auto-remove de arquivos infectados.

KUKU VIRUS

Kuku reescreve e infecta arquivos, desabilitando o teclado e enchendo a tela com títulos coloridos que dizem “Kuka!”.

LSD

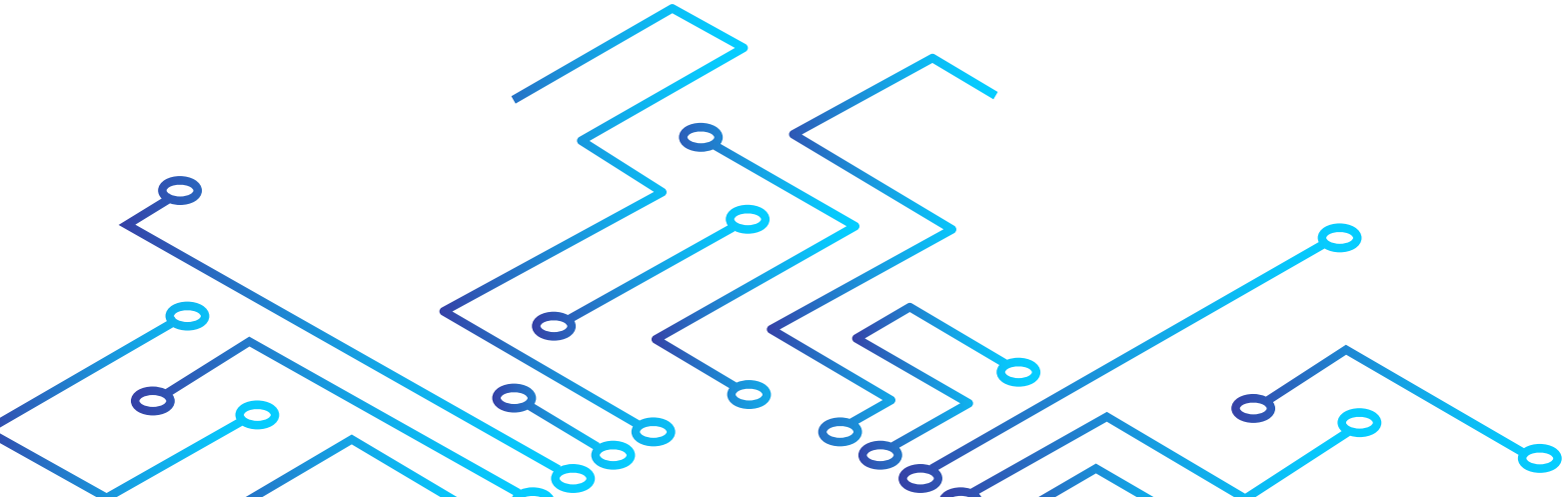
LSD é um vírus parasita não residente na memória muito perigoso que reescreve sobre todos os diretórios atuais de arquivos e manifesta-se com um efeito gráfico.

#7 O FUTURO DOS VÍRUS

Há mais de 60 anos os vírus de computador fazem parte da consciência coletiva, mas o que antes era simples vandalismo cibernético acabou se transformando rapidamente em crime virtual. Os worms, cavalos de Troia e vírus estão evoluindo. Os hackers são inteligentes e entusiasmados, e estão sempre dispostos a superar os limites de conexão e do código para desenvolver novos métodos de infecção. O futuro do crime virtual parece envolver mais invasões a PDVs (pontos de venda) e, talvez, o recente cavalo de Troia de acesso remoto Moker seja um bom exemplo do que está por vir. Esse malware recém-descoberto é difícil de detectar e de remover, e contorna todas as defesas conhecidas. Não existem certezas. A mudança é a alma dos ataques e das defesas.

ALÉM DISSO, AGORA FAZER VÍRUS E WORMS É UM MERCADO.

Agora a tática dos programadores é fazer dinheiro. Tudo que você precisa fazer é instalar um programa. Esse programa possui um afiliado. O afiliado faz a praga digital, que é incluída no programa que você queria instalar. Onde queremos chegar é que o afiliado desse programa faz dinheiro.

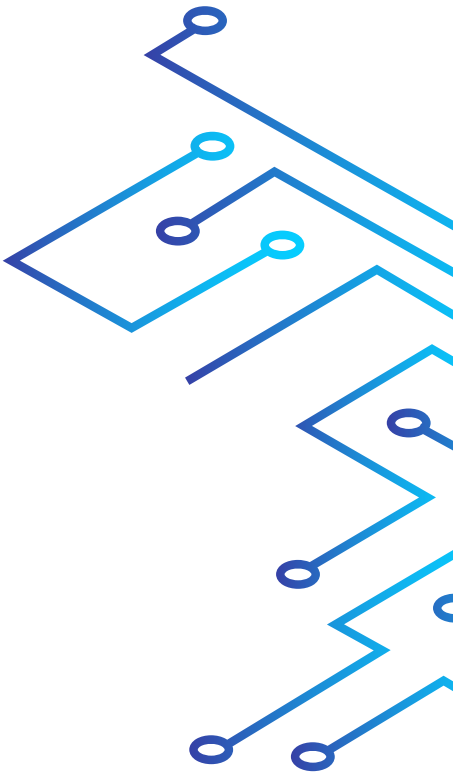


O afiliado inclui um programa junto com o programa original que faz algo que o usuário não quer, portanto, com objetivos duvidosos. Esse novo tipo de problema não recebeu muita atenção. Não eram destrutivos, apenas comerciais. Tantos outros programas servem para fazer dinheiro— eles são apenas mais alguns.

Mas rapidamente começou se tornar uma praga séria. Propagandas de produtos em pop-ups intrusivos faziam com que milhares de usuários ficassem aborrecido . Certas empresas estavam reclamando do momento em que as propagandas apareceriam. Processos começaram a serem jogados contra essas empresas que faziam as pragas.

Os antivírus ainda não davam atenção. Foi aí que surgiu o Adware. Os usuários, além do antivírus, deviam instalá-lo para remover esse tipo de problema. A popularidade do Adware subiu muito. Hoje, ele detecta mais de vinte e cinco mil pragas diferentes.

Têm alguém ganhado dinheiro com aquele programa que você instalou gratuitamente. Mas você não pagou, seu computador é que paga. Lembre-se: eles querem seu computador, não você. E embora eles façam o que quiserem com o seu computador, eles estão dentro da lei.



WALLINSON OLIVEIRA SCHUTTE

PÁGINA: HTTPS://WWW.DOUTORPW.COM.BR

INSTAGRAM: @WALLINSON.OLIVEIRA

E-MAILS: DOUTOR.PW@HOTMAIL.COM OU
CONTATO@DOUTORPW.COM.BR

CANAL NO YOUTUBE: HTTPS://WWW.YOUTUBE.COM/CHANNEL/
UCFUP4NJHLMQJCL-IB8FHHYW

PÁGINA DO PW CLEAN: HTTPS://WWW.DOUTORPW.COM/
SOLUCOES/PW-CLEAN

APRESENTAÇÃO DO PW CLEAN: HTTPS://WWW.YOUTUBE.COM/
WATCH?V=STMQHNRQXW8&T=1S