ptsoc digest

agosto 2023

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

ptsoc digest

agosto 2023

Estratégias nacionais de Dados, Web 3.0 e IA com novos coordenadores

No âmbito da Estratégia Digital 2030, está a decorrer a elaboração das estratégias nacionais de Dados, Web 3.0 e a revisão da estratégia nacional de Inteligência Artificial (IA), anunciou o secretário de Estado da Digitalização e da Modernização Administrativa, Mário Campolargo. A coordenação geral fica a cargo de Arlindo Oliveira, enquanto Graça Canto Moniz coordena o tema dos Dados, Miguel Pupo Correia a Web 3.0. e João Gama a IA.

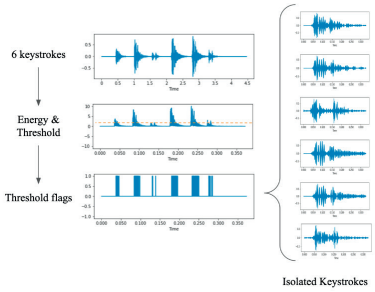
Ataques clínicos

O Serviço de Saúde da Região Autónoma da Madeira (SESARAM) sofreu um ataque de cibersegurança de dados a 6 de Agosto. O incidente obrigou à suspensão da atividade clínica não urgente, nomeadamente cirurgias. A instituição recordou "que situações semelhantes aconteceram nos Hospitais dos Açores e no Garcia de Orta", com quem falaram para obterem informação e experiência neste tipo de ataques.

Em Israel, um hospital foi obrigado a redirecionar novos pacientes para outras instituições após um ataque de ransomware que afetou o sistema informático administrativo. Nos EUA, cibercriminosos atacaram os sistemas informáticos do prestador de cuidados de saúde Prospect Medical Holdings, encerrando salas de emergência em vários estados, levando ao cancelamento de intervenções cirúrgicas e ao redireccionamento dos serviços de ambulâncias. Também a empresa sueca de software Ortivus sofreu um ataque que impediu o acesso de dois serviços de ambulâncias britânicos aos registos eletrónicos dos doentes.

Fontes: SESARAM, CBS News, The Record, Ortivus

Ciberataque acústico



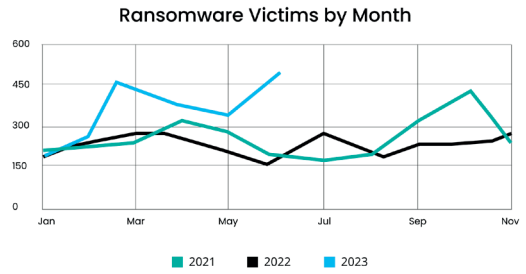
Investigadores desenvolveram um modelo de aprendizagem capaz de roubar dados através dos toques no teclado, gravados com um microfone. A técnica tem uma precisão de 95% e baixa para os 93% quando o Zoom foi utilizado no treino do algoritmo para a classificação do som, "o que continua a ser perigosamente elevado".

Este tipo de ataque é preocupante porque, com a generalização dos microfones nos computadores, é capaz de registar e transmitir dados do alvo, como passwords ou outra informação sensível. Os gestores de passwords podem atenuar o perigo, no primeiro caso, enquanto o acesso ao equipamento pode ser feito por autenticação biométrica ou usando um ecrã tátil.

Fontes: Bleeping Computer, arXiv

O papel dos CISO no ransomware

O "burnout" do diretor de segurança da informação (CISO) é um problema que parece estar a piorar, até porque, "quando ocorrem violações de segurança e ataques de ransomware, os CISOs muitas vezes assumem automaticamente a culpa". Mas, quando o governo dos EUA pondera proibir os pagamentos de ransomware, porque "se houver dinheiro a ganhar, os ataques continuarão", devem ser os CEOs, CFOs e conselhos de administração negligentes a serem responsabilizados pelas consequências. Até porque a Securities and Exchange Commission aprovou regras que obrigam as empresas reguladas a divulgar incidentes de cibersegurança e porque "os ataques de ransomware podem ser um teste de liderança" e estão a aumentar, enquanto os riscos com a IA se estão a diversificar.



Em junho, bateu-se um novo recorde nos ataques de ransomware, com 456 novas vítimas - 38% mais do que no mês anterior e 180% mais do que no mês homólogo. Também o custo das violações de dados atingiu a média "histórica" de 4,4 milhões de dólares em 2023.

Fontes: Axios, Harvard Business Review, WEF, The Hacker News, CSO, Corvus, IBM Security

Mais cautela ou mais regulação?

União Europeia, China e Estados Unidos adotaram abordagens diferentes na "grande experiência regulatória" da IA. "A UE é extremamente cautelosa", enquanto os EUA têm sido "os mais interventivos" e o governo chinês tenta "equilibrar a inovação com a manutenção do seu controlo apertado sobre as empresas e a liberdade de expressão". No geral, todos estão a tentar perceber se é necessária regulamentação específica para a IA ou se as leis atuais já abordam os ciber-riscos.

A reação às novas tecnologias pode resultar num excesso de regulação, com efeitos inesperados nomeadamente no setor da segurança. Esta regulamentação tende também a ser "demasiado ampla, o que sugere que os legisladores não têm conhecimentos técnicos" e dificulta qualquer "prospetiva estratégica, ou seja, a capacidade de prever e agir em função de potenciais futuros". Mesmo assim, antes de avançar, deve-se perguntar: "Estamos realmente a melhorar a segurança ou apenas a impor mais regulação"?

Fontes: Nature, Dark Reading (1, 2), WEF

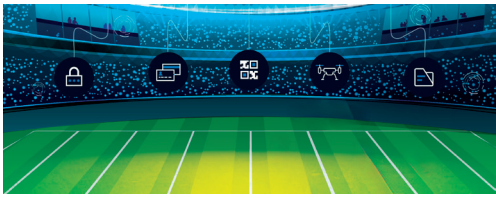
BREVES

• A operação Jackal, coordenada pela Interpol, resultou na apreensão e recuperação de quase 1,4 milhões de euros em Portugal. A operação visou o crime organizado da África Ocidental e levou a 103 detenções, identificação de 1.110 suspeitos, 208 contas bancárias bloqueadas e 2,15 milhões de euros apreendidos ou congelados.

• Uma empresa de segurança encontrou várias vulnerabilidades no sistema de rádio terrestre TETRA, utilizado por várias autoridades na Europa, como o SIRESP em Portugal.

• O Presidente da República de Angola, João Lourenço, quer instalar uma academia de

cibersegurança para ter "um serviço de telecomunicações e tecnologias de informação seguro e robusto em defesa dos utilizadores".



• A Microsoft alertou para o crescente interesse dos cibercriminosos nos eventos desportivos em direto – algo para que o Centro de Cibersegurança do Reino Unido já tinha chamado a atenção no relatório de 2020 "The Cyber Threat to Sports Organisations".

• O grupo RedHotel, alegadamente ligado ao governo chinês, recolheu informações e fez espionagem económica em pelo menos 17 países da Ásia, Europa e América do Norte.

• O impacto do MOVEit foi superior ao inicialmente divulgado, com mais de 40 milhões de indivíduos e 600 organizações atingidas em sectores sensíveis e regulados como saúde, educação, finanças, seguros ou administração pública.

• Organizações devem estar atentas ao inseguro Remote Desktop Protocol.

• Uma "oferta lucrativa de emprego" a um programador da CoinsPaid levou ao roubo de 37 milhões de dólares. "O ataque foi muito rápido. Eles são profissionais", disse o diretor financeiro da empresa.

• Hackers da Coreia do Norte acederam à rede informática do fabricante de mísseis russo NPO Mashinostroyeniya durante pelo menos cinco meses de 2022. "O incidente mostra como o isolado país pode até visar os seus aliados, como a Rússia, numa tentativa de obter tecnologias críticas", não se ficando pelos ataques aos EUA, incluindo o uso de engenharia social.

• Utilizadores de telemóveis na Rússia reportaram que as suas VPNs deixaram de funcionar, nomeadamente as que usam os protocolos OpenVPN e WireGuard.

• O maior motor de busca russo Yandex, que inclui mais de 90 outros serviços, sofreu em janeiro de 2023 a divulgação pública de quase 45 GB de código-fonte. A revelação permitiu conhecer em maior detalhe como o Yandex utiliza os dados dos utilizadores.

• Um ciberataque às comunicações por satélite em janeiro de 2022, de que dependia a Ucrânia, foi cometido por atacantes com conhecimentos do sistema. Autoridades dos EUA e ucranianas responsabilizaram a Rússia pelo ataque à rede Viasat KA-SAT, que interrompeu o acesso à Internet e usou métodos sofisticados para tentar impedir o seu restabelecimento. Mais recente foi o ataque de malware à constelação de satélites de acesso à Internet.

• Investigadores conseguiram aceder a três satélites e descobriram que a sua segurança está "anos atrasada" relativamente às normas mais básicas da cibersegurança.

• O setor dos seguros informáticos é criticado por dar cobertura ao pagamento de resgates em ataques de ransomware, mas um projeto de investigação conclui não existirem provas de que as vítimas com seguro são mais propensas a pagar esses resgates.

• A Finlândia viu quadruplicar os ataques de ransomware desde o início do seu processo de adesão à NATO - um aumento que pode estar ligado à geopolítica.

• A NATO levou a sério as alegações de criminosos hacktivistas que divulgaram 845 MB de informações não classificadas da aliança militar, pertencentes a 31 países.

• A Comissão Eleitoral do Reino Unido sofreu um "ciberataque complexo", iniciado em agosto de 2021 mas apenas confirmado em outubro de 2022. A Rússia foi acusada do ataque, que permitiu aceder aos dados de 40 milhões de eleitores aproveitando uma vulnerabilidade não corrigida.

• O governo britânico atualizou o National Risk Register, com riscos da segurança nacional interna antes classificados pelo governo e que inclui cenários do impacto dos ciberataques em sectores críticos.

• A plataforma de "phishing-as-a-service" (PaaS) 16shop foi encerrada após uma investigação coordenada pela Interpol, com um operador preso na Indonésia e outro no Japão. A plataforma vendia "kits de phishing" para defraudar utilizadores por email. A crescer em utilização está a plataforma EvilProxy, que procura sequestrar contas de executivos de empresas conhecidas.

• Centenas de pessoas de agências de defesa e de informação tiveram os seus nomes e endereços de email expostos pela VirusTotal, plataforma de análise de malware da Google.

• 100 horas a ver hackers (do tipo "Rangers", "Barbarians", "Wizards", "Thieves" e "Bards") a piratearem computadores.

• Malware Sogu e SnowyDrive distribuídos através de unidades USB infetadas.

• Como o FBI combate os cada vez mais sofisticados ataques DDoS.

• A Casa Branca deve atualizar a sua estratégia de cibersegurança perante os impactos da IA, quando o FBI alerta para as tentativas estrangeiras em usar a IA em atividades maliciosas. Entretanto, a Administração Biden lançou um "hackathon" para desenvolver sistemas de IA capazes de identificar e corrigir vulnerabilidades de software.

• Os cibercriminosos estão a criar versões de "Large Language Models" como o WormGPT para ataques com IA.

• Como funciona o grupo da Microsoft que, desde 2018, tenta perceber os ataques às plataformas de IA.

• O European Policy Centre argumenta que a UE precisa de um plano de ação coordenado para responder aos ataques por computação quântica.

• A Agência da União Europeia para a Cibersegurança (ENISA) revelou que o Team Europe alcançou, pela segunda vez consecutiva, o primeiro lugar no International Cybersecurity Challenge.

• A África do Sul está a caminho de ultrapassar a Nigéria como "a capital do cibercrime em África", continente onde o investimento em cibersegurança está a aumentar.

• "As organizações devem avaliar a sua cibersegurança no contexto da geopolítica e da evolução tecnológica".

A LER

Estudo Sobre a Comunidade de Competências em Cibersegurança

Checking-up on Health: Ransomware Accounts for 54% of Cybersecurity Threats

Acordo político sobre novas regras para reforçar a cibersegurança nas instituições, órgãos, organismos e agências da UE

Posição do Conselho Europeu sobre o Regulamento Ciber-Resiliência, sobre os requisitos de segurança aplicáveis a produtos digitais

European Union Agency for Cybersecurity (ENISA) & European Cybersecurity Certification Framework - avaliação

Acordo político provisório do Parlamento Europeu e do Conselho da UE sobre o Regulamento eIDAS

Carta aberta à UE em defesa do uso livre de criptografia

European Cyber Security Month

Cybersecurity Strategic Plan da CISA (EUA)

Global Fraud and Payments Report

IGF 2023 Best Practice Forum on Cybersecurity

SAS analisa as tendências de fraude em pagamentos digitais

State of Cybersecurity Resilience 2023

How Hygienic is Your Website and Email Service?

Comissão Federal do Comércio (FTC) norte-americana avançou com uma ampla investigação à OpenAI e ao seu chatbot de IA generativa ChatGP

Diretora | Inês Esteves

Edição | Pedro Fonseca

agosto 2023