ptsoc digest

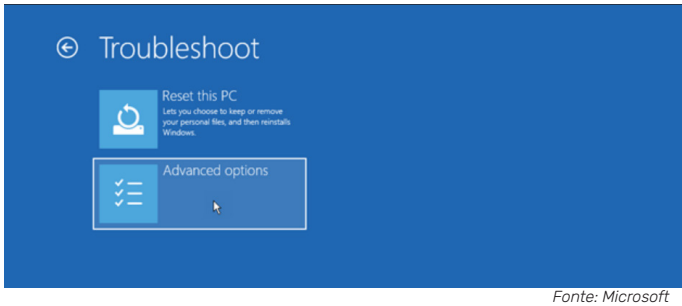
agosto 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt

ptsoc
Centro de Operações de Segurança

Os 10 dias que abalaram a CrowdStrike



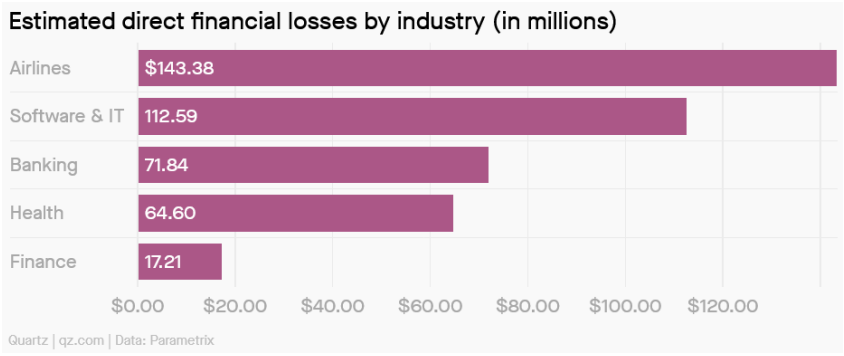
Fonte: Microsoft

A empresa de cibersegurança CrowdStrike só queria atualizar o seu software Falcon para as versões 10 e 11 do sistema operativo Windows. O resultado da operação a 19 de julho foi um constrangedor caos informático global, com os utilizadores a verem um repetitivo "blue screen of death" e um constante pedido de reinicialização dos mais de oito milhões de computadores afetados.

A deteção do problema foi rápida pela Microsoft e pela CrowdStrike mas não tão célere que conseguisse evitar problemas nas indústrias da aviação, media, retalho ou financeira.

Sem contabilizar o impacto na Microsoft, o custo para as empresas da Fortune 500 pode chegar aos 5.400 milhões de dólares, segundo a Parametrix, com as maiores perdas sentidas na aviação – apesar de companhias como a Southwest Airlines terem evitado os problemas por usarem versões antigas do Windows (3.1 ou 95).

Para o facto do sistema operativo da Apple não ter sido afetado, a Microsoft explicou que "não pode legalmente isolar o seu sistema operativo da mesma forma que a Apple o faz, devido a um acordo com a Comissão Europeia". No acordo de 2009, comprometeu-se a dar o mesmo nível de acesso ao Windows a todos os programadores – uma situação que a Apple deixou de permitir em 2019. No caso do Linux, a The Register notou alguns problemas.



Fonte: Parametrix

As seguradoras elevam os potenciais prejuízos entre os 300 milhões e os mil milhões de dólares, segundo a empresa especialista em resseguros Guy Carpenter.

Os litígios também se devem suceder. A Delta já contabilizou o impacto na companhia aérea em 500 milhões de dólares. A CrowdStrike também está a ser processada por investidores, acusando-a de fornecer informação falsa que baixou o seu valor bolsista, e por três viajantes que apontaram "a negligência" da empresa como razão para as perturbações nas viagens aéreas.

A questão coloca-se igualmente se a empresa pode ser processada fora dos EUA. Sim, pelo menos em França, nota o The HFT Guy usando o caso anterior do incêndio no fornecedor de serviços de cloud OVH.

Após ter de lidar com cibercriminosos a proporem falsas correções ou campanhas oportunistas de phishing (notadas por várias agências de cibersegurança, como a CISA nos EUA), a CrowdStrike deu o incidente por mitigado a 29 de julho.

No entanto, ficaram algumas evidências transversais ao setor da cibersegurança. Por exemplo, quais as razões para Las Vegas ter tido um menor impacto com a falha da CrowdStrike? Redundância e resiliência, assegurou Michael Sherwood, Chief Innovation and Technology Officer da cidade.

Algo que os clientes da CrowdStrike mais afetados demonstraram não ter, nem "sistemas de backup para falhas como esta, porque também são uma despesa que afeta a rentabilidade a curto prazo", resumiu a Lawfare.

Tudo isto é "uma chamada de atenção para a fragilidade da infraestrutura global da Internet. É complexa, profundamente interligada e cheia de pontos únicos de falha", em que "um único problema num pequeno software pode fazer com que uma grande parte da Internet e da economia mundial fique offline".

Fonte: CrowdStrike

Não foi a primeira vez: em 2010, a "McAfee lançou uma atualização das suas definições de antivírus para clientes empresariais que, por engano, eliminou um ficheiro crucial do Windows XP, colocando os sistemas num ciclo de reinicialização e exigindo reparações manuais entediantes", escrevia então a ZDNet.

Quanto ao futuro, antecipa a Vox, se houve alguma lição a retirar da falha da CrowdStrike "é que a escala das interrupções de serviço e dos ciberataques está a aumentar à medida que o mundo depende cada vez mais de dispositivos ligados à Internet para funcionar. Não há melhor altura do que agora para reconsiderar se estamos a fazer o suficiente para impedir o próximo" ciberdesastre.

Fontes: Axios, Bloomberg Law, CISA, CrowdStrike (1, 2), CyberScoop, Guy Carpenter, Lawfare, Mashable, Microsoft (1, 2), Quartz, TechNewsWorld, The HFT Guy, The Register, Tom's Hardware, Vox, ZDNet.

Acordo global contra cibercrime aprovado com muitas críticas

As Nações Unidas adotaram em votação unânime o seu primeiro tratado sobre cibercriminalidade, traduzido livremente como Convenção Internacional Global para Combater o Uso das Tecnologias da Informação e da Comunicação para Fins Criminosos.

O acordo foi proposto pela Rússia e, ao fim de vários anos de negociações, espera-se que seja aprovado em Assembleia Geral no Outono, apesar da oposição por organizações de defesa dos direitos humanos, por grandes empresas de tecnologia, preocupadas com a capacidade do sector privado conseguir cumprir o tratado, com ramificações até ao potencial impacto que poderá ter no sigilo bancário internacional.

No primeiro caso, essas organizações afirmam que "prejudica os direitos humanos globais de liberdade de expressão, uma vez que contém cláusulas que os países podem interpretar de forma a processar internacionalmente qualquer crime que ocorra num sistema informático".

Fontes: The Record, Convenção, Euractiv, Scientific American, The Rage.

BREVES

• A cibersegurança é um problema da qualidade do software, afirma Jen Easterly, responsável pela Cybersecurity and Infrastructure Security Agency (EUA). "Temos uma indústria multibilionária de cibersegurança porque, durante décadas, os fornecedores de tecnologia foram autorizados a criar software defeituoso, inseguro e com falhas". O problema pode ser atenuado com o desenvolvimento de software "secure by design".

• "A adoção de uma mentalidade militar em relação à cibersegurança" significa evoluir das atuais estratégias de proteção da rede para uma segurança centrada nos dados. O modelo CIA (confidencialidade, integridade, acessibilidade) pode ajudar, quando metade das PMEs não está preparada para ciberataques.

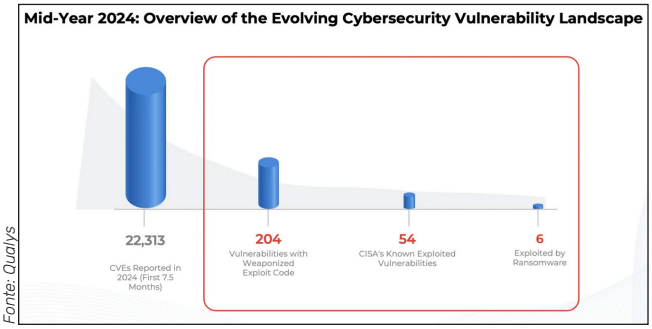
• Os desafios da proteção da infraestrutura crítica nacional.

• Como as "regulações regionais moldam a cultura mundial da cibersegurança".

• Os ciber-riscos organizacionais desconhecidos preocupam 86% de inquiridos num recente estudo, um aumento de 17% relativamente ao ano passado.

• O que devem os CEOs saber sobre cibersegurança e como podem fomentar um ambiente empresarial de cibersegurança que coloca as pessoas em primeiro lugar?

• No primeiro semestre do ano, foram referenciados 17.8 milhões de emails de phishing. Novos tipos de ataque, revelação de novas fragilidades na proteção, o Phishing as a Service (PhaaS) e a inteligência artificial estão a agilizar as campanhas de phishing.



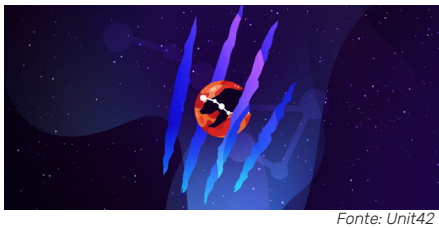
Fonte: Qualys

• O número de Common Vulnerabilities and Exposures (CVEs) registadas entre janeiro de 2023 e julho deste ano cresceu cerca de 30%, passando de 17.114 para 22.254 eventos. A análise da Qualys realça o "notável crescimento" de 10% no uso de CVEs antigas (descobertas antes de 2024), "realçando a necessidade de resolver vulnerabilidades previamente identificadas".

• A popularidade do Malware-as-a-Service (MaaS) deve-se ao lucrativo rendimento deste ecossistema, às baixas barreiras à entrada e à sua elevada procura: "ao oferecer malware pré-embalado e plug-and-play, o mercado MaaS permitiu que até mesmo atacantes inexperientes realizassem ataques potencialmente perturbadores, independentemente do seu nível de competência ou capacidade técnica".

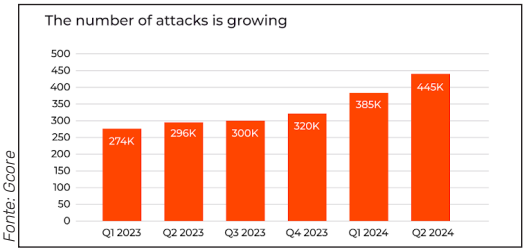
• Os crescentes ataques de ransomware, num mercado mais fragmentado, podem vir a ser classificados como "ameaças terroristas" nos EUA.

• Seis dos 53 grupos de ransomware referenciados no primeiro semestre do ano foram responsáveis por mais de metade do total de ataques. E qual o maior pagamento de ransomware alguma vez divulgado?


Fonte: Unit42

• O que se pode aprender com o ataque de ransomware à Change Healthcare e como fusões e aquisições amplificam perdas com os seguros de ransomware.

• Criador do primeiro grupo de ransomware-as-a-service, Reveton, acusado nos EUA uma década depois, também terá passado por Portugal.



Fonte: Gcore

• Ataques de DDoS aumentaram 46% no primeiro semestre de 2024. O sector dos videojogos teve um crescimento de 94% nos ataques entre janeiro de 2023 a junho de 2024.

Falha no Outlook da Microsoft permite a atacantes acesso através de email enviado ao utilizador, mesmo que este não abra a mensagem.

• Ciberataque mata na pecuária, outro afeta dadores de sangue e a insegurança dos painéis solares na Europa.

• EUA devolveram à Rússia dois cibercriminosos numa troca de prisioneiros, um deles com atividades financeiras ilegais em Portugal.

• A rápida expansão dos serviços digitais na cloud está a criar um cenário complexo para a cibersegurança e dificulta as organizações "manterem um inventário preciso dos seus ativos de TI, que são os principais alvos dos atacantes".

• Os resultados de um inquérito a 10 mil interessados em tecnologia, dos quais 500 portugueses, "demonstram que a comunidade da cibersegurança precisa de fazer mais para educar os utilizadores a manterem-se seguros online".

• A fragilidade do 2FA-SMS.

• Os EUA com uma estratégia nas novas normas de criptografia pós-quântica, tema que triunfou no prémio nacional Vencer o Adamastor.

• A agência norte-americana NSA aconselha, entre outros cuidados, a que se (des)ligue o telemóvel uma vez por semana.

• Atualização de firmware pode ocultar identificação do Bluetooth.

• Atacantes acedem a "smart speakers" para escutar utilizadores.

• O problema do "falso tráfego de rede".

• A Internet Corporation for Assigned Names and Numbers (ICANN) reservou o domínio .internal para utilização privada do DNS. E renovaram-se as críticas ao "pequeno número de casos, mas longe de inofensivos", de como o "DNS global está a ser administrado de forma negligente".

• Esquema de "prisão digital" tende a aumentar, assim como o swatting. E novas fraudes vão continuar a proliferar...

• O poder descentralizado dos Anonymous.

• A economia do spam (2022).

• A segurança da World Wide Web em 1996.

A LER

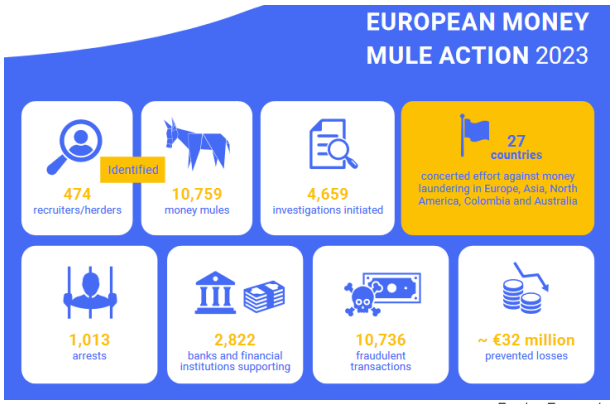
Internet Organised Crime Threat Assessment (Europol).

Recomendações da UE para atenuar riscos de cibersegurança nas telecomunicações e eletricidade.

Vision for the IC Information Environment: An Information Technology Roadmap.

Cibersegurança é área de cooperação em matéria de desafios globais e crises interligadas (G7).

Os desafios da ofuscação, seus efeitos e respostas.



Fonte: Europol

The Backbone of Cybersecurity: Hardware Security Modules.

Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment (2020).

Computer Archeology: Exploring the Anatomy of an MS-DOS Virus.

Diretora | Inês Esteves

Edição | Pedro Fonseca

Agosto 2024