

O Cibercrime em Angola: Uma Questão de Segurança Pública

Patrício Alexandre Gaspar Correia¹

¹ Assessor no Tribunal Constitucional. Licenciado em Ciências da Computação (Midrand Graduate Institute - South Africa); Pós graduando em Cibersegurança (Universidade Europeia - Portugal); Especialista em Gestão do Risco Cibernético (Harvard University - USA)

Nota Introdutória

Com o advento da internet o conceito de sociedade da informação vem ganhando, a passos galopantes, maior notoriedade pela forma como transformou, para o bem e para o mal, as sociedades. Em face desta realidade, novos conflitos e até desafios se vão conhecendo na relação entre o Direito, enquanto conjunto de regras disciplinadoras e dissuasoras do cometimento de crimes no ambiente virtual com a consequente imposição de condutas aos cidadãos e o facto de as TIC, nos dias que correm, constituírem uma necessidade essencial à vida colectiva. Ou seja, a conjugação dos vários factores que nos traz tal relação não deve possuir o condão de conflitar e/ou coartar os direitos fundamentais constitucionalmente consagrados destes, coexistência tal tanto mais difícil quanto o mundo se vai tornando cada vez mais globalizado e onde aspectos por vezes morais tendem a colidir com a lei. Portanto, urge a necessidade de se aperfeiçoarem as técnicas de manutenção da defesa do ciberespaço angolano ao mesmo tempo que se garante que as iniciativas do Estado angolano, neste domínio das TIC, não se evidenciem contraproducentes aos vários desideratos propostos.

O cibercrime representa uma realidade que inevitavelmente surge como um rosto incontornável na abordagem do fenómeno evolutivo que nos trazem as tecnologias de informação. Representam, por conseguinte, um problema que cresce cada vez mais e onde não se conhecem os limites geográficos, tampouco particularidades fáceis de se identificar. De tal modo que nos dias de hoje, através dos avanços tecnológicos que se conhecem, constitui uma obrigatoriedade percebermos, de antemão, que a rápida difusão da internet e a sua natureza anónima tornam, aparentemente, o ciberespaço numa fronteira sem lei e onde a anarquia prevalece.

¹ "Processo que dá forma ao saber graças à estruturação de fragmentos de saber". in MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, 2ª Edição Refundida e Actualizada, Almedina, Coimbra, 2006, p. 36.

Da variabilidade de ocorrências que têm lugar no ciberespaço, desde as maliciosas às criminosas, o cibercrime é uma acção que provoca danos/custos financeiros exorbitantes (na ordem dos vários milhares de kwanzas) cujo impacto pode potenciar consequências alarmantes, tais como: a interrupção no provimento de serviços críticos/essenciais, perdas abruptas de receitas, riscos sobre a manutenção da propriedade intelectual, interceptação indevida de comunicação electrónica, lavagem de dinheiro, burla, pirataria de software, calúnia, difamação, injúria, pedofilia, prostituição, incitação ao crime, falsa identidade, morte, entre outros fenómenos sociais indesejados — salienta-se que se reportou (pelas autoridades angolanas), no ano de 2021, um total de seiscentas (600) actividades criminosas com recurso às TIC.

Fonte: GSMA Intelligence e Statista

Período	Total populacional (Angola)	Total de ligações móveis (Angola)	Valor % de ligações móveis	Total de crescimento de usuários das redes sociais (população mundial)	Total global de usuários nas redes sociais (%)	Crescimento anual (%)	Usuários da internet em Angola	Rácio de penetração da internet em Angola (%)
Jan 2021 a Jan 2022	34.48 milhões	16.04 milhões	46.5 %	4.623 milhões	58.4 %	+10.1 %	12.41 milhões	36.0%

Figura 1: Tendência estatística na utilização das redes sociais no mundo inteiro e o número total de usuários da internet em Angola.

Em função do anteriormente abordado e com o objectivo de se estabelecer um paralelismo entre aquilo que constitui uma tendência global e os elementos concorrentes que trazem sustentação coerente com aquilo que nos apresenta o nosso contexto nacional, importa destacar que os números acima buscam evidenciar a exposição ao risco cibernético em função da maior disposição das pessoas de se ligarem às redes sociais, um fenómeno que ganhou maior incidência com os efeitos provocados pelo Covid-19 nos mais diversos quadrantes do nosso quotidiano.

Chama-se uma especial atenção ao facto de o crescimento exponencial na utilização das redes sociais, ou, se quisermos, da internet de modo individual e colectivo, alargar o escopo do panorama cibernético onde, inclusive, começa a evidenciar-se o surgimento de cibercriminosos dedicados ao “aluguer” de serviços específicos e moldados em função dos vários tipos² de ciberameaças que se conhecem (Crime-as-a-Service (CaaS)) — do impacto que cada incidente cibernético nos propõe, dever-se-á desenvolver, dentro de um conjunto de critérios de definição do ciber risco, um aturado plano de mitigação desse mesmo risco.

“PLUS ÇA CHANGE, PLUS C’EST LA MÊME CHOSE.” (KARR, Alphonse. Les Guêpes. Janeiro. 1849)³. Dentro de uma perspectiva da manutenção da segurança pública a ser levada a cabo pelos órgãos do Estado sobre os quais recai tal competência e porque tais iniciativas precisam encontrar uma normalização jurídico-legal que justifique as suas acções, é sobejamente sabido que na área da segurança da informação a tecnologia evolui com elevada rapidez. Adequando a citação acima à nossa discussão, podemos inferir então que a cada evolução tecnológica, novos meios e também métodos de comprometer os sistemas de informação surgirão. Tendo Angola ratificado em Junho de 2014 — numa clara e avisada iniciativa de reconhecimento que o cibercrime deve ser combatido dentro de uma narrativa geográfica internacional — a Convenção da União Africana Sobre Cibersegurança e a Protecção de Dados Pessoais (Convenção de Malabo), consolidou-se a ideia de que a estratégia a seguir no domínio da segurança do ciberespaço não podia estar dissociada daquilo que a União Africana estabelece como um dos seus marcos mais importantes, ou seja, a relação entre estados-membro.

² Distinguem-se por dois quadrantes gerais e dois subtipos específicos: Quadrante interno - Ameaças internas maliciosas e ameaças internas acidentais; Quadrante externo - Ameaças externas maliciosas e ameaças externas acidentais.

³ A citação em causa, numa tradução literal significa que “Quanto mais se alteram as coisas, mais elas permanecem na mesma «os problemas».” Numa ideia mais circunstancialmente ligada ao cibercrime, reflecte/traduz os problemas sistémicos causados pelo fenómeno da evolução das tecnologias associadas às más práticas delas decorrentes.

Sendo já um dado adquirido que a prevalência do uso da tecnologia no cometimento do cibercrime representa um problema crescente que requer dos órgãos do Estado que velam pela segurança do ciberespaço e da segurança pública angolana o reforço na implementação de medidas que tornem possível, célere e eficaz, a investigação e a condução de processos criminais com o sucesso que se deseja, sob que conjugação de noções poderemos então promover as acções de melhor gestão do *status quo* que nos impõe o impacto trazido pela inevitabilidade do convívio com as tecnologias de informação e as acções que se identificam com o cibercrime, sabendo de antemão que a) o nível de treinamento; b) a disponibilização de ferramentas adequadas; e, c) a alocação de recursos humanos nem sempre se prova suficiente em função do volume e da complexidade que casos do género acarretam?

Fundamentos do cibercrime

Segundo as deliberações trazidas do *X Congresso Sobre a Prevenção do Crime e Tratamento de Delitos* sob a égide das Nações Unidas, definiram-se duas categorias em torno do cibercrime com a seguinte estratificação:

- a) Sentido estrito: qualquer operação ilegal conduzida por meio de operações electrónicas que tem como alvo determinado sistema de informação e os dados nele processados.
- b) Sentido amplo: qualquer acto delituoso (incluindo a interrupção de serviços dependentes de serviços tecnológicos) levado a cabo por intermédio de, ou relacionado, a um sistema de informação ou rede de computadores.

O elevado índice de proliferação da tecnologia digital por associação a uma convergência entre dispositivos de computação e comunicação têm contribuído no processo de transformação de como hoje nos socializamos e conduzimos as nossas actividades comerciais e/ou organizacionais. Uma realidade que, aliás, permite-nos trazer desenvolvimento ao nosso quotidiano; porém, o crime quase que fareja as oportunidades e conforme anteriormente referenciado, a cada evolução, novas formas de se

explorar os benefícios decorrentes dessa tecnologia para fins criminosos surgem. Senão vejamos: a pornografia infantil ficou mais facilitada através da utilização dos telemóveis que hoje veem equipados com câmara fotográfica, a banca e o comércio electrónico providenciam um campo fértil para fraudes, enquanto as comunicações electrónicas tais como as SMS facilitam as burlas, etc., etc.

Ao passo que o uso dos computadores se tornou mais popular, mais se evidenciou a necessidade de se especializar o estudo no âmbito dos crimes com tais particularidades, surgindo assim a ciência do cibercrime. Em termos gerais, conhecem-se quatro papéis que se associam aos computadores no cometimento desses crimes (PARKER, D. *Fighting Computer Crime: For Protecting Information* (Wiley, New York, 1998)).

Computador enquanto:	Descrição:
Objecto	- Computador alvo de furto para extração de informação nele contido - Computador alvo de sabotagem/contaminação intencional
Sujeito	- Computador usado enquanto anfitrião (host) no cometimento de actividade criminosa
Ferramenta	- Computador usado enquanto ferramenta de criação e controlo de informação falsa (por ex.: phishing)
Símbolo	- Computador usado em esquemas ponzi

Figura 1: (*Ibid* (Adaptado))

Sendo o escopo de ocorrências no âmbito do cibercrime bastante vasto e dentro do enquadramento dos vários papéis que se podem associar nelas, toda a sua discussão deve suportar-se na base de um figurino jurídico-legal adaptado a cada contexto geográfico e que traga, em paralelo, uma definição devidamente estandardizada por entes colectivos orientados no estudo desse fenómeno. É inevitável que para se falar sobre o cibercrime seja necessário fazer-se um paralelismo com os crimes convencionais porquanto tal panorama diversificado refere-se,

conforme anteriormente assinalado, à perpetração de delitos qualitativamente novos habilitados pelas TIC ou por via da integração do ciberespaço em actividades mais tradicionais. Para uma classificação com maior precisão, necessita-se sempre de analisar três factores básicos:

- Examinação das características do crime;
- Que factores de vulnerabilidade que determinam a probabilidade de existir manipulação dos dados foram identificados;
- Quantificação sobre o grau de incidência e danos conexos coligidos (em forma de relatório preferencialmente).

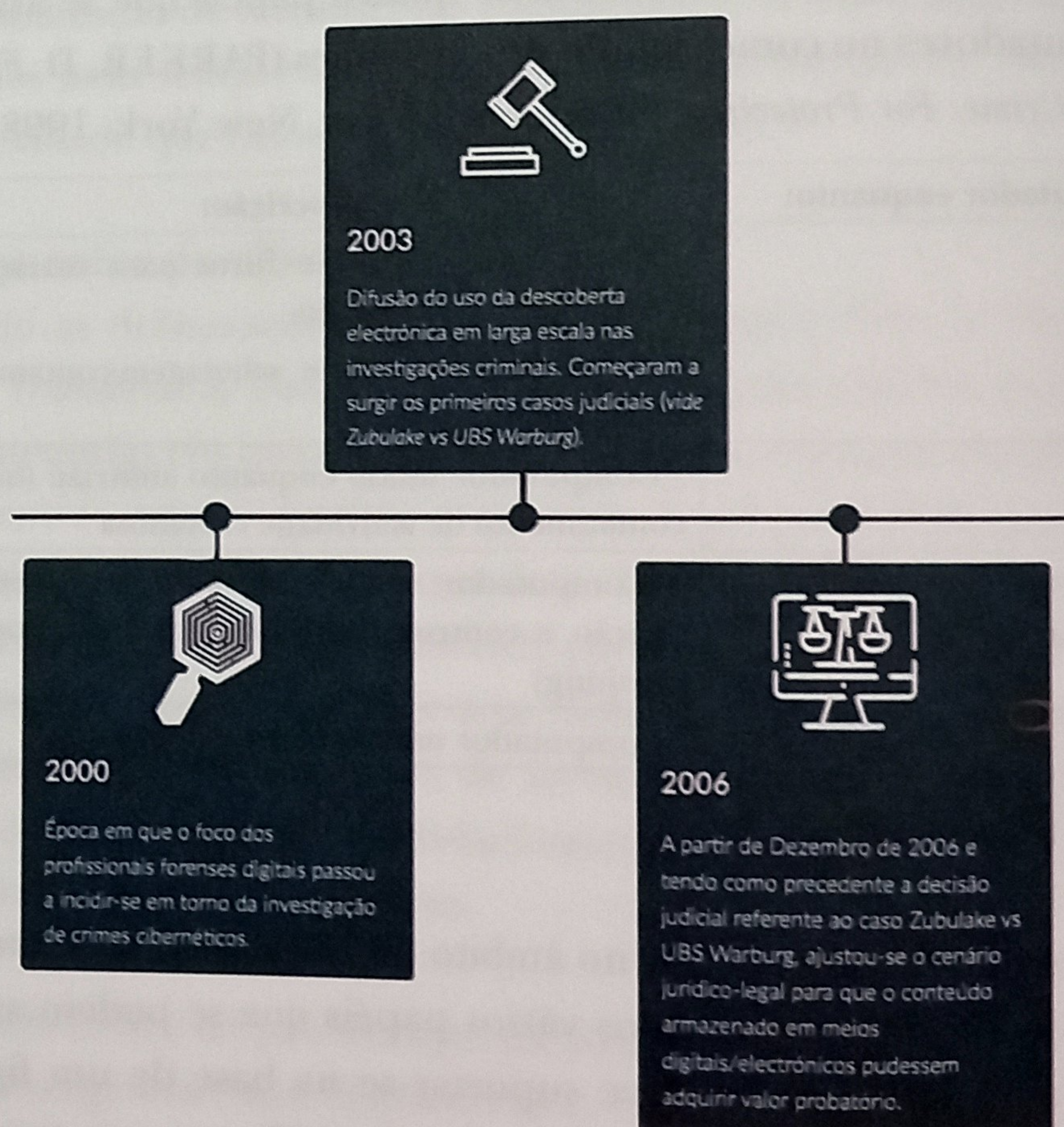


Figura 2: Informação difusa extraída de múltiplas edições da revista especializada em discussões científicas forenses Digital Forensics Magazine.

Com a ilustração (figura 2) acima pretendemos, contextualizando com o que já foi discutido, dar nota sobre o que consideramos ser a base da investigação forense que se conhece na actualidade e com um enquadramento evolutivo sobre aspectos que se definiram como sendo marcantes. Acessoriamente, importa destacar que as práticas de acção contra-forense, cada vez mais especializadas, constituem uma das principais vias por quais os ciber-criminosos procuram evadir-se das mãos da Justiça quando a acção forense se baseia tão somente na análise dos dados produzidos — desconsiderando toda a operacionalização “invisível” existente nos meios tecnológicos. Reflicta-se, por ex., sobre os efeitos básicos decorrentes da volatilidade da informação em trânsito dentro do processo de armazenamento de dados e o que acontece quando o equipamento que os armazena é desligado (pode-se, então, facilmente inferir que a análise forense digital deve cingir-se bem mais do que na análise daquilo que nos parece mais óbvio). Ou seja, para findar a nossa abordagem sobre este capítulo, independentemente da natureza do cibercrime, o investigador forense deve ter em consciência (*ab initio*) que poderá ter ocorrido algum tipo de manipulação das evidências digitais pelo que, em vez de se orientar pela busca técnica usual, deve começar por perceber que tipo de evidência digital poderá estar omissa — em nosso crer, este tipo de actividade precisa ser desenvolvida com base nalgum (muito) conhecimento em ciências da computação (principalmente no domínio dos sistemas operacionais).

O panorama dos cibercrimes

O acesso não-autorizado no domínio da cibersegurança caracteriza-se como uma acção normalmente punível por lei e, por definição, corresponde ao acesso inapropriado a um sistema de informação sem o consentimento do seu dono (BAINBRIDGE, D. *An Introduction to Computer Law* (Longman, New York, 2004)). Esse acesso não-autorizado não encerra, porém, o escopo de ciberameaças com que nos podemos deparar; pelo contrário, a maior parte de incidências associadas às

ciberameaças decorre sobre o aproveitamento do acesso legítimo dos utilizadores a determinado sistema de informação que, por sua vez, os torna vítimas de um ataque dirigido ou accidental. É elementar que a nossa discussão aborde o cibercrime enquanto uma acção que ocorre em função de uma ou mais variáveis de vulnerabilidade em que o computador pode servir de alvo para: a) o cometimento de uma actividade criminosa; b) como local de armazenamento de uma actividade criminosa; e/ou, c) enquanto ferramenta para uma acção de delito. Podemos considerar que a proporcionalidade existente entre a complexidade do cibercrime e a capacidade de se dar resposta aos ciberincidentes somente por se equipar um ambiente tecnológico com ferramentas de última geração, apesar de muito importante, é basicamente nula porquanto tal complexidade é melhor administrada num ambiente em que a ciber resiliência ocorre por intermédio de um conjunto de acções coerentes e que se baseiam na seguinte premissa, que o cibercrime NÃO é um problema informático; é sim, um problema das sociedades. Resumidamente e sem precisarmos nos desviar do nosso foco, importa salientar que os ambientes corporativos necessitam definir estratégias que prevejam a inevitabilidade da ocorrência de ciberataques; ou seja, devem estar estruturalmente organizados para reagir a estes definindo um aturado Plano de Mitigação do Risco que identifique adequadamente o conjunto de vectores de ataque que possam existir⁴.

De modo a melhor nos prepararmos para a inevitabilidade de um ataque cibernético, é importante perceber quais os tipos de ataques que poderão ser utilizados contra nós e o software malicioso – malware – apresenta-se como a forma mais comum dos ataques cibernéticos. Para

⁴ Prever a natureza exacta de ameaças futuras e como combatê-las é extremamente difícil – se não impossível, nalguns casos –, porém, quanto mais proactiva for a nossa estrutura de combate ao cibercrime, melhor.

⁵ “Malware é um termo que engloba vários tipos de software malicioso projectados especificamente para explorar vulnerabilidades e falhas no código do programa, permitindo que o hacker ataque outras formas de software e faça com que se comportem de maneira irregular. Após a instalação do malware, os hackers podem usar o software malicioso para roubar dados confidenciais, tornar o sistema inoperável ou até mesmo assumir o controlo do dispositivo visado.” (adaptado) in FALCO, Gregory J e ROSENBAUM, Eric, *Confronting Cyber Risk: An Embedded Endurance Strategy For Cybersecurity*, Oxford University Press, New York, 2022.

uma melhor compreensão sobre o que compõe o panorama cibernético global e qual o tipo de enquandramento/tipificação que se deve atribuir por especialidade de ocorrência, listamos de seguida os tipos de malware actualmente catalogados, os métodos mais comuns de difusão dos mesmos, bem como os tipos e subtipos de ataques igualmente mais comuns.

Tipos de malware:	Noções básicas:
Vírus	Um vírus é uma cadeia de código destrutiva anexada a outros programas. Depois que o programa infectado é executado, o vírus é instalado na máquina de destino. Os vírus se espalham quando o arquivo infectado é transferido de uma máquina para outra.
Vermes/ Worms	Um worm opera de maneira semelhante a um vírus, pois pode se espalhar para um computador por meio de um arquivo infectado. No entanto, o que diferencia os worms dos vírus é que eles podem se espalhar de forma independente, ou seja, sem a necessidade do arquivo infectado original. Em vez disso, os worms se espalham de forma autônoma, encontrando e explorando vulnerabilidades em redes informáticas.
Rootkits	Um rootkit é uma forma de malware projectada para conceder ao hacker direitos administrativos a um computador de destino. Como os rootkits são instalados manualmente nas subcamadas fundamentais da camada de aplicativos de um computador, eles não podem se replicar da mesma forma que os vírus, por meio de arquivos infectados que são compartilhados entre os computadores. No entanto, como são instalados fora da camada típica de aplicativos do usuário, são difíceis de detectar e remover.
Spyware	Spyware é um termo usado para se referir a software que rastreia a actividade de um usuário na Internet, reunindo dados armazenados no histórico do navegador tais como os hábitos de navegação na web e informações pessoais. Esses dados são então repassados a terceiros sem o consentimento do usuário. O spyware é frequentemente empregado por sites e aplicativos para exibir anúncios direccionados com base na actividade do usuário na web.

Tipos de malware:	Noções básicas:
Ransomware	Ransomware é um tipo de malware usado por cibercriminosos que bloqueia o acesso a um sistema ou ameaça divulgar informações confidenciais, a menos que uma quantia em dinheiro seja paga em forma de resgate. Ao contrário da maior parte dos outros tipos de cibercrimes, os hackers que usam ransomware notificam as vítimas sobre o ataque e fornecem instruções de pagamento, que geralmente é feito em moeda digital para proteger o anonimato do invasor. Existem dois tipos principais de ransomware, nomeadamente ransomware de criptografia, que serve para criptografar arquivos no computador da vítima, e ransomware de bloqueio, que não criptografa arquivos, mas bloqueia a vítima de aceder o computador.

Figura 3: Tipos de malware catalogados

Método	Noções básicas:
Download por drive-by	Um download por drive-by é um ataque que baixa software malicioso num computador sem o conhecimento da vítima e que pode ocorrer de duas maneiras. A primeira forma é quando a vítima do ataque visita uma página da Web que possui um código malicioso incorporado. Simplesmente acessar a página iniciaria uma investigação de rede no computador da vítima que encontraria uma vulnerabilidade oculta para baixar malware no computador da vítima sem o seu consentimento. A segunda forma é se a vítima fizer o download de software voluntariamente sem perceber que foi infectado por malware.
Trojan/ Cavalo de Tróia	Um Trojan é um código malicioso disfarçado como um aplicativo aparentemente inócuo. No entanto, depois que o aplicativo é baixado num computador e executado, o código de Trojan concede ao hacker acesso directo ao computador visado. O hacker tem a capacidade de monitorar todas as actividades no computador infectado, registando informações como actividades na Internet, pressionamentos de tecla e movimentos do mouse ou fazendo cópias do ecrã do computador de destino. Nalguns casos, os cavalos de Tróia permitem que o hacker assuma o controlo total da máquina infectada.

⁴ KASPERSKY, n.d. What are the different types of ransomware? Available: <https://usa.kaspersky.com/resource-center/threats/ransomware-examples> [2021, March, 28]

Engenharia social	A engenharia social é um método eficaz usado para implantar malware em um ou mais computadores e envolve a manipulação psicológica para induzir o alvo a realizar acções que levam à infecção de sistemas e redes com código malicioso. Dentro das técnicas de engenharia social, os ataques de phishing e spear phishing são considerados como sendo das técnicas mais bem-sucedidas usadas por hackers para infectar computadores direccionados ou coligir informações pessoais. Esse tipo de ataque disfarça o software malicioso como um anexo protegido ou um link confiável num e-mail. Abrir o e-mail instala automaticamente um software malicioso no computador de destino. Existem, também, os ataques de isca que são projectados para despertar a curiosidade humana. Um exemplo típico de um ataque de isca é quando os hackers deixam estrategicamente visíveis unidades flash/pendrives infectadas em locais onde os usuários-alvo provavelmente as encontrarão, na esperança de que os usuários as insiram em seus computadores corporativos, iniciando assim o download automático de software malicioso nas rede informática em causa.
-------------------	--

Figura 4: Métodos mais comuns de difusão

Tipos e subtipos de ataques

Conforme anteriormente referenciado, os métodos de ataques cibernéticos podem diferir com base nas motivações daqueles que os utilizam.

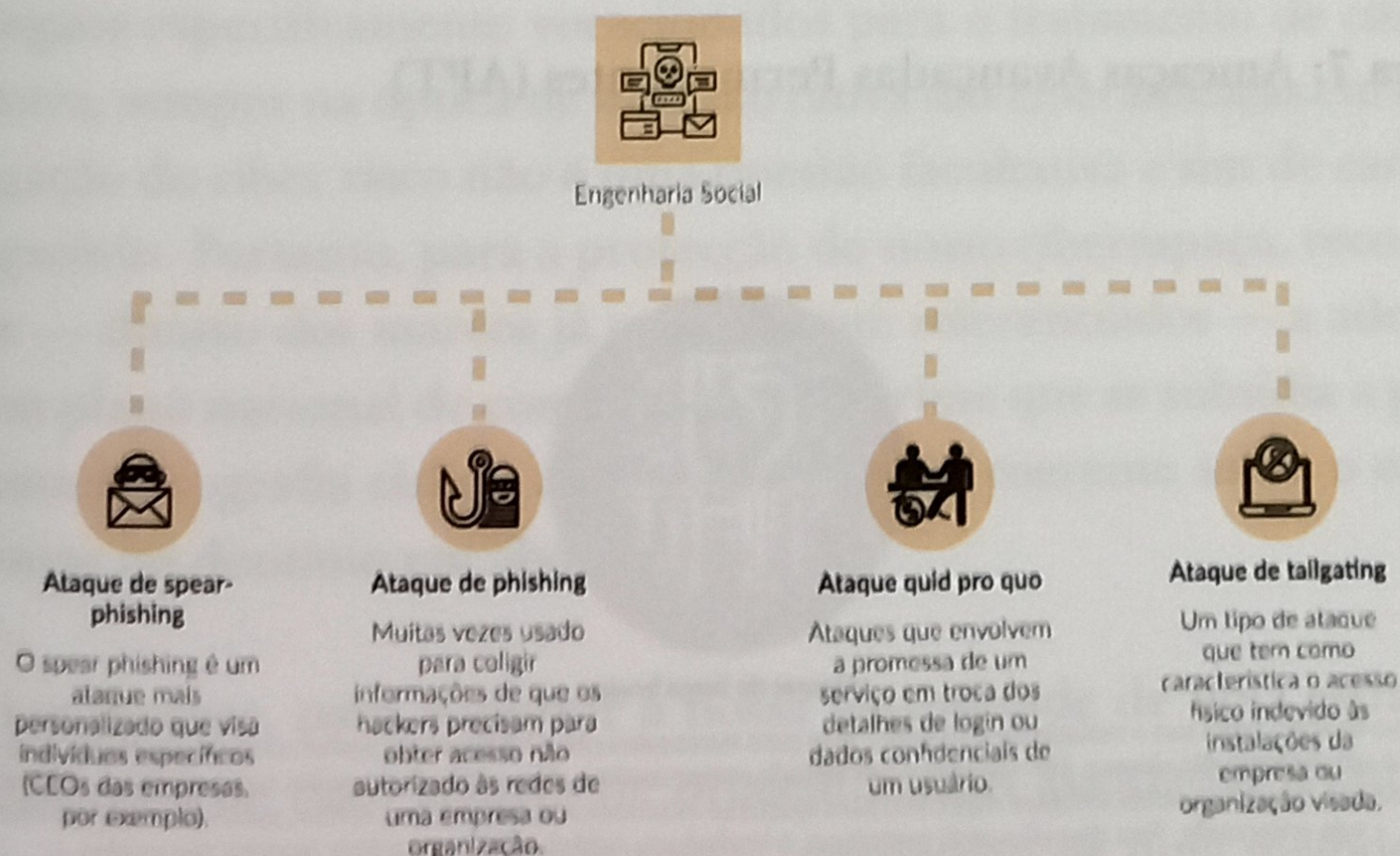
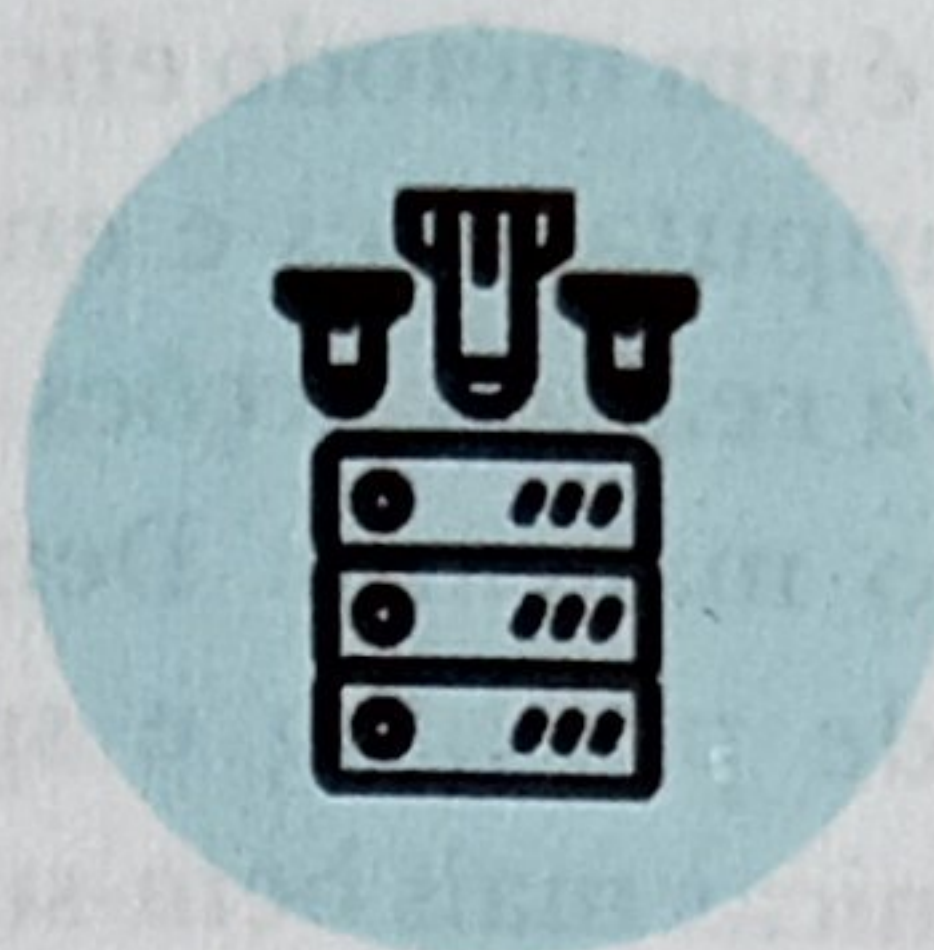


Figura 5: Subtipos de engenharia social⁷

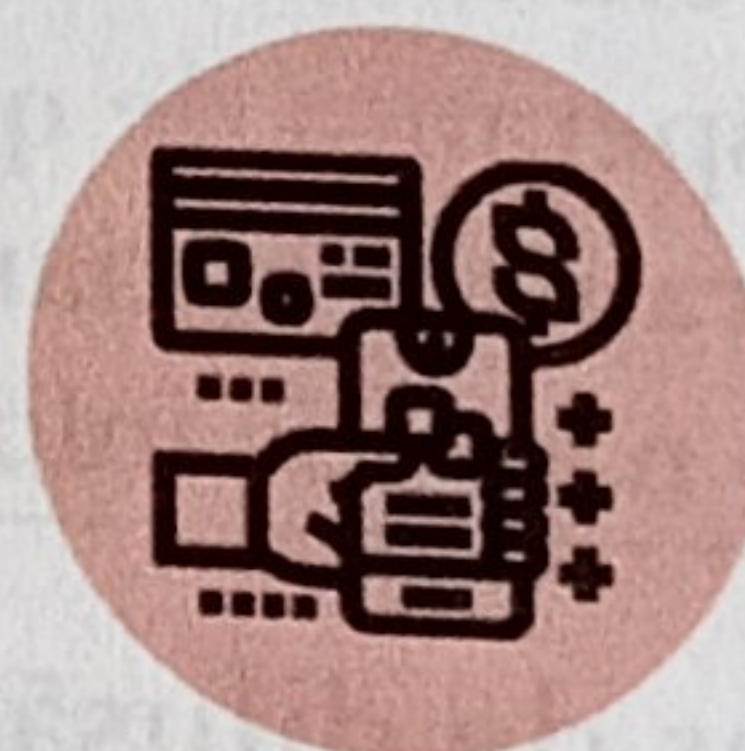
⁷ Propriedade intelectual do autor do texto



Ataque Distribuído de Negação de Serviços (DDoS)

Um tipo de ataque que causa interrupção/disrupção a websites, aplicativos serviços, redes de internet ou servidores através da inundação incessante de tráfego direccionado por intermédio de uma rede de computadores infectados com software malicioso.

Figura 6: Ataque Distribuído de Negação de Serviços

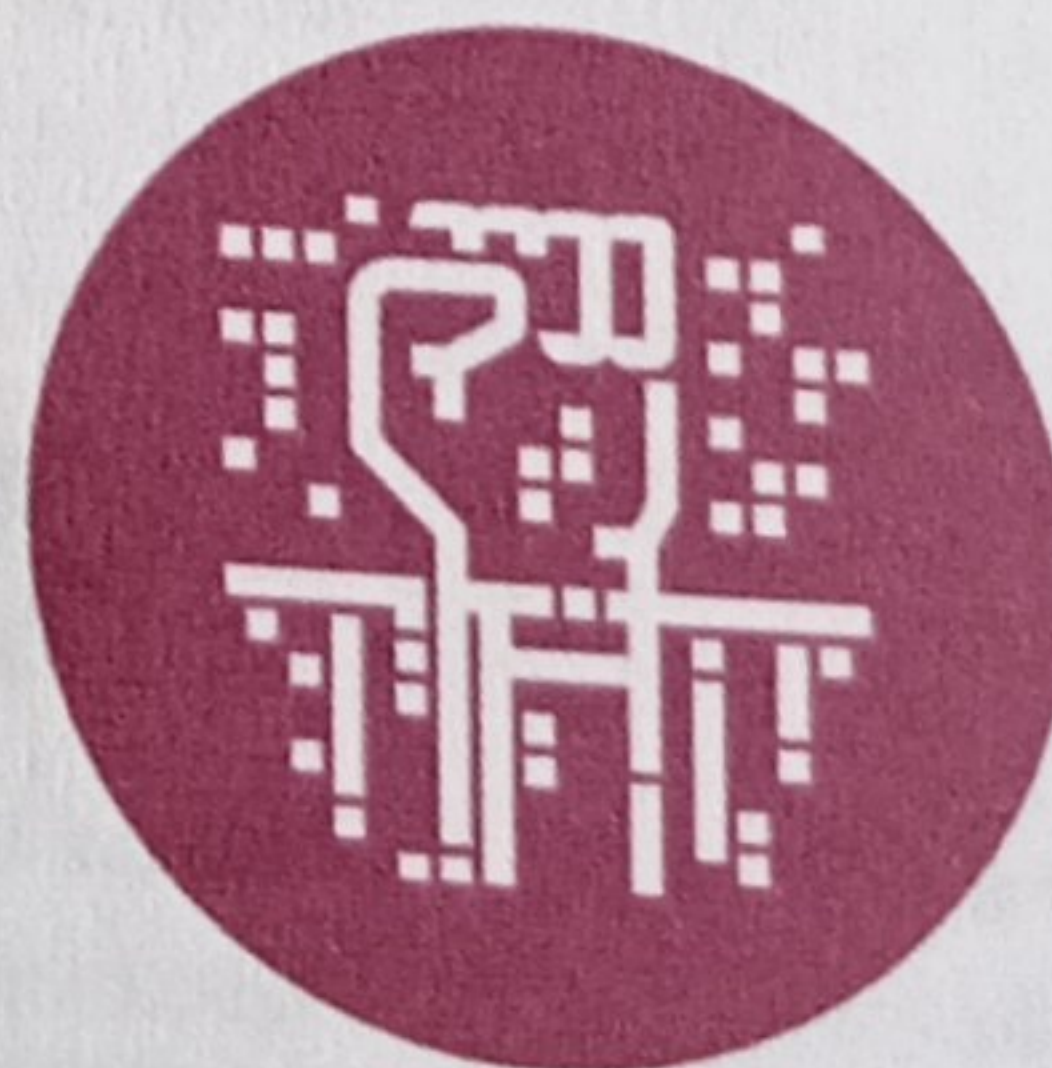


Ameaças Avançadas Permanentes (APT)

Uma ameaça persistente avançada é um ataque cibernético sofisticado que usa várias fases para obter furtivamente acesso não autorizado a uma rede para extrair o máximo de dados possível durante um período prolongado -- muitas vezes expandindo-se durante meses e até anos.

As APTs são consideravelmente mais complexas do que os ataques anteriormente mencionados por incorporarem, muitas vezes, vários tipos diferentes de ataques para garantir que os hackers possam se infiltrar num sistema sem serem detectados em todos os estágios do ataque -- por exigirem mais recursos do que o normal, são comumente levados a cabo/patrocinados por estados-nação.

Figura 7: Ameaças Avançadas Permanentes (APT)



Ataque de força bruta

Um ataque de força bruta usa o método de tentativa e erro para eventualmente desbloquear a senha correcta necessária para obter acesso a um determinado sistema. Por natureza é um método extremamente demorado, de tal modo que os hackers geralmente desencadeiam tal acção usando software específico para vasculhar sistematicamente todas as senhas possíveis até que a correcta seja encontrada. Para situações mais complexas, a Inteligência Artificial (IA) e o machine learning são usados.

Figura 8: Ataque de força bruta

Dentro do panorama dos cibercrimes e porque a segurança cibernética depende muito da capacidade de uma organização de impedir que softwares mal-intencionados atinjam os seus sistemas de informação críticos, importa reforçar que os malware assumem várias formas em que cada tipo possui particularidades muito próprias. No entanto, a tecnologia não é a única maneira de os hackers entrarem nos sistemas de destino. Eles frequentemente dependem de técnicas de engenharia social que tiram proveito da negligência e do erro humano. Portanto, proteger uma organização da engenharia social requer uma consciência astuta dos métodos que os cibercriminosos provavelmente empregarão.

Considerações finais

Sem o adequado patrocínio na forma de apoio político e o correspondente e necessário financiamento, pouco se conseguirá fazer no domínio da protecção do ciberespaço — alargando, assim, o apetite para que organizações cibercriminosas nos tenham como alvo preferencial. Por este motivo, pensamos que uma das formas mais eficazes de atingirmos, enquanto Nação, a resiliência digital que se requer, passará pela criação de órgãos especificamente vocacionados para o tratamento de ciberincidentes, sempre na óptica de uma narrativa das ciberameaças em que a mitigação do ciber risco não é uma questão facultativa e sim de carácter obrigatório. Portanto, para a protecção do nosso ciberespaço, recomenda-se — dentro dos marcos já previamente referenciados — a adopção de um plano nacional de combate ao cibercrime que se subsidia a partir de uma radiografia cíclica, ágil, colaborativa e coerente sobre o estado de coisas no domínio em abordagem.

Adicionalmente, para suportar a nossa necessidade de uma estratégia de mitigação de risco através de procedimentos associados a este conjunto de iniciativas que culminam na elaboração de uma metodologia organizacional, devemos fomentar a priorização dos riscos a que inevitavelmente estamos expostos. É com esta noção muito bem pensada que devemos, agravados pela nossa escassez de recursos, implementar

um plano que sirva de catalisador para a racionalização desses mesmos recursos, desenvolvendo uma estratégia objectivamente dedicada às prováveis ameaças e com base nessas constatações, um plano de ação deverá ser desenvolvido para auxiliar no processo de atribuição de responsabilidades para a implementação efectiva de tal plano.

Por fim, porque a estratégia corporativa/organizacional é o elemento que deverá conferir sustentabilidade à capacidade de gestão das incidências relacionadas com o cibercrime, a visão que se recomenda deve permitir que a segurança e resiliência digital no nosso cenário apresente práticas fortes de segurança cibernética que protejam o ciberespaço contra ameaças actuais e futuras, ou seja, devemos institucionalizar a cultura da proactividade, inclusive buscando parcerias com entes privados e até internacionais para que estejamos devidamente integrados na plataforma conceptual de partilha de informação que nos permita conhecer o cenário cibernético global de forma permanente e actuante.