Compugraf

# A ANATOMIA DAS AMEAÇAS CIBERNÉTICAS

## O CIBERCRIME EM EXPANSÃO

# ÍNDICE

# INTRODUÇÃO

Além de todas as dificuldades que estamos enfrentando fora do ambiente digital, os crimes cibernéticos evoluem diariamente e, em 2021, esse crescimento deve se tornar ainda mais acelerado, com as transformações nos modelos de trabalho tradicionais.

A opinião de que o mundo continuará batalhando ao longo deste ano é amplamente aceita pelos especialistas do setor, visto que estamos em meio a uma crise sem precedentes.

Por outro lado, o universo da cibersegurança nunca esteve mais preparado para proteger os usuários domésticos e corporativos, e as movimentações para prevenir de ameaças estão, aos poucos, sendo adotadas pela grande maioria das empresas.

Pensando nisso, decidimos desenvolver um material para explicar a anatomia das ameaças cibernéticas, permitindo que as organizações obtenham uma melhor visualização desses perigos e definam estratégias de prevenção mais eficazes.

O material foi dividido em duas partes. Esta, a primeira, tratando das ameaças de uma forma mais ampla, explicando os diversos tipos de ataque e a segunda, focada em um tipo específico de violação: os *malwares*.

Acesse a segunda parte do material através deste link.

Um dado interessante mostra que, em 2019, a segurança da informação no Brasil já representava um dos 10 maiores investimentos no mundo, com projeção de US$1,6 bilhão.

A necessidade de uma rápida transformação digital e a transição para o trabalho remoto, fizeram com que diversos setores recorressem a uma série de novas tecnologias, incluindo soluções de segurança, fortalecendo o mercado de SI em meio às mudanças no cotidiano.

# Mas qual é o prejuízo de um crime cibernético?

O mercado de Segurança da Informação não cresce anualmente à toa.

Na realidade, lidar com o cibercrime pode acabar custando caro, na medida em que as ameaças tornam-se cada vez mais sofisticadas.

Em uma pesquisa realizada pelo ***Center for Strategic and International Studies (CSIS),*** foi constatado que os crimes cibernéticos causaram prejuízo médio de US$ 445 bilhões em 2014, número que, hoje, já ultrapassa a faixa dos US$ 600 bilhões para as empresas (cerca de 0,8% do PIB mundial).

# O que podemos aprender com isso?

Existe um conflito sem fim entre o combate e a criação de novas vulnerabilidades e, como já falamos em um de nossos materiais anteriores, onde explicamos o conceito de guerra cibernética, todas as nações estão envolvidas nessa relação de alguma maneira.

Afinal, uma vulnerabilidade não parte necessariamente de uma tecnologia específica, ela pode surgir através de fake news, ou simplesmente de assuntos que estão em alta no momento, aproveitando-se do fator humano para atrair um alvo.

Isso faz parte de um conjunto de técnicas chamado de Engenharia Social, a qual já abordamos em um de nossos materiais anteriores, que você pode acessar clicando aqui.

Tendo isso em mente, quando criminosos cibernéticos passam a utilizar tecnologia de ponta, os defensores precisam investir em sua estrutura e deixá-la mais resistente a ataques.

# Quais são os países mais afetados?

Não é de hoje que os crimes cibernéticos se tornaram uma grande ameaça às pessoas, empresas e até mesmo governos.

Durante o processo de apuração dos dados para este material, nos deparamos com informações muito interessantes:

Dentre os prejuízos com crimes cibernéticos, estão inclusos os custos para o combate a invasões e, para citar esse complexo sistema, escolhemos abordar um tipo de ameaça que vem ganhando espaço no mercado: o *ransomware.*

## Ataques envolvendo *ransomwares* podem ser terceirizados.

Isso mesmo.

Foi constatada a existência de grupos especialistas na prática de sequestro virtual sob demanda, algo que nos leva ao conceito de "ransomware-como-serviço" (do inglês "*ransomware-as-a-service*") e, com o uso de criptomoedas como pagamento, fica cada vez mais difícil rastrear os prestadores do serviço e os contratantes do crime.

Enquanto bancos ainda são um dos principais alvos de crimes cibernéticos no mundo todo, tempos como a pandemia atual trouxeram novos grandes alvos, como a área de saúde.

Além disso, essas ameaças já foram utilizadas até mesmo entre países em conflito.

Nações como a Rússia (considerada a líder na execução de ataques), Coreia do Norte e Irã, que estão constantemente envolvidas em conflitos políticos, podem ser vistas como centros de operações voltadas para os crimes virtuais, sendo responsáveis pela grande maioria dos ataques envolvendo instituições financeiras.

Por outro lado, a China é um país conhecido no mundo cibernético como um dos maiorais quando o assunto é espionagem.

## Viu como não dá para duvidar da organização desse universo?

A Rússia é considerada a líder de crimes cibernéticos no mundo todo por uma série de razões que fazem com que seus cibercriminosos tenham menos escrúpulos com as possíveis consequências dos ataques, além do ostensivo desrespeito pelas leis ocidentais.

Quando todos os continentes foram avaliados, ficou visível que, embora todos os países sofram com crimes cibernéticos, nações com maior poder aquisitivo investem em ferramentas para o combate, diferentemente de países mais pobres, onde o dinheiro é direcionado para cobrir os danos causados.

# Os principais vetores de ataque

Na segurança cibernética, um vetor de ataque é o caminho pelo qual um invasor pode obter acesso não-autorizado a um computador ou rede para chegar ao seu objetivo final, que pode variar de acordo com o tipo de ataque.

Em suma, os vetores de ataque permitem que os invasores explorem as vulnerabilidades de um sistema, instalem diferentes tipos de *malware* e iniciem ciberataques.

Além disso, eles também podem ser utilizados para a obtenção de informações confidenciais ou dados sensíveis, que resultam em uma violação de privacidade.

Alguns vetores de ataque comuns incluem malwares, vírus anexos de e-mail, páginas, pop-ups, mensagens instantâneas, mensagens de texto e armadilhas de engenharia social.

Os vetores de ataque podem ser divididos em dois grupos, passivo e ativo, cada um com características específicas:

**Passivo**
É quando o ataque tenta obter acesso ou utilizar as informações do sistema, mas não afeta os seus recursos do sistema. Por exemplo: *typosquatting, phishing* e outros ataques baseados em engenharia social.

**Ativo**
É quando o cibercriminoso tenta alterar um sistema ou afetar seu funcionamento, explorando vulnerabilidades não corrigidas, falsificando e-mails ou recorrendo a *MitM*, sequestro de domínio e *ransomware*.

Isso posto, a maioria dos vetores de ataque compartilha algumas semelhanças, seguindo um caminho lógico comum:

1. **O hacker identifica um alvo em potencial;**

2. **São reunidas informações sobre a vítima usando engenharia social, *malware, phishing*, OPSEC (operações de segurança) e verificação automatizada de vulnerabilidades;**

3. Essas informações são utilizadas  para identificar possíveis vetores de ataque e criar ou se equipar de ferramentas para explorá-los;

4. O invasor obtém acesso não-autorizado ao sistema para roubar dados confidenciais ou instalar códigos maliciosos;

5. Começa o monitoramento do computador ou da rede, o roubo de informações e uso dos recursos disponíveis para extrair dados relevantes.

# A ANATOMIA DAS AMEAÇAS CIBERNÉTICAS

## O *Phishing* e as técnicas de persuasão do usuário

2020 mostrou um grande crescimento nos incidentes envolvendo o *phishing*, afinal, com tantos conflitos ao redor do mundo, o método ganhou o palco perfeito para se infiltrar nos sistemas das vítimas e se aproveitar da vulnerabilidade humana.

De acordo com uma pesquisa realizada por uma parceira da Compugraf, a Check Point, algumas empresas sofreram muito mais com tentativas de phishing do que outras.

Para começar, a DHL, empresa de entregas conhecida mundialmente, teve uma grande parcela de tentativas de ataque realizadas em seu nome, com mais de 57% de e-mails falsos envolvendo o nome da empresa.

Mas os números não param por aí.

A Amazon, empresa de tecnologia, também mundialmente conhecida, teve uma porcentagem de 37% na apuração, ou seja, uma grande recorrência de tentativas de golpe com o nome da empresa.

Outro sistema de entrega atingido foi a FedEx, que teve cerca de 7% dessa fatia, colocando os Estados Unidos como grande alvo desse tipo de ataque e definindo as empresas de maior popularidade como as principais vítimas do uso não autorizado de marca, o que acarretou em danos à reputação e aumento de reclamações via SAC.

## O *e-mail* é uma das ferramentas mais utilizadas no *phishing*, mas não é esse o seu único vetor

Segundo os dados da *Check Point*, é possível visualizar diversas formas de ataque, como o envio de mensagens com "ofertas imperdíveis" ou até mesmo supostas falhas em processos de entrega.

Para esses casos, constatou-se um aumento generalizado de 80% dos incidentes.

Em outras palavras, a cada 826 *e-mails* disparados em novembro de 2020, pelo menos 1 deles tratava-se de um ataque por *phishing*, sendo a média de crescimento global 13% maior em relação ao mês anterior, crescimento que provavelmente está relacionado à *Black Friday*.

Ao que parece, no entanto, os cibercriminosos brasileiros ainda não possuem o hábito de aplicar golpes utilizando nomes de empresas de frete como os Correios, assim como acontece em países vizinhos e também no continente africano, o que pode significar que o foco no Brasil pode ser um pouco diferente.

Afinal, as fraudes mais comuns em toda a América do Sul são voltadas ao setor bancário, o que já torna o cenário completamente divergente.

A alta nos ataques de phishing em 2020 ocorreu no final do ano, aproveitando-se de datas importantes para o comércio como a *Black Friday* e a *Cyber Monday*, facilitando o disfarce entre as "ofertas inacreditáveis", que são as grandes promessas dessas ocasiões.

**// Conclusão? Fraudes e mais fraudes.**

Vale lembrar que o *phishing* se enquadra na engenharia social e, dentro dela, é o método mais utilizado.

O crime consiste na obtenção de dados de uma pessoa ou organização através de técnicas de comunicação e persuasão.

E, quando falamos em comunicação corporativa ou serviços gerenciados e utilizados por muitas pessoas, qualquer usuário pode ser uma porta de entrada para uma brecha de segurança.

Ainda em 2013, por exemplo, mais de 110 milhões de informações e números de cartões de crédito dos clientes da *Target* acabaram sendo expostos e, após a perícia, foi concluído que tudo começou quando um subcontratado da empresa foi vítima de *phishing*.

O contato do criminoso pode ocorrer a partir de qualquer meio de comunicação na tentativa de fazer com que pessoas caiam em um golpe (também conhecido como *scam*).

# De simples execução, o phishing também é facilmente reconhecível quando o usuário está ciente de suas características.

São *e-mails* chegando de remetentes duvidosos, ligações telefônicas suspeitas ou qualquer outra forma de comunicação que seja, no mínimo, questionável para o alvo, já que é direcionado a um grande público e, na maioria das vezes, não possui qualquer seleção.

Por isso, a chance de sucesso da prática depende de dois fatores: o momento certo e a desatenção do usuário.

Sendo assim, o *phishing* depende mais da atenção e da calma para verificar as informações antes de qualquer ação, embora possa causar desespero e impulsividade em um momento importuno.

# Ataques DoS, DDoS e os limites de um servidor corporativo

O DoS (*Denial Of Service* ou Negação de Serviço) é um ataque que inunda o sistema, servidor ou rede com tráfego, visando esgotar os recursos e a largura de banda.

Trata-se, basicamente, de uma invalidação por sobrecarga, em que um sistema não consegue responder às solicitações legítimas.

Dentro dessa vertente, os invasores também podem usar vários dispositivos invadidos para iniciar a operação. Isso é conhecido como ataque DDoS (*Distributed Denial of Service).*

O tema é tão importante no Brasil, que o país já é um dos que mais sofrem com esse tipo de ameaça, com o setor bancário como principal alvo, mesmo com o crescente investimento em segurança que temos observado no mercado.

Um estudo realizado por uma das parceiras da Compugraf, a *Fortinet*, nos trouxe um ponto de vista interessante: o objetivo dos ataques não é apenas causar desconforto às instituições, mas sim, efetivamente roubar dinheiro dos clientes.

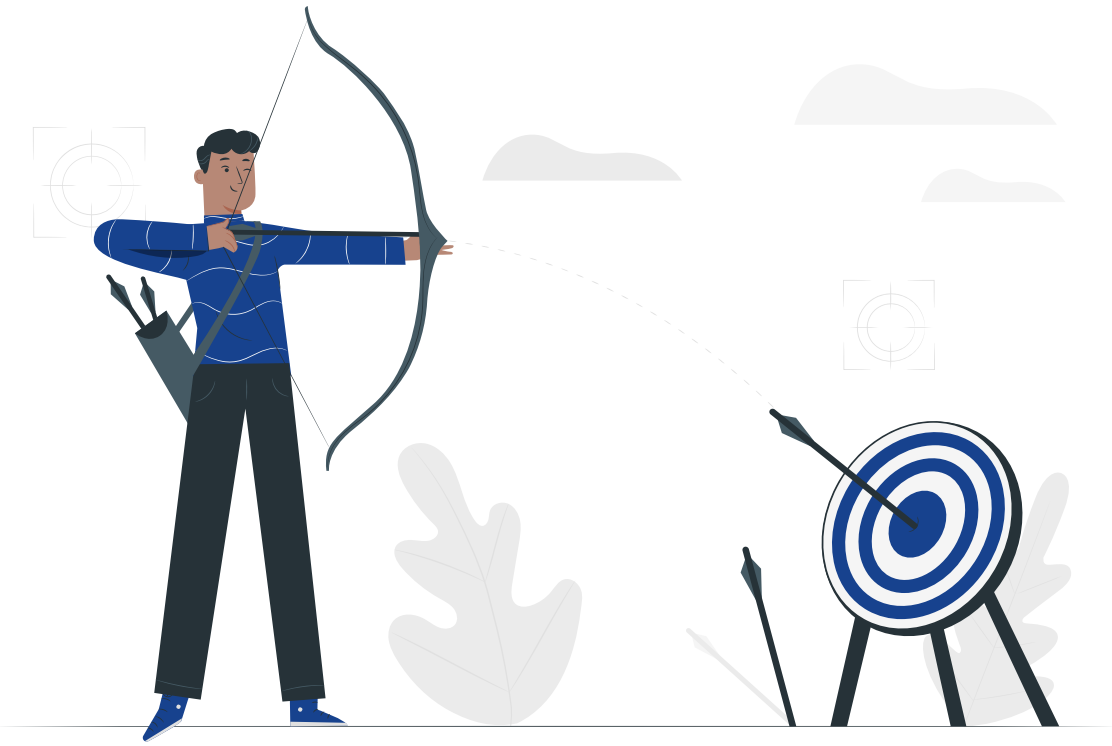
**Pensando nisso, podemos dizer que esse tipo de ameaça está caminhando para ser um dos possíveis protagonistas de 2021.**

O ataque de DDoS mostra que nenhum servidor é à prova de sobrecarga, ou seja, todo ambiente possui limites e, por esse motivo, o custo dos ataques é alto até mesmo para os criminosos, já que, quanto maior o alvo, maior será a estrutura para a realização do ataque.

Vale ressaltar que a maioria dos ataques de grande escala envolvendo DDoS, utilizam-se não apenas da estrutura local dos criminosos, mas de todos os dispositivos sobre os quais os atacantes exercem controle, inclusive máquinas infectadas anteriormente.

Em outras palavras, o seu dispositivo pode estar sendo usado como um dos soldados dessa prática sem que você saiba, caso esteja infectado.

Os sistemas operacionais, quando invadidos, possibilitam uma série de ações através de linhas de comando, executando as mais diversas tarefas. Nessa etapa, a maioria das vítimas não é o alvo final.



# Para entender melhor, imagine o seguinte:

Um site que você está acessando está muito lento devido ao número de acessos simultâneos (neste caso, sem motivações criminosas), que podem estar sobrecarregando o servidor e causando o atraso na resposta.

O administrador dessa página dispõe de manobras para contornar a situação, como aumentar o limite de tráfego (de acordo com sua estrutura), mas, caso ele não consiga fazer isso a tempo, provavelmente o site sairá do ar.

Se o servidor se mantiver funcionando (mesmo com lentidão) e o número de usuários aumentar, é bem provável que muitos desses usuários não consigam acessar a página, já que isso é uma resposta do sistema para instabilidades.

E é nisso que se baseia o DDoS: lentidão, instabilidade temporária e até mesmo a queda do servidor.

Quando um sistema apresenta instabilidades ou deixa de funcionar, os riscos vão desde o comprometimento da experiência de navegação do usuário até o corrompimento de dados, que é uma das hipóteses mais perigosas.

# Como podem ocorrer os ataques de DDoS

As formas são inúmeras, mas citaremos as mais comuns ao redor do mundo:

## Ataques Volumétricos

O mais comum, tratando-se justamente da agressiva quantidade de conexões simultâneas, maior do que o servidor está acostumado ou, ainda pior, do que o mesmo suporta;

## Ataques de Protocolo

Os ataques de protocolo funcionam de maneira um pouco diferente, eles exploram brechas nas camadas de rede e impedem o acesso a determinados recursos do servidor, causando instabilidades;

## Ataques aos Aplicativos de Destino

Uma versão mais robusta do DDoS envolve as solicitações que aparentemente ocorrem a partir de usuários legítimos, podendo envolver sistemas previamente corrompidos, sendo os mais difíceis de descobrir e rastrear.

# A importância de um *Firewall*

Para evitar ataques de DDoS, o processo é um pouco mais complexo do que se proteger de outras ameaças, já que o mesmo possui particularidades avançadas.

Um dos grandes desafios em deter esse tipo de ameaça, que também define o sucesso do ataque, é o tempo de identificação.

Em outras palavras, o intervalo entre o início do ataque e a percepção da equipe de segurança de que há algo errado faz toda a diferença na redução de danos ou encerramento da ação.

As soluções mais indicadas nesses casos devem envolver a defesa contra ataques de grande volume, até mesmo em conexões seguras (SSL), além da análise do sistema de domínios (DNS) e vetores IoT (*Gadgets* conectados a uma rede) e sua variedade de dispositivos, que devem possuir um mapa de comportamento dos acessos.

Uma outra forma de barrar um DDoS é o *Firewall*, que bloqueia os endereços IP mais atacados e permite o estabelecimento de regras para evitar os ataques.

O *Firewall* pode ser um dispositivo físico ou um *software* monitorado remotamente, sendo uma poderosa ferramenta capaz de reduzir custos e aumentar a eficiência das operações de segurança envolvendo principalmente o acesso entre servidores, sejam eles externos ou internos.

O sistema é capaz de analisar todo o tráfego em tempo real dos dispositivos conectados a uma rede, possibilitando a suspensão de qualquer atividade antes que algum dano seja causado.

E isso vale tanto de dentro para fora, como de fora para dentro.

O administrador do *Firewall* pode, por exemplo, bloquear o acesso de funcionários a sites específicos, como no caso da concorrência e redes sociais.

Uma das grandes vantagens do método é o seu preço. Por sua capacidade de facilitar o monitoramento de tantas camadas de proteção, o sistema é relativamente barato comparado a outras ferramentas do mercado, mas isso não significa que o *Firewall* deve ser a única linha de defesa de uma empresa.

Se o seu *Firewall* está desativado, considere ativá-lo imediatamente, pois a mecânica do DDoS, embora possa causar danos devastadores, é facilmente aprendida por *hackers* iniciantes, já que existem diversos tutoriais simples para a sua execução.

**// E você não quer que sua empresa seja o campo de treino de um deles, não é mesmo?**

# Cavalos de Tróia e o plano histórico para assumir o controle

Assim como nos épicos gregos, um cavalo de troia é um mal maquiado para parecer algo bom.

Sua ação ocorre quando o usuário executa um *software* aparentemente legítimo que, em algum momento, foi corrompido.

A ameaça age de maneira silenciosa e, quando a infiltração é bem-sucedida, abre diversos pontos de entrada para novas ameaças.

Justamente pelas comparações com os poemas da Grécia Antiga, os cavalos de troia são os tipos de *malware* mais antigos e conhecidos, recebendo sua alcunha em 1974 pelas forças aéreas americanas, que a escolheu ao traçar seu *modus operandi.*

Apesar de já possuir um nome, o primeiro ataque com um cavalo de troia só veio a acontecer um ano depois, a partir de um programa conhecido como *ANIMAL-PERVADE*, que nada mais era do que um bloco de códigos disfarçado de jogo para que os usuários que executassem o arquivo liberassem um *malware* em seus dispositivos.

Na época, a ameaça não causou grandes danos e foi rapidamente combatida, mas surpreendeu por sua velocidade de multiplicação.

# Os trojans de acesso remoto

Nos últimos meses, uma variação do *malware* conhecida como RAT (*Remote Access Trojans*), uma evolução dos backdoors, tem ganhado espaço no cenário digital, fornecendo uma interface gráfica ao invasor e diversas maneiras de comprometer os sistemas.

A maioria dos dispositivos infectados não sentem impactos imediatos, já que estes são apenas ferramentas para objetivos ainda maiores (como um *DDoS*) e, portanto, não são alvos diretos dos criminosos.

Ainda assim, em alguns casos, durante a exploração, os cibercriminosos encontram algo de seu interesse, como acesso privilegiado à rede de uma empresa, páginas de banco ou dados específicos, que podem levar a crimes de estelionato.

Em outras situações, o dispositivo da vítima pode acabar inutilizado.

Lembramos que os cavalos de troia, citados acima, se encaixam na categoria de *malwares*. **Se você quiser saber mais a respeito desse tipo de ameaça, confira a segunda parte desse material, totalmente dedicado aos *malwares*, através deste link.**

# Quanto custa uma campanha de conscientização?

O fator humano é a maior vulnerabilidade das estratégias contra ciberataques, então falaremos aqui como aplicar um plano consistente e sustentável para a sua organização.

Campanhas de conscientização sobre segurança da informação são essenciais para instruir uma equipe sobre o que fazer para evitar ameaças.

Confira 12 etapas para criar uma campanha forte e memorável:

## 1. Foco em problemas reais

Foque no que é realmente um problema para sua organização.

Embora a ideia de resolver todos os problemas de uma vez seja algo interessante, nenhuma campanha que tenta cobrir todas as possibilidades de uma só vez funcionará da maneira esperada. O melhor é focar nos principais conceitos e, somente quando os funcionários sentirem-se confortáveis com aquilo, partir para outras medidas.

## 2. Reforço das principais medidas

Verifique cada setor para tentar compreender as necessidades de segurança de cada um.

## 3. Segmentação para os diferentes grupos de trabalho

Reconhecendo as necessidades de cada setor, chegou a hora de definir qual mensagem será passada para cada um, pensando no que seria mais efetivo para determinado público e também em suas aplicações diárias.

## 4. Repetição das mensagens em diferentes canais

A repetição de canais é um recurso que funciona no *marketing* digital e, com toda certeza, deve auxiliar no *marketing* de conteúdo e *offline*, também. Repita as mensagens da campanha em diferentes canais para facilitar a memorização das boas práticas.

## 5. Utilização de influenciadores para transmissão de mensagens

Para uma organização, um influenciador não precisa necessariamente ser alguém famoso, pode ser um líder de equipe, por exemplo, um formador de opinião. Compartilhar histórias de gestores ou até mesmo do dono da empresa pode ser inspirador para muita gente.

## 6. Desafio de crenças em cibersegurança

É muito importante que alguns profissionais sejam desafiados para que a campanha seja vista com bons olhos. Selecione, junto à equipe de TI, convidados e profissionais mais experientes para receber desafios específicos que os aproximem dos outros colaboradores.

## 7. Ilustração de situações

Durante a campanha, utilize formas e cores distintas, busque trazer o máximo de atenção para as peças da campanha, além de verificar boas referências para tornar a campanha única.

## 8. Exemplos de ocorrências anteriores

A empresa em questão já sofreu algum tipo de ataque no passado? Trazer ocorrências passadas é uma ótima maneira de criar consciência sobre como certos ataques são possíveis e quais podem ser os danos em caso de reincidência.

## 9. Inclusão de informações relevantes para além do trabalho

Ninguém deve questionar um bom plano de conscientização, mas considerando que muitos funcionários podem trabalhar utilizando celulares ou outros dispositivos remotos, por que não pensar em soluções que possam ser aplicadas em casa também?

## 10. Contar histórias

Além de um visual atrativo, a melhor maneira de captar a atenção dos funcionários é com textos persuasivos. Uma das maneiras de se obter esse resultado é através de um bom storytelling.

## 11. Justificar os motivos

É sempre bom lembrar, as pessoas gostam de saber o porquê de estarem fazendo algo. Seja transparente sobre as razões por trás de certas medidas para que o processo de transição faça sentido para todas as partes envolvidas.

## 12. Compartilhar resultados

Compartilhe os resultados de todas as campanhas com as pessoas envolvidas, colete feedbacks, sugestões e o mais importante: não pare de realizá-las.

# Conclusão

Entender o que são e como funcionam as ameaças cibernéticas é fundamental para visualizar a maneira como elas afetam uma organização, assim como traçar os melhores planos para combatê-las.

Existem diversas ameaças não mencionadas aqui e muitas ainda desconhecidas por uma grande parcela da população, mas acreditamos que com este guia você poderá se atualizar sobre alguns dos ataques mais recorrentes e esperados para 2021.

Para que essa não seja uma preocupação e, pensando na "zona desconhecida" que são os crimes não citados neste material ou os que nascem e são reportados dia após dia, recomendamos realizar um assessment gratuito com um dos especialistas da Compugraf, que irão te apresentar um amplo portfólio de soluções para o seu ambiente.

A sua empresa necessita de soluções que atendam as necessidades de maneira integrada, então solicite agora mesmo o assessment gratuito para agendar um bate-papo com um de nossos especialistas e definir a melhor ferramenta para a sua infraestrutura.

**Solicitar Assessment Gratuito**

**Já acessou a segunda parte do material?**

Entenda os riscos por trás dos malwares clicando no botão abaixo:

**Os riscos por trás dos *malwares***

No mercado de soluções tecnológicas desde 1982, a Compugraf, empresa 100% brasileira, possui mais de 300 clientes ativos em nível nacional.

Nosso objetivo é sempre satisfazer nossos clientes com soluções avançadas, buscando melhorar continuamente nossos processos e equipe para fornecer produtos de alta tecnologia e excelência de serviços profissionais.

Conheça mais sobre nossas soluções em:
www.compugraf.com.br

Compugraf