bilingual edition

ptsoc{news}

01

.pt

Luisa Ribeiro Lopes

Presidente do Conselho Diretivo do .PT
President of .PT

Informar e educar para a cibersegurança

A cibersegurança tornou-se um tema incontornável durante a pandemia de Covid-19. Se a exposição a ataques e ameaças cibernéticas já era permanente e real no período pré-pandémico, mais se acentuou com a aceleração digital a que a sociedade se viu sujeita ao longo do último ano.

A velocidade a que assistimos ao nível da transformação digital fez aumentar o risco de exposição do ciberespaço a novos ataques e é expectável que o número de incidentes permaneça elevado por força do crescimento das atividades online e por algumas limitações ao nível de uma política de cibersegurança efetiva no nosso tecido empresarial, a que se junta uma, ainda, considerável iliteracia ao nível da segurança digital.

Não é demais lembrar que além dos danos financeiros e reputacionais irreparáveis para empresas, organizações, marcas e pessoas, o impacto estimado dos ciberataques tem um custo para a economia comparável apenas aos efeitos provocados, por exemplo, por um furacão de grande intensidade, sendo o risco de um ciberataque superior ao de um ataque terrorista.

Enquanto entidade responsável pela gestão e operação do serviço de registo de domínios em .pt e consciente

Informing and educating for cybersecurity

Cybersecurity has become an inevitable topic during the Covid-19 pandemic. The exposure to cyberattacks and threats were already a reality in the pre-pandemic period, and it has taken a further turn for the worse with the digital acceleration that society came across over the last year.

The fast pace of the digital transformation has increased the risk of exposure of the cyberspace to new attacks and it is predictable that the number of incidents remains high due to the growth of online activities and some constraints at an effective cybersecurity level in our business sector. Furthermore, a significant illiteracy in the field of digital security is also contributing to the above-mentioned increase of the number of incidents.

In addition to the irreparable financial and reputational damages to companies, organisations, brands, and people, we must stress out that the estimated impact of cyberattacks has a cost for economy which is only comparable to the effects caused, for instance, by a hurricane with maximum intensity, being the risk of a cyberattack likely superior to the risk of a terrorist attack.

As the responsible entity for the management and operations of domain registration service at .pt, .PT is aware of the challenges in cyberspace, hence is making

dos desafios do ciberespaço, o .PT tem feito um investimento na área da cibersegurança, ao colaborar com as entidades competentes a nível nacional e internacional, mas acima de tudo ao melhorar e acelerar a capacidade de resposta a incidentes de segurança através de soluções inovadoras que permitam um maior grau de resiliência, mantendo a confiança dos utilizadores e contribuindo para uma utilização mais segura e fiável da Internet. O Centro de Operações de Segurança (PTSOC) e a plataforma webcheck.pt são exemplos de iniciativas estruturantes que materializam a estratégia que estabelecemos em matéria de segurança.

É neste quadro de responsabilidade partilhada e cooperante que nasce a revista **PTSOC news**. Um projeto trimestral dedicado exclusivamente à cibersegurança e que promete informar, esclarecer e educar, através de notícias, análises, artigos de opinião, documentos e indicadores relevantes da área. Pretende-se criar um espaço livre, aberto e independente que promova a partilha de conhecimento em relação ao ciberespaço.

A primeira edição da **PTSOC news** traz como temas principais uma análise à indústria do ransomware e mostra qual o propósito do PTSOC e da plataforma webcheck.pt.

Boas leituras!

a significant investment in cybersecurity by partnering with competent entities at a national and international level and, above all, by improving and accelerating the responsiveness to security incidents through innovative solutions which allow a higher degree of resilience. By doing so, .PT keeps users' trust and contributes to a safer and reliable use of the internet. The Centre of Security Operations (PTSOC) and the webcheck.pt platform are two examples of structuring initiatives that concretise the strategy we set out in terms of security.

It is within this framework of shared and collaborative responsibility the magazine **PTSOC news** is created. A quarterly project exclusively dedicated to cybersecurity which aims at informing, enlightening, and educating through news, evaluations, opinion articles, documents, and relevant indicators of the field. It is intended to create a free, open, and independent room which can promote the share of knowledge on cyberspace.

The first **PTSOC news** edition includes an evaluation of the ransomware industry and shows the purpose of PTSOC and the platform webcheck.pt.

Enjoy your reading!

Colonial Pipeline

A indústria do ransomware

O ataque de ransomware ocorrido em maio passado à Colonial Pipeline, empresa gestora de oleodutos nos EUA, confirma o cibercrime como um setor cujo objetivo é maximizar lucros, diminuir perdas e garantir uma reputação para manter uma organização criminosa a funcionar.

O ataque foi atribuído pelo FBI ao DarkSide, grupo alegadamente com ligações à Rússia e à Europa de Leste, que se vangloriou de doar dinheiro para obras de caridade, numa alegada atitude de responsabilidade social recusada pelas entidades conhecedoras da proveniência do dinheiro.

As ferramentas para os cibercrimes estão à venda a preços acessíveis e quem quiser pagar por um serviço mais "profissional" contrata grupos anónimos em modelos de RaaS ("ransomware as a service").

As vítimas, assumindo a débil segurança interna, tendem a pagar - apesar das autoridades afirmarem que assim se incentivam mais ataques.

Os ataques a infraestruturas essenciais - como hospitais, oleodutos ou empresas de energia -, fragilizam a estabilidade

The ransomware industry

The ransomware attack that took place last May on Colonial Pipeline, a US fuel pipeline company, confirms cybercrime as a sector whose goal is to maximise profits, decrease losses and ensure a reputation to keep a criminal organization going.

The FBI attributed the attack to DarkSide, a group with alleged ties to Russia and Eastern Europe, which boasted of donating money for charities, in an alleged attitude of social responsibility refused by entities knowing the money's provenance.

Cybercrime tools can be purchased at affordable prices and anyone who wants to pay for a more 'professional' service hires anonymous groups working as RaaS ('ransomware as a service').

Victims, assuming weak internal security, tend to pay - despite authorities claiming that such behaviour encourages more attacks.

Attacks on essential infrastructures - such as hospitals, pipelines or energy companies -, undermine countries' internal stability and stimulate transnational action, aiming at geopolitical influence based on the difficulty of

interna dos países e estimulam a ação transnacional, visando a influência geopolítica assente na dificuldade da atribuição de culpas e na negação plausível dos líderes das nações atacantes.

Por fim, a disseminação das criptomoedas facilita pagamentos difíceis de rastrear e agiliza a monetização dos cibercrimes. As autoridades apelam à regulação das criptomoedas para conhecer a sua proveniência e, se derivar de atividades ilegais, evitar a introdução no circuito financeiro tradicional.

Será isso possível? "Neste momento, existem quase 10 mil criptomoedas [registadas no CoinMarketCap]. Tentar fechar ou controlar todos esses meios de pagamento parece-me uma tarefa utópica", nota Miguel Pupo Correia, professor na área da segurança da informação no Instituto Superior Técnico (Lisboa).

O que se passou com a Colonial Pipeline?

O ataque à Colonial levou ao racionamento de gasóleo, afetou indivíduos e companhias aéreas. O presidente norte-americano Joe Biden ameaçou multar quem aproveitasse a situação para aumentar o preço do combustível. E assinou uma ordem

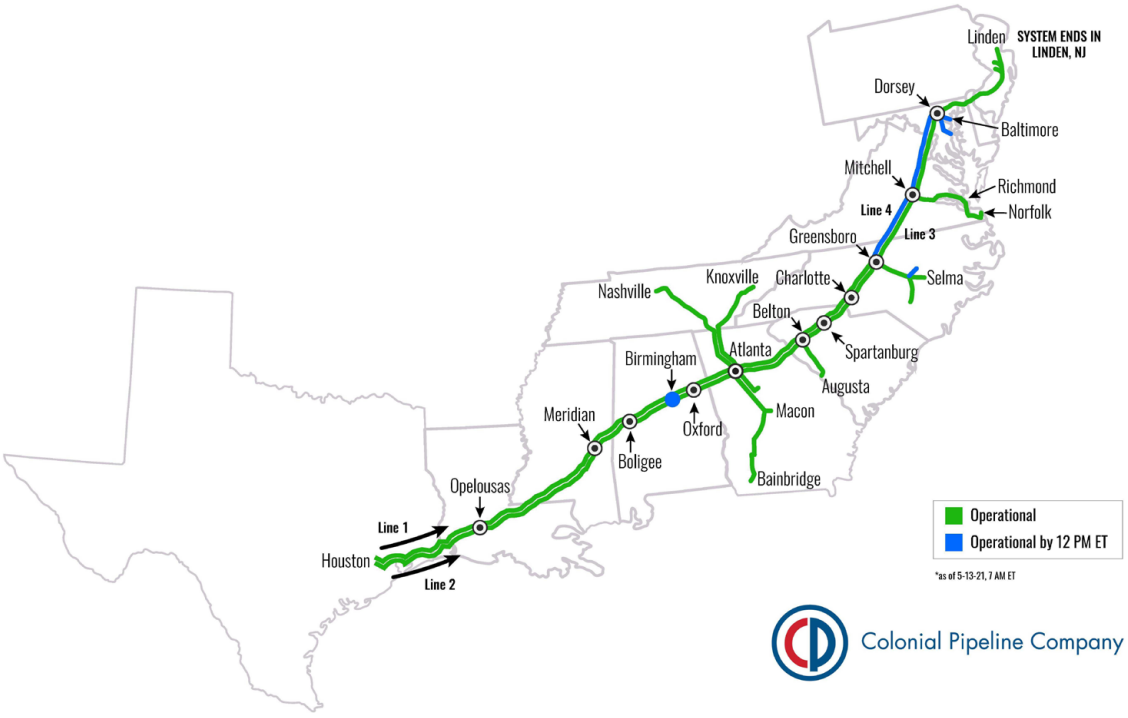
assigning blame and the plausible deniability by leaders of the attacking nations.

Finally, the spread of cryptocurrencies makes it more difficult to track down payments and streamlines cybercrime monetization. Authorities call for the regulation of cryptocurrencies to know where they come from and, if derived from illegal activities, to avoid their introduction in the traditional financial circuit.

Is that possible? 'Currently, there are almost 10 000 cryptocurrencies [registered with Coinmarketcap]. Trying to close or control all these means of payment seems, to me, to be a utopian task,' comments Miguel Pupo Correia, a professor in the area of information security at Instituto Superior Técnico (Lisbon).

What happened with Colonial Pipeline?

The attack on Colonial led to fuel rationing, affecting individuals and airlines. US President Joe Biden threatened to fine anyone who took advantage of the situation to raise fuel prices. In addition, he also signed an executive order to establish a roadmap to upgrade the federal systems' cybersecurity.



executiva a estabelecer um "roadmap" para atualizar a cibersegurança dos sistemas federais.

Nessa altura, também o governo inglês iniciou um processo de consulta pública (que decorre até julho) para determinar requisitos de segurança nas cadeias de fornecimentos de bens. Segundo a proposta, à medida que estas cadeias "estão interligadas, as vulnerabilidades nos produtos e serviços dos fornecedores tornam-se alvos mais atraentes para os atacantes que desejem obter acesso às organizações. Recentes ciberincidentes de elevado perfil, em que os atacantes usaram fornecedores de serviços geridos como

At that time, the British government also started a public consultation process (which will run until July) to determine security requirements in the supply chains of goods. According to the proposal, as these chains 'are interconnected, vulnerabilities in suppliers' products and services become more attractive targets for attackers who wish to gain access to organizations. Recent high-profile cyber incidents, in which attackers have used managed service providers as a means of targeting businesses, recall that cyber threats are more than capable of exploiting vulnerabilities in supply chain security, and seemingly small players of that organization's chain may present

um meio de atacar empresas, recordam que as ciberameaças são mais do que capazes de explorar vulnerabilidades na segurança da cadeia de fornecimentos, e 'players' aparentemente pequenos dessa cadeia numa organização podem apresentar níveis desproporcionalmente elevados de ciber-risco".

Joseph Blount, o CEO da Colonial, aceitou pagar o resgate de 4,4 milhões de dólares por desconhecer a dimensão do ataque. Reconheceu assim os resultados de uma anterior auditoria interna que considerava o sistema informático tão inseguro que "até uma criança lhe podia aceder".

Para forçar o pagamento, o DarkSide anunciou a intenção de publicar dados de mais empresas atacadas no Brasil, EUA e Inglaterra. A subsidiária alemã Toshiba Tec Group revelou ter desligado a rede de comunicações entre Japão e Europa após um ciberataque do grupo.

O ataque iniciou-se a 7 de maio, o pagamento foi efetuado no dia seguinte, mas os problemas prosseguiram durante vários dias. Em troca do pagamento, o DarkSide entregou uma ferramenta de desencriptação dos dados demasiado lenta e a Colonial acabou por recorrer a "backups" de segurança. A companhia de seguros AXA declarou não reembolsar

disproportionately high levels of cyber-risk.'

Joseph Blount, CEO of Colonial, agreed to pay the ransom of $4.4 million, not knowing the scale of the attack. He thus acknowledged the results of a previous internal audit that considered the computer system so insecure that 'even a child could access it'.

To force payment, DarkSide announced its intention to publish data from more companies attacked in Brazil, the USA and England. The German subsidiary Toshiba Tec Group revealed to have shut down the communications network between Japan and Europe after they were cyberattacked by the group.

The attack began on 7 May, payment was made the next day but the problems continued for several days. In exchange for the payment, DarkSide delivered a too slow data decryption tool and Colonial eventually turned to security backups. Insurance company AXA stated not to reimburse ransomware payments, after which its Asian subsidiaries were attacked.

Victim retaliation to attackers does not seem to be a practical solution. 'To carry out cyberattacks, even against criminal groups, is a crime and, undoubtedly,

os pagamentos de ransomware, após o que as suas filiais asiáticas foram atacadas.

A retaliação da vítima aos atacantes não parece ser uma solução prática. "Executar ataques informáticos, mesmo que contra grupos criminosos, é crime e sem dúvida arriscado", lembra Pupo Correia, notando que apresentar "queixa à polícia costuma ser boa ideia".

Deve-se (ou não) pagar o resgate?

Também em maio, o Department of Health e o Health Service Executive (HSE) na Irlanda sofreram ataques de ransomware, atribuídos ao grupo do leste europeu Wizard Spider pela National Cyber Security Agency, a quem o HSE entregou o caso após recusar pagar por 700 GB de dados de pacientes. O primeiro-ministro irlandês, Micheál Martin, assegurou que as agências do governo não pagam por ciber-extorsão.

Neste âmbito, as opiniões dividem-se perante o risco das vítimas não pagarem (para não fomentar novos ataques) e ficarem sem os dados.

Não é uma resposta simples, concede o professor do IST. "Por um lado pagar a criminosos é um mau princípio; por

risky', recalls Pupo Correia, noting that filing 'a police complaint is usually a good idea'.

Should the ransom be (or not) paid?

Also in May, Ireland's Department of Health and the Health Service Executive (HSE) suffered ransomware attacks, attributed to the Eastern European group Wizard Spider by the National Cyber Security Agency, to whom the HSE handed the case after refusing to pay for 700 GB of patient data. Irish Prime Minister Micheál Martin assured that government agencies do not pay for cyber extortion.

In this regard, opinions are divided on the risk that the victims will not pay (so as not to encourage new attacks) and lose the data.

It is not a simple answer, says the IST professor. 'On the one hand, paying criminals is a bad principle; on the other hand, the data can be greatly missed.'

So, 'the first thing to do is to contact a company which specialises in that problem so they can help solve it. Oftentimes, ransomware has bugs and data can be retrieved free of charge. The No More Ransom! project has a compilation of tools that allows you to

outro, os dados podem fazer muita falta".

Assim, "a primeira coisa a fazer é contactar uma empresa especialista no problema de modo a que possa ajudar a resolvê-lo. Muitas vezes o ransomware tem bugs e os dados podem ser obtidos sem pagar. O projeto No More Ransom! tem uma compilação de ferramentas que o permitem fazer". Mas "se isso não for possível, a vítima tem de fazer a sua própria análise do custo de pagar *versus* o custo de ficar sem os dados".

Para a Europol, pagar não é opção por não se garantir a resolução do problema. O software de desencriptação pode não funcionar ou servir de disfarce para instalar novo malware.

O pagamento por ransomware deve ser ilegalizado por afetar as vítimas mas também a sociedade ao possibilitar mais ataques, defendem outros. Esta regra deve ter exceções, como quando se colocam vidas humanas em perigo.

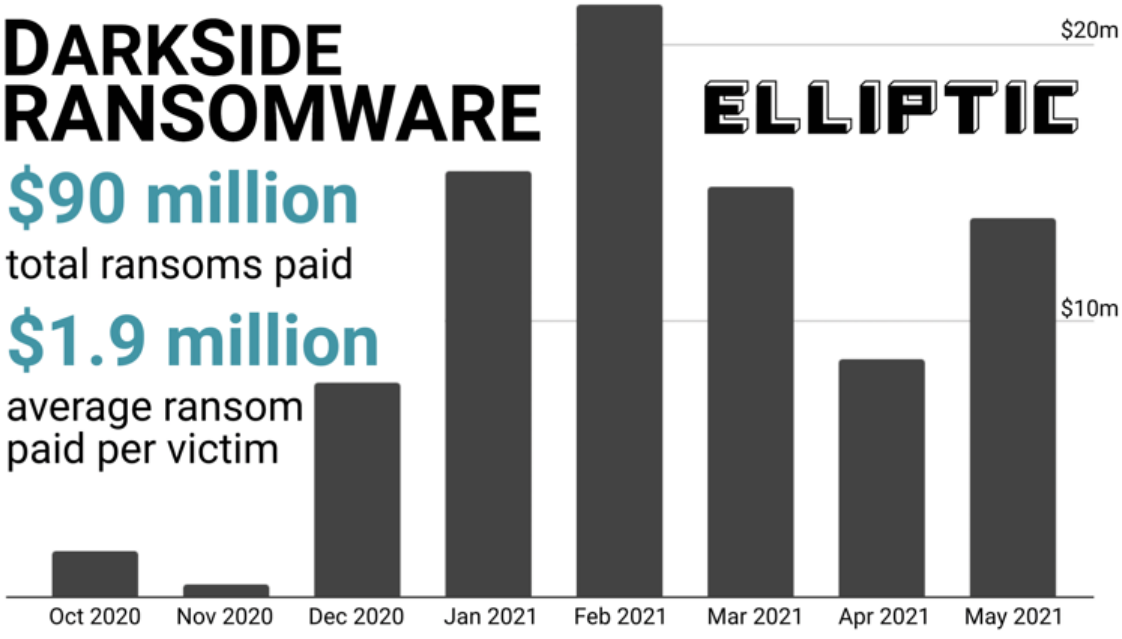
Do lado legal, o crime não existe por si em Portugal mas pode ser julgado noutras acusações. "O ransomware fez surgir as expressões sequestro de dados (ato de bloquear, inutilizar ou inviabilizar o acesso à dados) e extorsão digital ou criptoviral (ato de solicitar

do it.' But 'if this is not possible, the victim must conduct its own analysis of the cost of paying *versus* the cost of losing the data.'

For Europol, paying is not an option because the problem cannot be solved. The decryption software may not work or serve as a cover to install new malware.

Ransomware payment must be made illegal as it affects the victims as well as society by allowing more attacks, others defend. There must be exceptions to this rule, as when human lives are in danger.

From a legal standpoint, the crime itself does not exist in Portugal, but criminals can be tried on other charges. 'Ransomware gave rise to the terms "data hijacking" (act of blocking, disabling or invalidating access to data) and "digital or cryptoviral extortion" (act of requesting illicit advantage/payment in exchange for data release)', wrote Judge Duarte Nunes in Cyberlaw by CIJIC (September 2019). 'Given that our legal system does not have a specific ransomware charge, an attempt should be made to subordinate the agent(s) conduct to some of the types of crime provided for in the law", namely "(1) the illegitimate access to a third-party



vantagem ilícita/pagamento em troca da liberação dos dados)", escreveu o juiz Duarte Nunes na Cyberlaw by CIJIC (Setembro de 2019). "Dado que a nossa ordem jurídica não possui uma incriminação específica do ransomware, haverá que tentar subsumir a conduta do(s) agente(s) a algum dos tipos de crime previstos na lei", nomeadamente "(1) o acesso ilegítimo ao sistema informático e aos dados informáticos alheios, (2) o impedimento de o titular aceder aos dados e (3) a exigência e o pagamento do resgate".

Ascensão e queda

O sucesso do ataque do DarkSide foi

computer system and computer data, (2) preventing the data subject from accessing the data and (3) the demand for a ransom payment.'

Rise and fall

The success of DarkSide's attack was also its demise. Faced with massive publicity and loss of access to their extortion operations management infrastructure and the affiliate 'bank account' payments, DarkSide announced the suspension of its activities.

Official US sources have ensured that they are not responsible for the group's reported disappearance, which has

também a sua perda. Perante a enorme publicidade e perda de acesso à infraestrutura de gestão das operações de extorsão e à "conta bancária" de pagamentos dos afiliados, o DarkSide anunciou a suspensão das suas atividades.

Fontes oficiais dos EUA garantiram não serem responsáveis pelo anunciado desaparecimento do grupo, ativo desde agosto de 2020 e detetado pela empresa de segurança Intel 471 num fórum russo em novembro de 2020 a anunciar o serviço de RaaS.

Mas o episódio ocorreu após Biden ter ameaçado estas atividades. E, apesar de não haver qualquer indício de retaliação, existe um "exército secreto" de 60 mil militares e civis nos EUA, agrupado na última década pelo Pentágono, capaz de executar missões "na vida real e online, por vezes escondendo-se em negócios privados e consultoras", revelou a revista Newsweek. O modelo é semelhante a estruturas de "ciberwarfare" da Rússia ou China, em que os líderes assumem uma negação plausível perante as queixosas nações atacadas.

O especialista em cibersegurança Brian Krebs explicou recentemente como as autoridades russas são tolerantes com os ataques a alvos estrangeiros mas

been active since August 2020 and detected by Intel 471 security company at a Russian forum in November 2020 announcing the RaaS service.

But the episode occurred after Biden threatened these activities. And, although there is no indication of retaliation, there is a 'secret army' of 60 000 military and civilians in the US, grouped over the last decade by the Pentagon, capable of carrying out 'real-life and online [missions], sometimes hidden in private businesses and consulting companies', Newsweek revealed. The model is similar to Russia or China's cyberwarfare structures, in which leaders assume plausible deniability before the attacked nations.

Cybersecurity expert Brian Krebs recently explained how Russian authorities are tolerant of attacks on foreign targets but rather tough on those targeting Russian organizations. To avoid deception (and retaliation), attackers program malware to detect the presence of Cyrillic keyboards.

The difficulty in assigning direct blame to any attacking group stems from RaaS' own model. In its DarkSide 2.0 version, ransomware was distributed to a group of affiliates who, according to FireEye, had to pay 25 % of the

bastante duras se visam organizações russas. Para evitarem enganos (e retaliações), os atacantes programam o malware para detetar a presença de teclados com alfabeto cirílico.

A dificuldade em atribuir culpas diretas a qualquer grupo atacante decorre do próprio modelo de RaaS. Na sua versão DarkSide 2.0, o ransomware era distribuído a um grupo de afiliados que, segundo a empresa FireEye, tinham de pagar 25% dos pagamentos obtidos nos "resgates abaixo de 500 mil dólares e 10% de qualquer tentativa de extorsão bem-sucedida acima dos 5 milhões".

A empresa de "crypto compliance" Elliptic contabilizou a receção de 17,5 milhões de dólares numa conta do DarkSide aberta a 4 de março passado. Foi neste "wallet" que a Colonial depositou os 75 bitcoins (ou 4,4 milhões de dólares) a 8 de maio. No total, a conta recebeu 57 pagamentos de 21 outros "wallets", incuindo 78.29 bitcoins da empresa de distribuição de produtos químicos Brenntag a 11 de maio.

A Elliptic conseguiu traçar os pagamentos até outubro do ano passado e calculou que o grupo recebeu mais de 90 milhões de dólares de 47 vítimas.

payments obtained from 'ransoms below $500 000 and 10 % of any successful extortion attempt above $5 million.'

Crypto compliance company Elliptic accounted receiving $17.5 million from a DarkSide account opened on 4th March. It was in this wallet that Colonial deposited the 75 Bitcoins (or $4.4 million) on 8th May. In total, the account received 57 payments from 21 other wallets, including 78.29 Bitcoins from the Brenntag chemical distribution company on 11th May.

Elliptic managed to trace the payments until October last year and calculated that the group received more than $90 million from 47 victims.

The group used 'double extortion tactics' by pressuring victims with threats to publish stolen confidential information if they refused to pay. A website with the stolen documents and 'operated by DarkSide went so far as to create a space for journalists and "recovery" companies to see them directly,' reports ZDNet magazine. Also available is the code of conduct banning 'attacks on funeral services, hospitals, palliative care organizations, nursing homes and companies that participate in the distribution of COVID-19 vaccines'.

O grupo usava "táticas de dupla extorsão" ao pressionar as vítimas com ameaças de publicar informações confidenciais roubadas se elas recusassem pagar. Um site com os documentos roubados e "operado pelo DarkSide chegou ao ponto de criar um espaço para jornalistas e empresas de 'recuperação' os verem diretamente", contava a revista ZDNet, estando igualmente disponível o código de conduta a proibir "ataques contra serviços de funerais, hospitais, cuidados paliativos, enfermagem e empresas envolvidas na distribuição de vacinas para a Covid-19".

Evolução na diversidade

A Internet evoluiu rapidamente para uma rede global de comércio e serviços, frágil e insegura porque a ciberseguran-ça não acompanhou a evolução, vista por várias entidades como um custo e não como investimento preventivo, quando aumentam os equipamentos interligados e os utilizadores, as funcio-nalidades e os documentos sensíveis continuam a ser colocados online, os ciberataques sucedem-se e os alertas de perigo também. Pode ser diferente, nomeadamente em Portugal?

Em 2015, a Polícia Judiciária revelou que "80% das vítimas" de ciber-

Evolution in diversity

The Internet has rapidly evolved into a fragile and insecure global network of commerce and services because cybersecurity has not been able to keep up with its evolution, seen by many entities as a cost rather than a 'preventive investment'; when interconnected equipment and users increase, sensitive features and documents continue to be put online and cyberattacks occur one after the other, as do danger alerts. Can it be different, namely in Portugal?

In 2015, the criminal police Polícia Judiciária revealed that 80 % of the victims of cyber extortion were chartered accountants, statutory auditors, lawyers and staff responsible for processing salaries in schools. In 2017, WannaCry affected a few national systems. The following year, there were attacks on the email network of military and civilian staff of the Portuguese Armed Forces General Staff and the José de Mello Saúde company. The organization did not pay, nor did the Champalimaud Foundation, which complained of a similar attack in July 2019. That year, the Municipal Councils of Mirandela and Vinhais were attacked, as was Prosegur. Last year, the attacks turned to Altice and EDP companies.

-extorsão eram técnicos e revisores oficiais de contas, advogados e responsáveis do processamento dos vencimentos nas escolas. Em 2017, o WannaCry afetou alguns sistemas nacionais. No ano seguinte, registaram-se ataques à rede de email de funcionários militares e civis do Estado-Maior General das Forças Armadas e à José de Mello Saúde. A organização não pagou, assim como a Fundação Champalimaud, que se queixou de um ataque semelhante em julho de 2019. Nesse ano, as câmaras municipais de Mirandela e de Vinhais foram atacadas, tal como a Prosegur. No ano passado, foi a vez de se conhecerem ataques à Altice e EDP.

Parecem poucos mas, salienta Pupo Correia, "Portugal tem um número enorme de casos de ransomware; só não aparecem nas notícias".

Segundo a Chainalysis, empresa de analítica de blockchain, os pagamentos de ransomware cresceram 337% entre 2019 e 2020, para mais de 400 milhões de dólares em criptomoeda. Até maio passado, o total conhecido atingiu os 81 milhões.

Apesar disto, a consultora Accenture nota no seu relatório "2021 Future Cyber Threats" que os grupos estão mais hostis e, mesmo após serem pagos,

They seem few but, as Pupo Correia points out, 'Portugal has a huge number of ransomware cases; they just don't make it to the news.'

According to Chainalysis, a blockchain analytics company, ransomware payments grew by 337 % between 2019 and 2020 to over $400 million in cryptocurrency. As of last May, the total amount known had reached $81 million.

In spite of this, the consulting company Accenture notes in its '2021 Future Cyber Threats' report that the groups are becoming more hostile and, even after being paid, avoid the recovery of the affected systems.

'We are on the cusp of a global pandemic,' said Christopher Krebs, the first director of the Cybersecurity and Infrastructure Security Agency. However, 'it is not an unsolvable problem. To solve it, one just needs to have updated backed up data and recovery plans in case of attack,' remembers IST's director.

'The problem is cultural: the digitization of our society is too recent and organisations have not realised quickly enough that there are associated risks. On the other hand, despite the saying "better be safe than sorry", our organizations are prone to do the

evitam a recuperação dos sistemas afetados.

"Estamos à beira de uma pandemia global", referiu Christopher Krebs, o primeiro diretor da Cybersecurity and Infrastructure Security Agency. No entanto, "não é um problema intratável. Para o resolver basta ter backups atualizados dos dados e planos de recuperação em caso de ataque", lembra o responsável do IST.

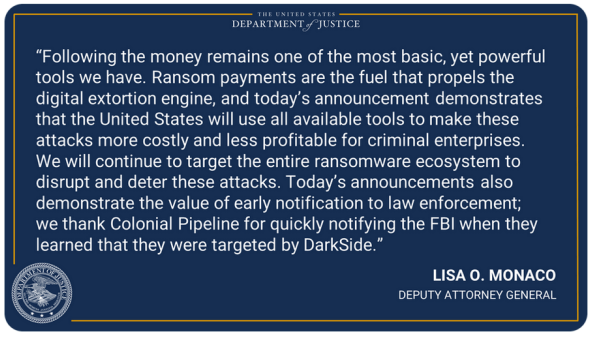
"O problema é cultural: a digitalização da nossa sociedade é demasiado recente e as organizações não se aperceberam suficientemente depressa que existem riscos associados. Por outro lado, apesar do ditado 'mais vale prevenir do que remediar', as nossas organizações são propensas a fazer o contrário: remediar em vez de prevenir. Nomeadamente, em termos de cibersegurança, não se apercebem que quando quiserem remediar já pode ser tarde demais e terem ficado sem dados ou sem sistemas. Muitas organizações também não se apercebem que sem dados ou sistemas vão à falência. Esse é o problema do ransomware: a falta de prevenção pode ser letal". ■

opposite: to remedy rather than to prevent. Namely, in terms of cybersecurity, they do not realise that, when they want to remedy, it may already be too late and they might have run out of data or systems. Many organizations also do not realise that, without data or systems, they will go bankrupt. That's the problem with ransomware: the lack of prevention can be lethal.' ■

Justice Department @TheJusticeDept · Jun 7

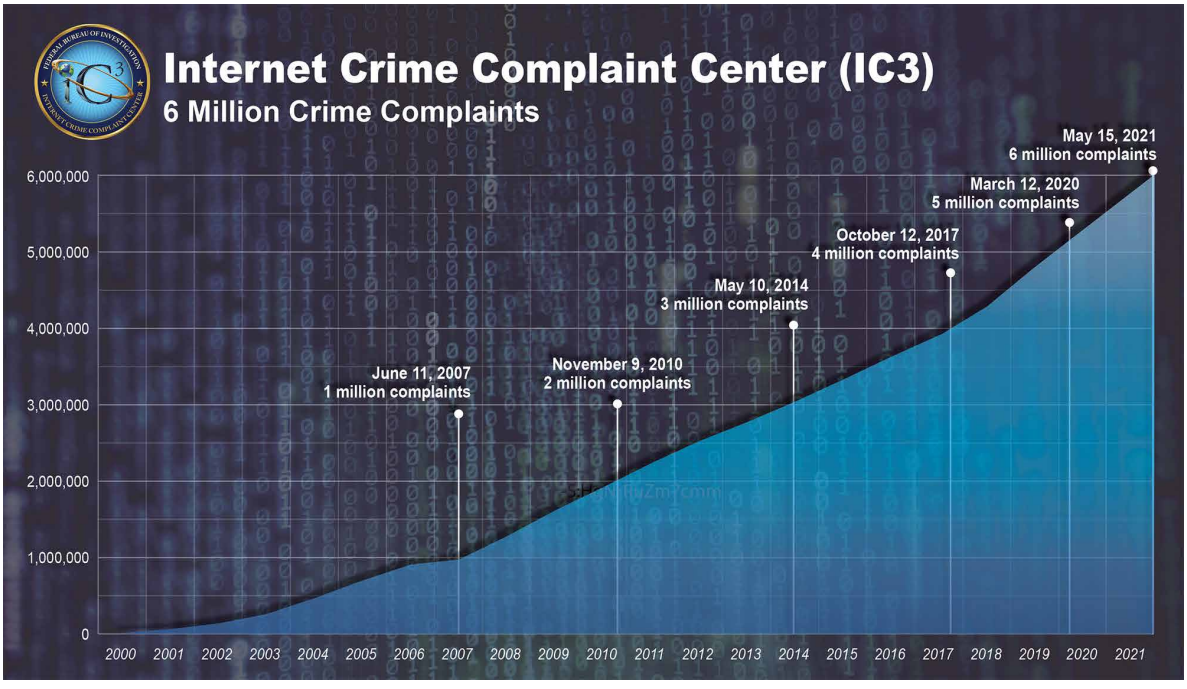
Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside

justice.gov/opa/pr/departm...



IC3 regista 6 milhões de queixas

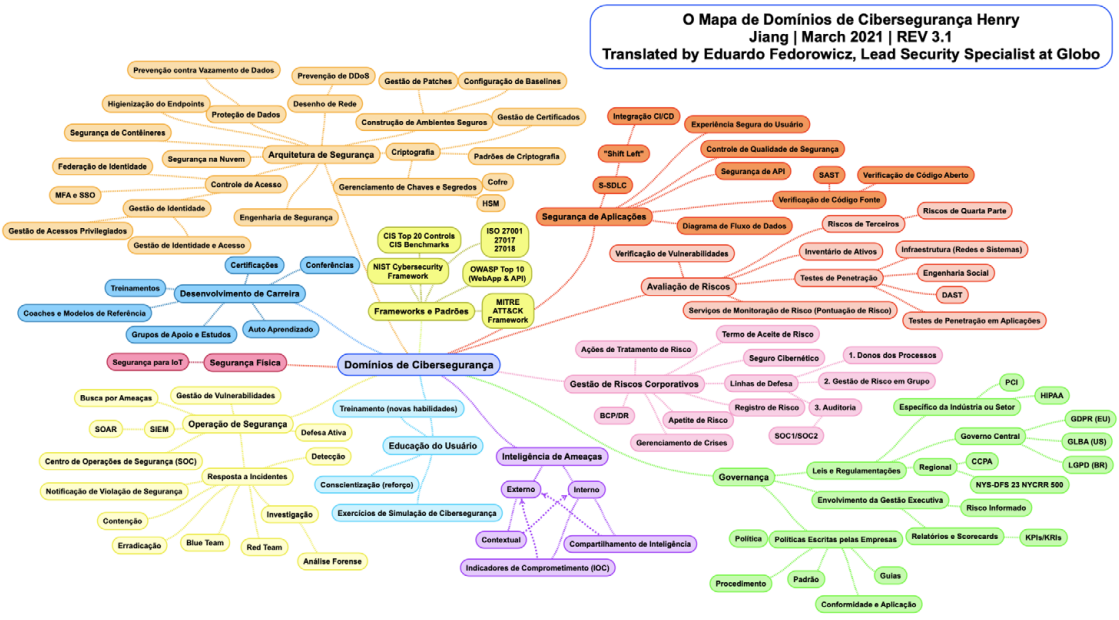
"Demorou quase sete anos para o Internet Crime Complaint Center (IC3) do FBI registar o primeiro milhão de reclamações. Demorou apenas 14 meses para adicionar o milhão mais recente".

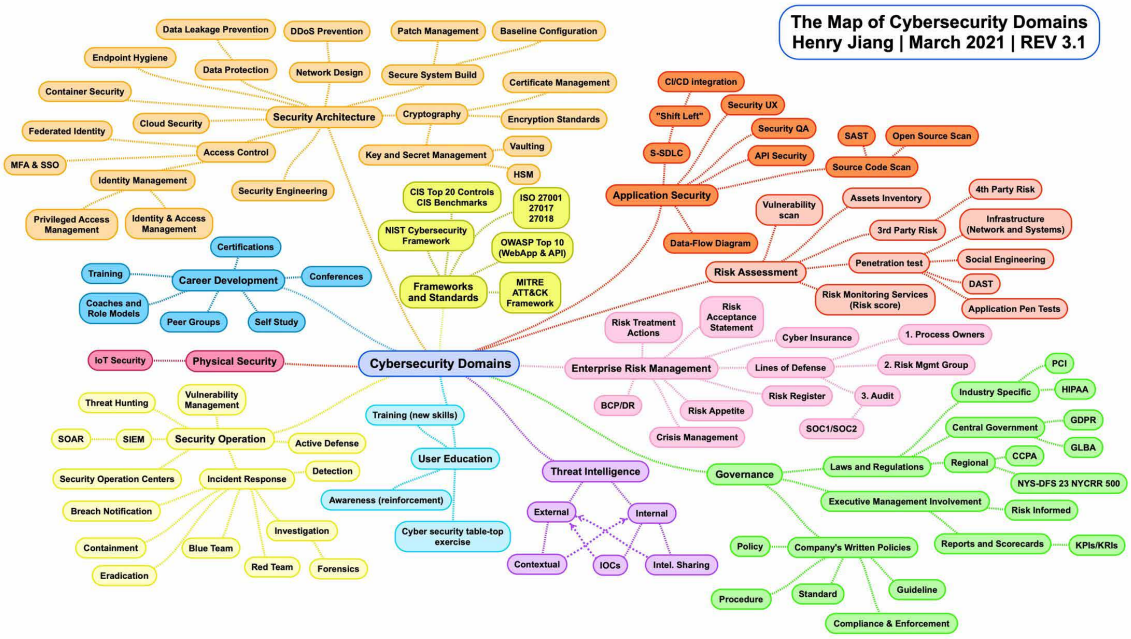


IC3 Logs 6 Million Complaints

"It took nearly seven years for the FBI's Internet Crime Complaint Center (IC3) to log its first million complaints. It took only 14 months to add the most recent million".

Mapa dos Domínios da Cibersegurança





3

Inês Esteves

Vogal do Conselho Diretivo do .PT
Member of .PT's Board of Directors

1. Quais são os objectivos do Centro de Operações de Segurança do .PT (PTSOC)?

Enquanto registry nacional, o .PT assume um papel essencial na manutenção da confiança e segurança do ciberespaço nacional, tendo a responsabilidade de garantir elevados níveis de qualidade, resiliência e fiabilidade os quais assegurem a efetiva proteção do domínio de topo de Portugal contra um número crescente de ameaças que podem comprometer o exercício das suas operações. A necessidade de proteção efetiva das funções críticas cometidas ao .PT, que leva a que esteja qualificado à luz da lei nacional como operador de serviços essenciais, enquadrado em concreto no setor das infraestruturas digitais, foi sempre um pilar fundamental na sua gestão, pelo que assume, desde o início, o compromisso de estudar e implementar continuamente soluções que permitam ser mais resiliente e seguro e, simultaneamente, promover a confiança da comunidade internet nacional.

O PTSOC nasce precisamente deste posicionamento e tem dois grandes objetivos de atuação: por um lado, acelerar e aprofundar internamente as capacidades de deteção, resposta e prevenção de incidentes de segurança e ameaças cibernéticas, dotando o .PT dos meios tecnológicos, processuais e humanos necessários à proteção da sua infraestrutura e serviços críticos e, por outro, densificar os níveis de cooperação no contexto do ecossistema da gestão dos nomes de domínio, em particular com a autoridade nacional, com a indústria de registrars e a comunidade de utilizadores, contribuindo, desta forma, para a preservação de um ciberespaço mais seguro e confiável sob .pt.

1. What are the objectives of .PT's Security Operations Centre (PTSOC)?

As a national registry, .PT takes on an essential role in maintaining the trust and security of the Portuguese cyberspace, having the responsibility to guarantee high levels of quality, resilience and reliability which ensure the effective protection of Portugal's TLD against a growing number of threats that may compromise their operations. The need for an effective protection of .PT's critical functions, which leads it to being qualified, under Portuguese law, as an essential services operator, specifically framed within the digital infrastructure sector, has always been a fundamental pillar in its management, which is why it takes on, from the beginning, the commitment to continuously study and implement solutions that allow it to be more resilient and secure and, at the same time, promote the trust of the Portuguese internet community.

The PTSOC was born precisely from this position and has two main objectives of action: on the one hand, to accelerate and internally deepen the capabilities for detection, response and prevention of security incidents and cyber threats, providing .PT with technological, procedural and human means necessary to protect its infrastructure and critical services. On the other hand, to enhance cooperation levels in the context of domain names management, namely with the Portuguese authority, with the registrars industry and user community, thus contributing to the preservation of a safer and more reliable cyberspace under .pt.

2. What services does PTSOC offer?

Through a collaborative approach, of shared responsibility with .PT's stakeholders, the PTSOC aims to strengthen cooperation in the domains of cybersecurity, positioning itself as a reference partner in the adoption of good practices and standards of security, in the development of key competences and self-awareness for the themes of cybersecurity, sharing knowledge and relevant information that contribute to a greater resilience and security of online presence and communication.

2. Qual é a oferta de serviços do PTSOC?

Através de uma abordagem colaborativa, de responsabilidade partilhada com as partes interessadas do .PT, o PTSOC pretende reforçar a cooperação nos domínios da cibersegurança, posicionando-se como um parceiro de referência na adoção de boas práticas e standards de segurança, no desenvolvimento de competências-chave e self-awareness para os temas da cibersegurança, na partilha de conhecimento e informação relevante que contribuam para uma maior resiliência e segurança da presença e comunicação online. A oferta de serviços especializados do PTSOC concretizam estas dimensões de cooperação, nomeadamente ao nível da:

- Deteção e comunicação de DNS Abuse na zona .pt;
- Investigação e partilha de indicadores de compromisso (IOC);
- Identificação e apoio na resposta a incidentes de segurança na zona .pt;
- Identificação e partilha de vulnerabilidades relevantes;
- Conceção e partilha de guias e materiais sobre segurança da informação;
- Implementação de referenciais de segurança;
- Sensibilização e formação;
- Disponibilização de serviços e soluções que contribuam para uma maior segurança e resiliência da presença e comunicação online em .pt, como o Webcheck e o Registry Lock.

3. Porquê lançar esta publicação?

Através do seu centro de operações de segurança, o .PT assume também o compromisso de uma atuação mais participativa e cooperante para os temas da segurança no ciberespaço. Esta publicação, que se pretende trimestral, dirigida aos registrars e registrants de .pt, aos parceiros e partes interessadas, é também uma concretização desse propósito. Pretendemos que seja um espaço de referência, aberto e independente de partilha de informação e conhecimento, mas também de debate, que cremos relevante, sobre temas atuais, boas práticas e tendências registadas no contexto da segurança no ciberespaço.

PTSOC's specialised services embody these cooperation dimensions, namely at the level of:

- DNS Abuse detection and communication in the .pt zone;
- Research and sharing of indicators of commitment (IOC);
- Identification and support in responding to security incidents in the .pt zone;
- Identification and sharing of relevant vulnerabilities;
- Conception and sharing of guides and materials on information security;
- Implementation of security benchmarks;
- Awareness raising and training;
- Provision of services and solutions that contribute to a greater security and resilience of online presence and communication on .pt, such as Webcheck and Registry Lock.

3. Why launch this publication?

Through its security operations centre, .PT is also committed to a more participatory and cooperative action on the cyberspace security issues. This publication, intended to be quarterly, addressed to .pt registrars and registrants, partners and stakeholders, is also a realization of this purpose. We want it to be a reference space, open and independent to share information and knowledge, but also a space for debate, which we believe to be relevant, on current topics, good practices and trends on the context of cyberspace security.

Principais indicadores | Main indicators

* DNS Abuse is a domain name that intentionally or unintentionally supports malware, phishing, pharming, botnets and/or spam dissemination activities. More information in the FAQs at www.dns.pt

Security channels
abuse@: public channel, made available to the community to report potential security incidents to .PT.
security@: internal channel, made available to the .PT Team, for the communication of potential security incidents.
siem@: internal solution to identify potential security incidents using the analysis and correlation of activity records in our systems and applications.

Ricardo Pires

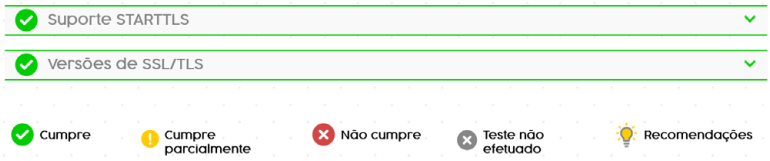
.PT Cybersecurity Manager

A plataforma Webcheck.pt é uma iniciativa conjunta do Centro Nacional de Cibersegurança (CNCS) e da Associação DNS.PT (.PT) que tem como objetivo promover a adoção de boas práticas e standards que contribuam para garantir a segurança das comunicações através da internet.

A Webcheck.pt permite a qualquer cidadão ou entidade, de forma muito acessível, verificar se uma página de internet e serviço de correio eletrónico implementam da forma mais segura standards para a comunicação segura entre sistemas como, por exemplo:

Webcheck.pt is a joint initiative of the Portuguese National Cybersecurity Center (CNCS) and Associação DNS.PT (.PT) to promote the adoption of good practices and standards that contribute to ensure the security of Internet communications.

Webcheck.pt allows any citizen or entity to verify, in an easily accessible and in the most secure way, if a given webpage and email service implement standards for a secure communication between systems, such as:



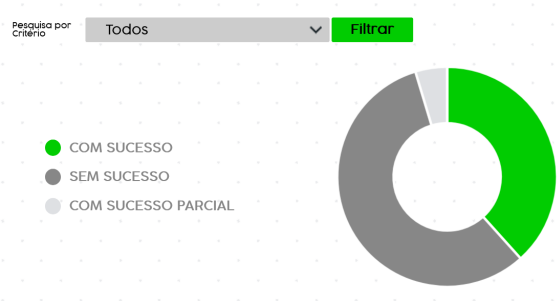
- HTTP/S: permite impedir que as comunicações entre o navegador (browser) e o servidor da página de internet possam ser intercetadas e/ou manipuladas por terceiros.

- DNSSEC: impede que as informações trocadas entre servidores DNS e entre estes servidores e as aplicações do utilizador possam ser manipuladas por terceiros.

- SPF: previne a utilização abusiva do domínio por terceiros não autorizados para envio de correio eletrónico mal-intencionado.

Como resultado do teste efetuado na webcheck.pt é apresentado ao utilizador um relatório sistematizado do estado atual de conformidade da página de internet e/ou serviço de correio eletrónico pesquisado. Se todos os standards estiverem corretamente implementados é associado a cada uma das categorias o símbolo, reconhecendo-se o cumprimento dos requisitos de segurança para a presença e comunicação online, com destaque no "Hall of Fame" desta plataforma.

Para auxiliar a implementação dos principais standards avaliados, a Webcheck.pt disponibiliza ainda um conjunto de informação técnica e tutoriais que podem ser consultados no menu "Recomendações" desta plataforma.



- HTTP/S: prevents communications between the browser and the web server from being intercepted and/or manipulated by third parties.

- DNSSEC: prevents information exchanged between DNS servers and between these servers and user applications from third party manipulation.

- SPF: prevents misuse of the domain by unauthorized third parties to send malicious email.

As a result of the test performed at Webcheck.pt, the user is presented with a systematised report on the searched website and/or email service current compliance status. If all standards are correctly implemented, each category is awarded a symbol, recognising compliance with the safety requirements for online presence and communication, highlighted in this platform's 'Hall of Fame'.

To assist the implementation of the main standards assessed, Webcheck.pt also provides a set of technical information and tutorials that can be consulted under this platform's "Recommendations" menu.

Cibersegurança em Portugal: Riscos & Conflitos 2021

(Observatório de Cibersegurança)

O relatório do Observatório de Cibersegurança salienta como "os incidentes de cibersegurança e os indicadores de cibercrime cresceram de forma significativa em 2020", com uma "coincidência temporal" relacionada aos confinamentos. As ameaças mais relevantes ocorreram ao nível do phishing/smishing, malware e ransomware, normalmente acompanhadas por técnicas de engenharia social. Os principais culpados pelas ameaças foram cibercriminosos e agentes estatais.

Cybersecurity in Portugal: Risks & Conflicts 2021

(Cybersecurity Observatory)

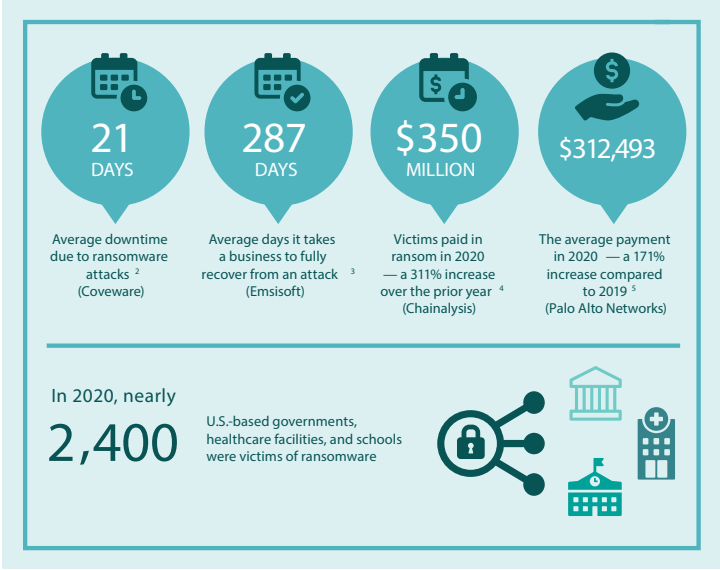
The Cybersecurity Observatory report stresses how 'cybersecurity incidents and cybercrime indicators grew significantly in 2020', showing a 'temporal coincidence' between them and lockdowns. The most relevant threats were phishing/smishing, malware and ransomware, usually accompanied by social engineering techniques. The main culprits for these threats were cybercriminals and state agents.

Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force

(Institute for Security and Technology)

Os especialistas e autores do documento classificam o ransomware como "ameaça à segurança nacional". A maioria dos cibercriminosos opera com alguma impunidade e as barreiras à entrada de novos elementos são muito baixas. O modelo de "ransomware as a service" facilita os crimes a iletrados tecnológicos. Governos e indústrias têm aqui 48 propostas de ação para intervir neste modelo de negócio.

Experts and the document's authors classify ransomware as a 'threat to national security'. Most cybercriminals operate with some impunity and barriers to entry to new elements are very low. The 'ransomware as a service' model makes crimes easier for criminals without technology sophistication. This report includes 48 actions that governments and industries can pursue to intervene in this business model.



2021 Voice of the CISO Report
(Proofpoint)

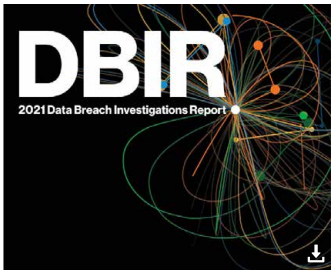
66% dos Chief Information Security Officer (CISO) sentem-se mal preparados para lidar com ciberataques e estão mais preocupados em 2021 do que no ano passado. 58% dos 1.400 CISOs entrevistados em todo o mundo confirmaram o erro humano como a maior fragilidade na cibersegurança. Ataques ao email (34%), à presença na cloud (33%), as ameaças internas (31%) ou o ransomware (27%) integram os principais temores.

66 % of Chief Information Security Officer (CISO) feel ill-equipped to deal with cyberattacks and are more concerned in 2021 than in the previous year. 58 % of the 1 400 CISOs interviewed around the world confirmed human error was the greatest weakness when it came to cybersecurity. Attacks on email (34 %), cloud presence (33 %), internal threats (31 %) or ransomware (27 %) are among the main fears.

Global Threat Intelligence Report
(NTT)

Em 2020, os ciberataques aumentaram 200% no setor da saúde, 300% na fabricação e 53% na indústria financeira. Estes três setores foram visados por 62% de todos os ataques, enquanto a criptomineração foi responsável por 41% de todo o malware, com o maior impacto sentido no setor educativo. A segurança na cloud será uma prioridade nos próximos 18 meses.

In 2020, cyberattacks increased by 200 % in the health sector, 300 % in manufacturing and 53 % in the financial industry. These three sectors were targeted by 62 % of all attacks, while cryptomining was responsible for 41 % of all malware. The greatest impact was felt in the education sector. Cloud security will be a priority for the next 18 months.



Data Breach Investigations Report
(Verizon)

Na região EMEA (Europe, Middle East and Africa), o DBIR salienta que os ataques a aplicações Web e a engenharia social foram responsáveis pela maioria das falhas de segurança, aproveitadas principalmente por atores externos (83%), motivados por ganhos financeiros (89%) e espionagem (8%). Derivado da pandemia, aumentaram os ataques de phishing e ransomware a profissionais em teletrabalho.

In the EMEA (Europe, Middle East and Africa) region, the DBIR points out that attacks on web applications and social engineering were responsible for most security flaws, mainly due to external actors (83 %), motivated by financial gains (89 %) and espionage (8 %). Due to the pandemic, there was in increase in the number of phishing and ransomware attacks to professionals working from home.

Directora | Director
Inês Esteves

Edição
Pedro Fonseca

Design gráfico | Graphic design
Sara Dias

Tradução | Translation
Sara Pereira

Fotografia de Capa | Cover Photography
Christopher Farrugia

Publicação trimestral | Quarterly publication
Junho 2021 | June 2021

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia