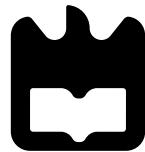


CIBERCRIMINALIDADE

os casos mais impactantes

Universidade de Aveiro

Joana Gião, Matilde Sanches



VERSAO 1

CIBERCRIMINALIDADE

os casos mais impactantes

Dept. de Eletrónica, Telecomunicações e Informática
Universidade de Aveiro

Joana Gião, Matilde Sanches
126489 joanagiao@ua.pt, 125369 matilde.sanches@ua.pt

29 de novembro de 2024

Resumo

Nesta era digital, é quase impossível não ter sido vítima de, pelo menos, uma tentativa de ataque cibernético. Estes ataques tornaram-se muito comuns porque a internet possibilitou algo que todos os criminosos desejavam, "uma nova identidade". Ou seja, um criminoso pode muito bem cometer crimes e nunca ser apanhado pelos mesmos. É destes casos e mais que este relatório se focou.

Deste modo, este trabalho tem como objetivo analisar o impacto que o cibercrime consegue ter no mundo e abordar a importância da cibersegurança, a única solução para este tipo de ataque.

Através de uma análise dos casos apresentados, são explorados os perigos da tecnologia e as suas consequências. Estas consequências indicam que, embora esta melhore a nossa vida quotidiana, também pode ter um impacto muito negativo na mesma se não estivermos devidamente informados. Esta análise também revela que a proteção cibernética é igualmente crucial para as grandes empresas e para utilizadores comuns.

Com isto, conclui-se que a falta de investimento e conhecimento em medidas de segurança aumenta a vulnerabilidade a ataques informáticos. Isto é, empresas bem preparadas, com políticas de segurança atualizadas e bons profissionais na área conseguem reduzir os riscos de maneira mais eficaz.

Índice

1	Introdução	1
2	Os Crimes	2
2.1	O rapaz que roubou milhões de euros com o computador	2
2.2	Os adolescentes que hackearam a Central Intelligence Agency (CIA)	4
2.3	A Koobface <i>Gang</i>	5
2.4	A criadora da <i>OneCoin</i>	7
2.5	Os Hackers da Coreia da Norte	8
2.6	O rapaz que hackeou a The National Aeronautics and Space Administration (NASA)	10
3	A Solução	12
3.1	A importância da Cibersegurança	12
3.2	A evolução dos Ciberataques e da Cibersegurança	12
4	Conclusões	16

Lista de Figuras

2.1	Evil Corp	2
2.2	Maksim com polícia e Lamborghini atrás	3
2.3	Audi R8 alterado	3
2.4	John Brennan	4
2.5	Foto publicado por um membro da Koobface que mostra o escritório e as suas coordenadas em St.Petersburg	6
2.6	Alguns membros da gangue	6
2.7	Ruja Ignatova	7
2.8	Estabelecimento da OneCoin	8
2.9	Lazarus	9
2.10	Jonathan James	10
2.11	NASA	11
2.12	Estação Espacial Internacional	11
3.1	Quebras de informação em 2022, Fonte: Identity Theft [12]	13
3.2	Quebras de informação em 2023, Fonte: Identity Theft [12]	13
3.3	Quebras de informação em 2024, Fonte: Identity Theft [12]	13
3.4	Tipos de ataques em 2022, Fonte: Crimes cibernéticos [13]	14
3.5	Tipos de ataques em 2017, Fonte: Crimes cibernéticos [13]	14

Capítulo 1

Introdução

Como a cibersegurança é algo muito relacionado ao nosso curso, Engenharia de Computadores e Informática, havendo até um mestrado da mesma, é pertinente aprofundar os nossos conhecimentos nesta área. Trata-se de um tema que desperta interesse e que é cada vez mais importante na sociedade atual.

Por essas mesmas razões, é oportuno realizar um trabalho que aborde o mesmo e que sensibilize a importância de nos mantermos informados e seguros no âmbito digital. O relatório apresenta o tema de forma indireta, através de uma exposição sobre a cibercriminalidade, apresentando os exemplos que se consideram mais impactantes e envolventes, de modo a compreender as consequências que uma rede insegura pode causar.

Para tal, no Capítulo 2, são abordadas as histórias de vários indivíduos com habilidades informáticas invejáveis, que lhes possibilitaram a cometer crimes maiores do que se esperava.

No Capítulo 3, chega-se ao cerne da questão e levanta-se o que poderia ter evitado todos estes crimes, a cibersegurança.

Finalmente no Capítulo 4, encontram-se as conclusões que são possíveis retirar com este relatório.

Capítulo 2

Os Crimes

Neste capítulo, vamos abordar os acontecimentos mais impactantes de cibercriminalidade até hoje.

2.1 O rapaz que roubou milhões de euros com o computador

O grupo russo de *hackers* “Evil Corp”, é acusado de roubar cerca de 300 milhões de euros em cerca de 10 anos. Alegadamente, o líder desse grupo é o informático, e *hacker*, Maksim Yakubets. Para além de líder deste grupo, o mesmo também é responsável pela conspiração do *malware* nomeado “Bugat”, também conhecido como Dridex ou Cridex. Este malware está programado para roubar as credenciais do banco das vítimas usando, maioritariamente, ataques de “phishing”, ou seja, fingindo ser uma entidade ou pessoa, de modo a fazer a vítima instalar o *malware*.



Figura 2.1: Evil Corp

No mais recente ataque, estes criminosos ligados ao *malware*, mandaram emails a membros do LinkedIn, como se fossem a própria empresa, a alertar

de mensagens não lidas, seguido de um link perigoso, no seguimento da abertura deste link, um *java applet*¹ foi instalado e, assim, o *malware* também o foi. Posteriormente, os *hackers* tiveram acesso a toda a *data* roubada, que, por suas vezes, utilizaram as informações para fraudes, como a "ACH fraud", que consiste em transferências não autorizadas feitas a partir da conta bancária utilizando a rede Automated Clearing House (ACH), rede que processa pagamentos e transferências eletrónicas nos Estados Unidos e no Canadá.

Este *malware*, ao longo do tempo, foi atualizado diversas vezes de modo a ser cada vez mais eficiente. A mais recente e conhecida versão rouba informações sensíveis a quem usa o Firefox e a quem usava o Internet Explorer (antigo Microsoft Edge). Este tipo de roubo costuma acontecer a médias empresas.

Para além do envolvimento no Bugat, Maksim Yakubets, também esteve muito envolvido no *malware* Zeus, conhecido também como Zeus Trojan Malware (Malware Cavalo de Troia Zeus), isto porque o mesmo atua como um cavalo de Troia, ou seja, vigia sites e regista as teclas que foram pressionadas no mesmo, para que quando o *malware* perceber que a vítima está no site, guardar as teclas usadas para o login. Desse modo, quebra toda a segurança e consegue aceder à conta da vítima. Conseguindo, assim, roubar municípios, bancos, organizações sem fins lucrativos e uma congregação religiosa, e ganhar cerca de 60 milhões de euros. [1]

Com estes dois *malwares*, o grupo conseguiu roubar mais de 100 milhões de euros.

Ainda, em 2017, o governo norte-americano afirmou que Maksim começou a trabalhar para os serviços secretos russos e que no ano a seguir estava a trabalhar para obter uma licença de acesso a informações confidenciais da mesma.

O mais interessante e revoltante desta história é o facto de Maksim Yakubets não precisar de se esconder, aliás, o mesmo exibe de forma exuberante o dinheiro. Na Figura 2.2 é possível verificar isso mesmo: Maksim com o seu lamborghini modificado, com "BOP"na matrícula, que significa ladrão em russo, a falar com um polícia, como se não fosse nada. Na Figura 2.3 é possível observar um Audi R8, alterado com o mesmo padrão e com a matrícula também alterada. Para além disso teve um casamento que custou cerca de 300 mil euros.



Figura 2.2: Maksim com polícia e Lamborghini atrás



Figura 2.3: Audi R8 alterado

¹java applet é um programa incorporado na página web. Ele funciona tanto dentro do navegador como no lado do cliente.

Isto acontece porque, mesmo com as imensas acusações americanas contra o *hacker* e com a oferta de uma recompensa de 5 milhões de euros a quem fornecesse informações sobre o paradeiro de Yakubets por parte do Departamento de Estado norte-americano [2], o governo russo ignora as acusações de crimes cibernéticos vindas dos Estados Unidos da América (EUA) contra os seus cidadãos. A National Crime Agency (NCA) continua a garantir que: “Se Maksim Yakubets deixar a segurança da Rússia, será imediatamente detido e extraditado para os Estados Unidos”. Porém, até hoje, parece que o mesmo não aconteceu e Maksim continua em liberdade.

2.2 Os adolescentes que hackearam a CIA

Em outubro de 2015, John Brennan, um dos homens mais poderosos da Terra, o chefe da CIA, recebe uma chamada telefónica de um estranho. Isto poderia ter parecido uma brincadeira comum. "Quem é? Como conseguiu este número? O governo dos EUA classificará esta chamada como parte de uma grande conspiração de roubo de identidade, assédio a funcionários do governo e ciberterrorismo." O estranho exigiu que parassem de bombardear o Médio Oriente antes de desligar. Um miúdo de 15 anos, no seu quarto, com o telefone ainda na mão, não consegue acreditar no que acabou de fazer. Ele é líder dos Crackers With Attitude, um grupo que aterrorizou e humilhou as organizações secretas do EUA.

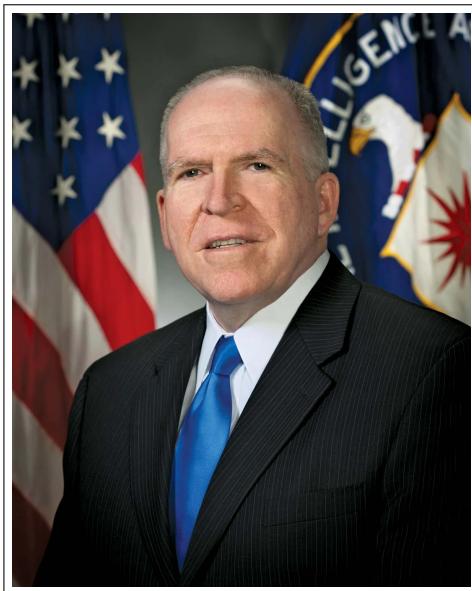


Figura 2.4: John Brennan

Cada vez mais, os *hacks* deste grupo eram motivados pelo altruísmo, em

vez da simples curiosidade. Como por exemplo, em 2014, quando a bestialidade era legal na Dinamarca. Outros países europeus, como a Alemanha, o Reino Unido e a Suécia, já a tinham proibido. Isto significou para a Dinamarca um aumento do turismo sexual com animais. Durante anos, os ativistas pelos direitos dos animais na Dinamarca tentaram chamar a atenção para esta situação. Chamavam-lhe "canil de cães". O rapaz, de nome Kraker, tinha um cão e isso irritou-o, levando o grupo a desligar o site oficial do governo dinamarquês e depois desfiguraram-lo. Não só isto, mas também desligaram sites através de ataques de negação de serviço e publicaram no Twitter provas de animais sexualmente maltratados. A informação repercutiu-se em todo o mundo e foi amplamente condenada [3].

Enquanto isso, em Virgínia, um rapaz que se autodenomina "default" começou a aprender tudo o que era possível sobre computadores apenas guiado pela curiosidade. Ele ficou impressionado com um grupo chamado Anonymous no início, mas começou a perder o interesse quando entendeu que o grupo estava a crescer astronomicamente, tornando difícil saber em quem confiar. Então, este junta-se ao grupo *krakas with Attitude* unidos pelo ódio que tinham contra o governo americano especialmente com a sua posição no conflito entre Israel e a Palestina. Hackearam documentos confidenciais de membros da Intelligence Community conseguindo entrar no email de um dos membros mais importantes da mesma. Em outubro de 2015, o grupo publicou os documentos incluindo o formulário SF-86 de 47 páginas de Brennan, um documento sensível exigido para obter uma autorização de segurança governamental de alto nível. Além disso, a partir dos e-mails de Brennan, o WikiLeaks publicou recomendações da era Bush sobre como a presidência deveria operar no Médio Oriente.

Infelizmente, devido a dois deslizes, um dos membros acabou por se entregar ao contar a uma rapariga o que eles faziam enquanto estava bêbado. Consequentemente, Default recebeu uma visita do Federal Bureau of Investigation (FBI) no dia seguinte que encontrou todo o seu equipamento e prendeu-o de imediato. Kraka é também preso pelas forças policiais Inglesas. Default foi condenado a 5 anos de prisão, com uma multa de 145 mil dólares. Atualmente, Kraka deixou a vida de crime e está atualmente a estudar cibersegurança [4].

2.3 A *Koobface Gang*

No ano de 1997 o website mais popular é o Yahoo! Com mais de 17 milhões de utilizadores ativos por mês a descobrir um novo mundo: a internet. No entanto dia 8 de dezembro às 7 da noite, o Yahoo é hackeado. Qualquer pessoa que abra o browser terá uma mensagem no seu computador a dizer que todos os computadores que acederam ao Yahoo no mês passado serão destruídos por uma bomba que será detonada no Natal. Isto é, apenas se as exigências dos hackers não forem cumpridas, que se referem a libertar um tal Kevin. E muitos se perguntaram, quem é o Kevin? Ele não é um chefe da máfia ou um assassino, e ele não está na prisão por ter ameaçado agentes dos estados unidos. Este indivíduo é muito mais perigoso do que isto: dizem que com apenas uma chamada

telefónica ele consegue entrar e tomar controlo do arsenal nuclear dos EUA.

No início, o grupo KoobFace utilizava contas manualmente criadas para espalhar o vírus mas com o crescimento das empresas, estes precisavam de uma maneira de autocriar dezenas de contas falsas que passassem pelas verificações humanas e atrair as suas vítimas. Primeiro, o login e a password são codificadas através de um processo que envolve ler letras e comparar o seu valor AC a uma string de números de 0 a 1, de 2 a 3 a 4 conseguindo assim entrar na plataforma e personalizando o perfil com informações pessoais autogeradas que parecem realistas o suficiente. De seguida, o site pede CAPTCHA. Para circundar isto, o puzzle é espelhado na área de trabalho de qualquer indivíduo do seu exército de bots. Milhões de pedidos de amizade são mandados na rede social Facebook conseguindo infetar cerca de 600 mil máquinas.

Um dia, sem qualquer explicação aparente, o controlo de comandos simplesmente fica offline. Desde então o seu centro de controlo original nunca mais foi ativado. Os seus membros continuam por aí, e os vírus dormentes nos computadores infetados.

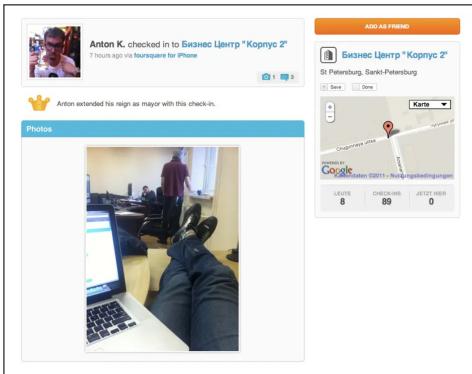


Figura 2.5: Foto publicado por um membro da Koobface que mostra o escritório e as suas coordenadas em St.Petersburg



Figura 2.6: Alguns membros da gangue

Quando criança, Kevin infiltrou-se no sistema dos Estados Unidos por pura diversão. Mais tarde foi apanhado e preso por 12 meses. No entanto no seu

julgamento, Kevin mostra as suas incríveis habilidades de manipulação, conseguindo manipular o juiz a libertá-lo mais cedo. O hacker rouba milhares de empresas mas acaba por ser apanhado devido a um deslize. Kevin provocou um hacker de elite que conseguiu descobrir onde este vivia. Este quase conseguiu escapar da situação, mas um dos agentes do FBI encontra um paycheck com o nome dele. É preso por cerca de quatro anos. A noite de Natal passa sem problemas, não há bomba e o site Yahoo voltou ao normal. Quando saiu da prisão, Kevin ajudou o governo a fortalecer a sua segurança digital, tornando-se um "White hacker".

Informações encontradas num artigo do New York Times [5].

2.4 A criadora da *OneCoin*

Em 2014, A OneCoin foi criada, uma suposta criptomoeda rival da original Bitcoin, uma grande promessa para retornos gigantes. Esta moeda foi criada por Ruja Ignatova, também conhecida por "rainha das criptomoedas", antiga estudante de Oxford e doutorada em Direito Privado Europeu na Universidade de Kontanz, Alemanha [1].



Figura 2.7: Ruja Ignatova

A OneCoin foi um sucesso! Ignatova convenceu milhares de investidores de mais 170 países a investirem na moeda através de uma plataforma de cursos online sobre criptomoedas e tokens. Estes tokens eram depois usados para obter as tais OneCoins. Mas na verdade, o que Ruja escondia, era que por trás da moeda, esta totalmente falsa, estava uma fraude de investimento imensa, sem o registo digital subjacente às criptomoedas de facto legítimas, que levou a diversos alertas por parte das autoridades financeiras e bancos nacionais. Mesmo assim, entre 2014 e 2016, Ignatova conseguiu lucrar cerca de 3,5 mil milhões de euros [1].



Figura 2.8: Estabelecimento da OneCoin

Com tanto lucro, era muitas vezes vista a frequentar os mais ricos locais. Porém, ao contrário do caso de Maksim, tratado acima, Ignatova não conseguiu viver em legítima liberdade depois deste esquema. A OneCoin foi investigada e descobriram tudo. O dinheiro era feito pela angariação de novos clientes, e não pela valorização da moeda, tal como qualquer esquema em pirâmide. Assim, em janeiro de 2017, a plataforma foi encerrada. Com as buscas, em outubro de 2017, Ignatova fugiu para Atenas e nunca mais foi encontrada. Diz-se que a mesma fez uma cirurgia plástica de modo a passar despercebida nas ruas e complicar a descoberta do seu paradeiro [1].

Atualmente, é a única pessoa diretamente relacionada com a OneCoin que ainda não foi presa. O cofundador, Sebastian Greenwood foi preso com 20 anos de prisão, e o irmão da mesma, Konstantin Ignatov, foi preso também, porém já se encontra em liberdade, depois de 34 meses atrás das grades pois o mesmo concordou com 2 anos sob supervisão judicial e devolveu 118 mil euros dos fundos que conseguiu ao trabalhar na OneCoin. A rainha das criptomoedas continua em liberdade e tornou-se parte dos 10 mais procurados do FBI [6].

2.5 Os Hackers da Coreia da Norte

A Coreia do Norte começou a investir desde muito cedo em ciber operações, roubando milhões de dólares a bancos, crypto e companhias, o que atraiu a atenção global. Dois dos mais famosos são:

- o *hack* da Sony Pictures em 2014
- o banco do Bangladesh em 2016

Este tipo de operações, que necessitam de muito pouco investimento e têm grande recompensa permitiram ao governo de se estabelecer e se financiar. Os hackers da Coreia do Norte são estritamente treinados e monitorizados para prevenir a sua lealdade sendo um dos departamentos mais secretos e restritos do país. Estas operações são normalmente realizadas pelo grupo Lazarus que treina hackers do mais alto nível, envolvidos em diversas operações a escala mundial. Com o crescimento deste grupo, o investimento em cibersegurança subiu drasticamente, especialmente depois do ataque ao governo da Coreia do Sul, que custou milhões de dólares a este [7].



Figura 2.9: Lazarus

A história de Jong Yuli começa numa pequena cidade da Coreia do Norte, um país em que o estatuto social e as oportunidades de vida estão fortemente dependentes da família em que nasceste e o seu status. Jong nasceu numa família relativamente boa, dando-lhe espaço para se focar nos estudos. Desde muito pequeno que tinha um talento especial com números e seu pai decidiu investir nesse talento, o que o levou mais tarde a ser selecionado para as Olimpíadas Internacionais da Matemática (OIM). Devido ao facto da Coreia do Norte levar as competições muito mais a sério, Jong passou por uma preparação muito rigorosa, passando horas a resolver problemas complexos que não só tem o objetivo de melhorar as suas capacidades matemáticas, mas também o seu senso de patriotismo e dever para com o país.

Depois da sua primeira saída do país para as OIM em Colômbia, Jong apenas obteve a medalha de prata e não a de ouro, o que levou ao descontentamento do regime já que tinham investido muito para o treino dele, esperando que este ganhasse o ouro. Yuli começou a perguntar-se o porquê de o seu país investir tanto

em jovens como ele, e a perguntar-se sobre os seus objetivos, descobrindo através de um amigo que o governo estava a interrogar a sua família e a prepararem-se para o treinarem para ser um hacker.

Jong percebeu que se fosse selecionado não teria o direito de recusar, e que viveria num regime restrito e afastado da sociedade. Como tinha até aos 18 anos para participar nas Olimpíadas, percebeu que a sua última oportunidade para escapar do país seria em 2016. Depois de ganhar prata novamente, Jong aproveitou a chance e entrou em contacto com diplomatas da Coreia do Sul, que negociaram pacificamente a sua saída. Nos 2 anos que se seguiram a Coreia do Norte suspendeu a sua participação nas Olimpíadas e devido a este incidente, os participantes são acompanhados por um agente, para impedir que escapem.

Jong vive agora na Coreia do Sul sob outro nome, tendo estudado Matemática na universidade. Ele nunca mais viu os pais desde que escapou.

2.6 O rapaz que hackeou a NASA

NASA, o sistema mais seguro do mundo, invadido por um rapaz de 15 anos. Jonathan James foi um *hacker* dos EUA. Foi a primeira pessoa a ser presa por um cibercrime na América com 16 anos no ano 2000, um ano depois de cometer o seu maior crime cibernético: Invadir a NASA.

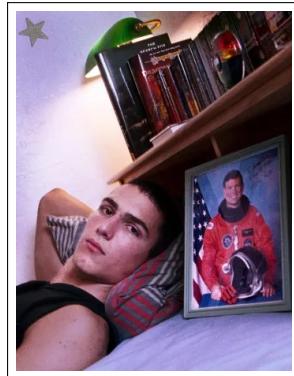


Figura 2.10: Jonathan James

Como qualquer criança, James jogava horas a fio no computador, ainda mais por o ser pai ser programador e o computador estar muito presente na sua vida. O problema começou quando o mesmo se começou a interessar mais em como o computador funcionava do que nos jogos. Numa entrevista em 1990, o pai de Jonathan disse que um dia chegou a casa e o filho tinha substituído o Windows pelo o Linux, num tempo em que o conhecimento tecnológico não era nem metade do que é hoje.

A partir daí, foi-se interessando cada vez na arte da programação, e por diversão, invadia vários servidores. Em junho de 1999, Jonathan encontrou um servi-

dor com uma segurança vulnerável em Alabama, o mesmo plantou um malware e ganhou o controlo de 13 outros computadores no sistema. James depois reparou que conseguiu acesso ao Marshall Space Flight Center, em Huntsville, uma unidade que trabalha em desenvolver foguetes e mantinha comunicações com a Estação Internacional do Espaço. Conseguiu roubar 1,7 milhões de euros em textitdata. Foi depois revelado que muita da informação roubada era o código fonte para um software que controlava a temperatura e humidade do espaço vital da Estação Espacial Internacional (EEI), elementos vitais para a sobrevivência. Quando a NASA reparou na quebra de segurança, fecharam a rede por 21 dias, resultando em 41 mil euros de perda [8].

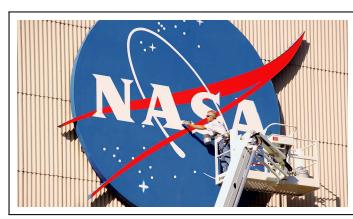


Figura 2.11: NASA



Figura 2.12: Estação Espacial Internacional

Daí adiante, o FBI focou-se em encontrar Jonathan. Tal aconteceu no dia 26 de janeiro de 2000. Como Jonathan tinha apenas 16 anos, acabou por ser sentenciado com 6 meses de prisão domeciliária e com uma proibição de uso do computador para qualquer outro assunto sem ser estudos. Para além disso, teve de escrever uma carta de desculpas para as empresas atacadas pelo mesmo, entre elas a NASA. Também teve de trabalhar para as mesmas ao mostrar exatamente como conseguiu aceder aos sistemas. Mais tarde, Jonathan desrespeitou as regras e foi apanhado drogado na rua. Por essa razão, foi mandado para uma prisão juvenil em Alabama, onde permaneceu 6 meses. [9]

Tempos depois de regressar a casa, em janeiro de 2008, foi desmascarado um vírus e deduziram que James fez parte do mesmo por haver várias menções de um "JJ" e por ser amigo do líder desse ataque. Jonathan negou todas as alegações. Porém, mesmo assim, a polícia decidiu investigar a sua casa. Acabaram por não encontrar nada que ligasse Jonathan James e o vírus, mas encontraram uma pistola e uma carta de suicídio e mesmo assim, não desistiram da especulação. Duas semanas depois, Jonathan foi encontrado morto em casa, com uma carta ao lado, escrito: "(...) Eu não acredito no sistema da "justiça". Talvez as minhas ações hoje, juntamente com esta carta, transmitam às pessoas uma mensagem mais forte. De qualquer das formas, perdi o controlo desta situação, e esta é a única maneira de conseguí-lo de volta. (...) "de acordo com Daily Mail [10]. Mais tarde foi descoberto que "JJ" era de Jim Jones, apelido de Stephen Huntley Watt.

Capítulo 3

A Solução

3.1 A importância da Cibersegurança

Tal como referimos no Capítulo 1, a cibersegurança é um tópico de cada vez mais importância na sociedade atual, uma sociedade em que há cerca de 4000 ciberataques por segundo, e mais de 600 milhões de ataques por dia [11]. Uma das razões pelas quais este tipo de crime continua a aumentar é porque é barato, rápido e com uma alta recompensa e menos risco de ser apanhado, se comparado a outros tipo de crime.

Cibercrimes podem custar milhões às empresas em termos de danos, como visto no Capítulo 2 e não estamos a falar apenas de dinheiro, mas da credibilidade da mesma, a sua capacidade de fazer negócios bem como a segurança dos seus trabalhadores e afiliados. A cibersegurança é muito importante pois mantém os dados dos seus clientes privados e a salvo, dando-lhes a confiança necessária na marca utilizada. É importante que todas as empresas e indivíduos deem atenção à cibersegurança já que algumas instituições dependem de sistemas digitais para operar. Isto significa que uma violação de segurança pode causar interrupções afetando a receita da empresa, e em casos mais extremos a falência desta.

3.2 A evolução dos Ciberataques e da Cibersegurança

Como é possível ver acima, a cibersegurança é **muito importante** e por isso mesmo, é importante que a mesma evolua. Mas será que a mesma está a crescer da mesma forma que o uso da internet cresce atualmente?

Analizando os gráficos da Figura 3.1, da Figura 3.2 e da Figura 3.3, é possível verificar a quantidade de quebras de informação por indústria para diferentes anos. No ano de 2022, houve um pico de 973 quebras de informação em agosto, no ano de 2023, um pico de 1151 em setembro e, agora em 2024, o máximo

obtido foi de 525 em janeiro, até onde se sabe. Dentro disto, o ano de 2024 parece o mais controlado e com menos quebras de informação.

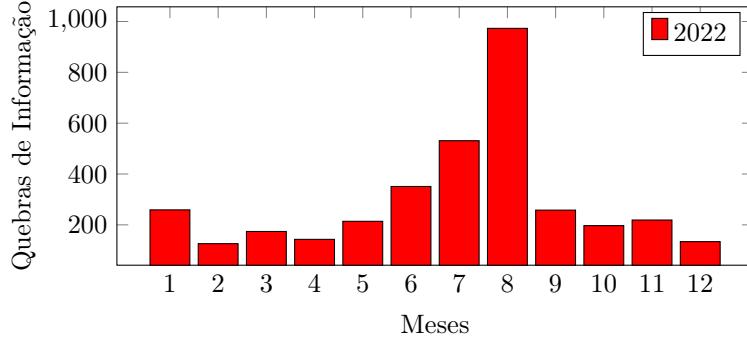


Figura 3.1: Quebras de informação em 2022, Fonte: Identity Theft [12]

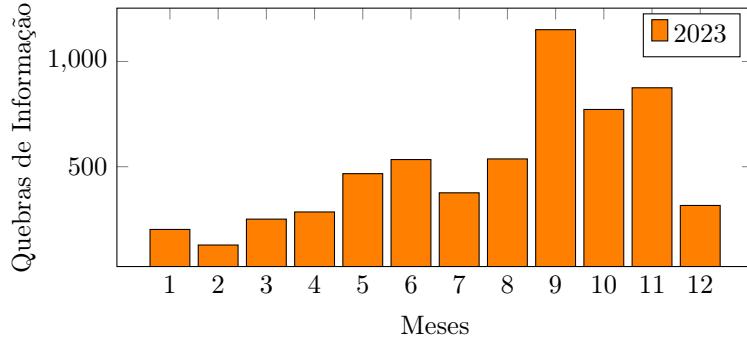


Figura 3.2: Quebras de informação em 2023, Fonte: Identity Theft [12]

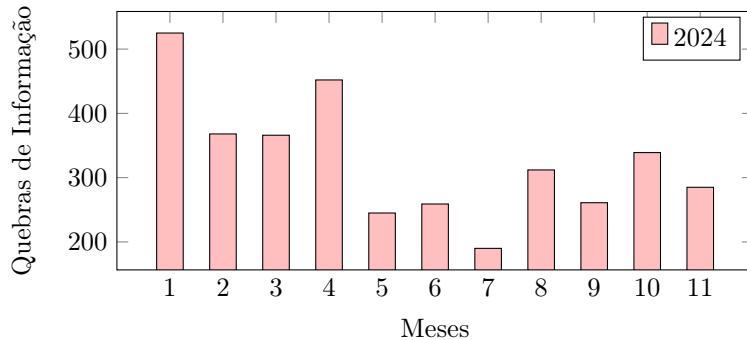


Figura 3.3: Quebras de informação em 2024, Fonte: Identity Theft [12]

Dentro destes ataques existem vários tipos, na Figura 3.4 é possível ver os mais utilizados em 2022:

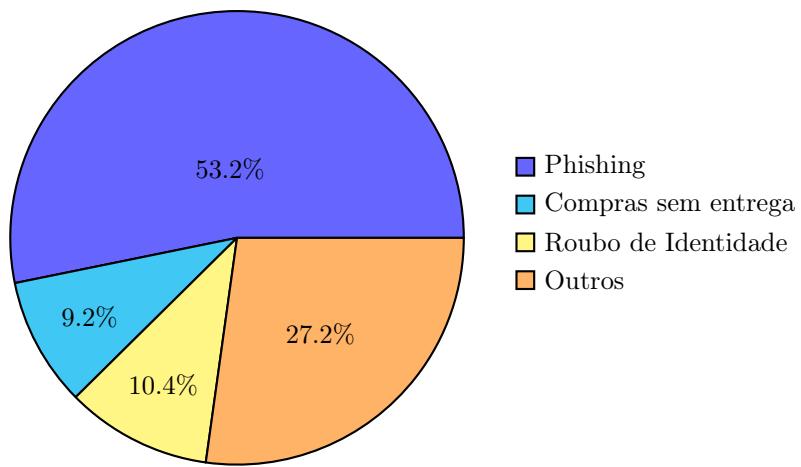


Figura 3.4: Tipos de ataques em 2022, Fonte: Crimes cibernéticos [13]

Como **ainda** não existe nenhum dado para este tema em 2024, só podemos deduzir que não tenha mudado muito. Porém, em 2017 houve também uma análise:

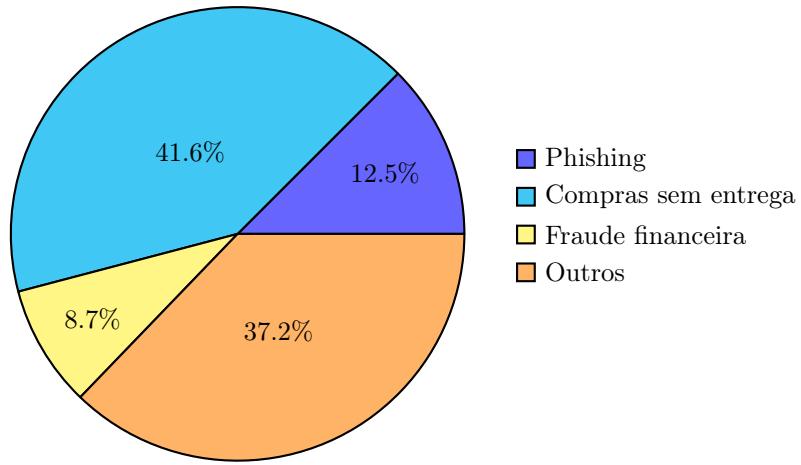


Figura 3.5: Tipos de ataques em 2017, Fonte: Crimes cibernéticos [13]

Comparando os dois, verifica-se um **grande aumento** no *phising*, um aumento em roubos de identidade e uma diminuição de compras sem entrega. Mas, para analisar melhor estes dados, é importante ter uma noção de quantos ataques houve em cada ano. Em 2022 houve um aumento de 51% em tentativas de ataque comparativamente ao ano de 2021. Esse aumento continua a ser revelado hoje em dia, havendo cada vez mais tentativas a cada ano que passa. E não só tentativas, de acordo com a Huawei, o número de ciberataques tem crescido 20% a cada ano, causando, de acordo com a Cybersecurity Ventures, uma perda de quase 1 500 triliões euros [14].

Com estes dados, conclui-se que a cibersegurança ainda tem muito espaço para evoluir e que se deve investir cada vez mais. Felizmente, com a Inteligência Artificial a crescer, a cibersegurança vai ganhar outros meios e pode vir a crescer exponencialmente. Até lá, simples conhecimentos sobre como navegar de forma segura na internet são fulcrais para os dias de hoje e podem salvar muita informação.

Capítulo 4

Conclusões

Como foi abordado, os ataques cibernéticos **não** vão parar de acontecer, pelo contrário, vão cada vez acontecer mais. As consequências destes ataques são grandes e, infelizmente, quando acontecem são difíceis de reverter. Por causa disso, é muito importante permanecer seguro na internet e caso possível, manter as outras pessoas seguras também.

Com este relatório ganha-se uma noção diferente do que de facto são **ciberrataques e a sua dimensão**. Fica-se a conhecer as inúmeras consequências que estes têm e o que conseguem causar. O Capítulo 2, os crimes, aborda este tema de uma forma interessante e cativante onde mostra várias situações, todas elas diferentes, mas com o **mesmo intuito**, isto é, remeter o leitor para a **importância da cibersegurança**. No Capítulo 3 aborda-se isso mesmo, agora de uma forma mais técnica e direta, porém visual, com a ajuda dos gráficos apresentados. Nestes gráficos estão dados importantes para perceber melhor como a cibersegurança e os ataques estão a evoluir.

Contribuições dos autores

Joana Gião (JG):

- Escolha do tema e capítulos abordados
- Introdução
- Capítulos 2.1, 2.4 e 2.6
- Capítulo 3.2
- Capítulo 4
- Acrónimos
- Bibliografia

Matilde Sanches (MS):

- Escolha do tema e capítulos abordados
- Introdução
- Resumo
- Capítulos 2.2, 2.3 e 2.5
- Capítulo 3.1

Percentagem de contribuição de cada autor: JG 65%, MS 35%

Repositório GitHub: infor2024-ap-52

Acrónimos

JG Joana Gião

MS Matilde Sanches

NASA The National Aeronautics and Space Administration

CIA Central Intelligence Agency

ACH Automated Clearing House

EUA Estados Unidos da América

NCA National Crime Agency

FBI Federal Bureau of Investigation

EEI Estação Espacial Internacional

OIM Olimpíadas Internacionais da Matemática

Bibliografia

- [1] P. Falardo, «Esquivos, dissimulados, cruéis: 7 dos criminosos mais procurados do mundo», *CNN*, 2021, [Online; acedido em outubro de 2024].
- [2] U. D. O. STATE, «Reward for Information: Maksim Viktorovich Yabubets», FBI, rel. téc., [Online; acedido em outubro de 2024].
- [3] O. Globo, «Adolescente de 16 anos é preso suspeito de hackear CIA, NSA e FBI», *O Globo*, 2016, [Online; acedido em outubro de 2024].
- [4] D. Redação, «Jovem britânico é preso suspeito de hackear chefe da CIA», *Exame*, 2016, [Online; acedido em outubro de 2024].
- [5] R. Richmond, «Web Gang Operating in the Open», *New York Times*, 2012, [Online; acedido em outubro de 2024].
- [6] FBI, «FBI TEN MOST WANTED FUGITIVE», FBI, rel. téc., [Online; acedido em outubro de 2024].
- [7] Desconhecido, «Os hackers norte-coreanos que tentam roubar segredos nucleares e militares», *BBC News*, 2024, [Online; acedido em outubro de 2024].
- [8] Desconhecido, «Jonathan James – The teenager who hacked NASA for fun», *Black Hat*, 2021, [Online; acedido em outubro de 2024].
- [9] Cybergirl, «The Boy Who Hacked NASA : The Tragic Life of Jonathan James», *Medium*, 2023, [Online; acedido em outubro de 2024].
- [10] K. LAB, «Top 10 Most Notorious Hackers of All Time», *Kaspersky*, 2024, [Online; acedido em outubro de 2024].
- [11] Microsoft, «Relatório de Defesa Digital da Microsoft: fraudes de suporte técnico dispararam 400% desde 2022», *Microsoft*, 2024, [Online; acedido em outubro de 2024].
- [12] P. Baldin, «Crimes cibernéticos, o que são, 3 exemplos e como se proteger», *itshow*, 2024, [Online; acedido em outubro de 2024].
- [13] I. Theft, «Breach Trends», Identity Theft, rel. téc., [Online; acedido em outubro de 2024].
- [14] Huawei, «“O número de ciberataques tem crescido 20% ao ano”, diz a Huawei», *Exame*, 2024, [Online; acedido em outubro de 2024].