HIGH SECURITY CENTER

RELATÓRIO DE AMEAÇAS POR E-MAIL

SPAM & PHISHING

Análise do 1º semestre de 2020

Sumário

Escopo do Relatório

Este relatório analisou dados obtidos de forma anônima da nuvem Smart Defender, enviados por mais de 100.000 empresas na América Latina. Hoje, são mais de 10 milhões de contas de e-mail protegidas e analisadas diariamente pela Inteligência Artificial do E-mail Secure Gateway Mailinspector. A plataforma registrou um fluxo de mais 69% de ataques, SPAM e mensagens indesejadas em um universo de aproximadamente 5,4 bilhões de mensagens processadas nos 6 meses iniciais de 2020.

A equipe HSC Incident & Response, examinou toda essa base de dados e relacionou com os mesmos meses de 2019 para evidenciar insights importantes. Considerou-se e-mails indesejados e ataques cibernéticos via phishing, BEC Mail, vírus, malwares, entre outras técnicas sofisticadas para obter ganhos financeiros sobre empresas.

Contribua para a próxima edição enviando suas dúvidas, perguntas e amostras para ***spamreport@hsclabs.com.***

Insights sobre um 2020 atípico

Foram consolidadas informações sobre ameaças direcionadas nossa base de clientes para trazer um panorama dos principais ataques e ameaças digitais no primeiro semestre de 2020. Foi analisado o tráfego de e-mails indesejados, incluindo SPAM e Phishing, em médias e grandes empresas em toda a América Latina. Também foram observadas novas técnicas e principalmente após grande mudança de comportamento produzida pelo pandemia do vírus COVID-19, o aumento na superfície de ataque das empresas como consequência da corrida para o trabalho remoto..

As consequências da pandemia requerem ações imediatas dos CIO, com reflexos de curto e longo prazo. Segundo pesquisa publicada pela EBC, 46% das empresas aderiram ao Home Office. Além disso, o percentual de companhias que adotou o tele-trabalho durante a quarentena foi maior no ramo de serviços hospitalares (53%) e na indústria (47%).

Os gestores das empresas já consideram os efeitos provenientes da pandemia permanentes, e que modificará de forma significativa o ambiente de trabalho em relação às décadas anteriores. Acelerando o processo de consolidação do trabalho remoto.

Com este novo horizonte, a exposição dos usuários de e-mail aos ataques avançados que empregam engenharia social, podem ser devastadores. Não restam dúvidas que usuários parados, perda de produção, desvalorização da marca, perda de propriedade intelectual, além do sequestro dados via ransomwares são os piores cenários de riscos associados aos portfólio de serviços de TI de qualquer empresa.

Mudanças abruptas no mercado global, assim como as consequências geradas por essas mudanças, são os principais desafios dos responsáveis pelas áreas de tecnologia. Os times de segurança da informação e gestores das áreas de tecnologia devem considerar o significativo e permanente aumento da superfície de ataque, agora híbrida entre serviços na nuvem e recursos locais, além de administrada de forma descentralizada, fora da infraestrutura corporativa.

Portanto, as novas políticas de segurança da informação devem levar em conta esses aspectos, como os recursos computacionais sendo utilizados na casa dos colaboradores e conectados a dispositivos pessoais e redes vulneráveis.

Como forma de facilitar a interpretação do cenário de cybersecurity, a HSC Labs, através da equipe HSC Incident & Response, elaborou este relatório focado nos principais ataques identificados em 2020 e suas principais características.

Romulo Boschetti, CEO High Security Center

Visão Geral de Phishing na América Latina

Durante todo o ano de 2019, as mensagens indesejadas e phishing representaram 67% das mensagens filtradas por nosso módulo de inteligência artificial chamado HSC Smart Defender. Somente no primeiro semestre de 2020, nossos sensores já bloquearam mais de 850 milhões de mensagens indesejadas, o que representa aumento de 23%, comparando com o mesmo período de 2019. Também foi identificado que o direcionamento, personalização e complexidade dos ataques, aumentaram na mesma proporção que a quantidade dos ataques.

Neste documento preparamos um relatório com muita informação, além da análise de especialistas e sugestões para sua empresa se preparar para as novas ameaças digitais.

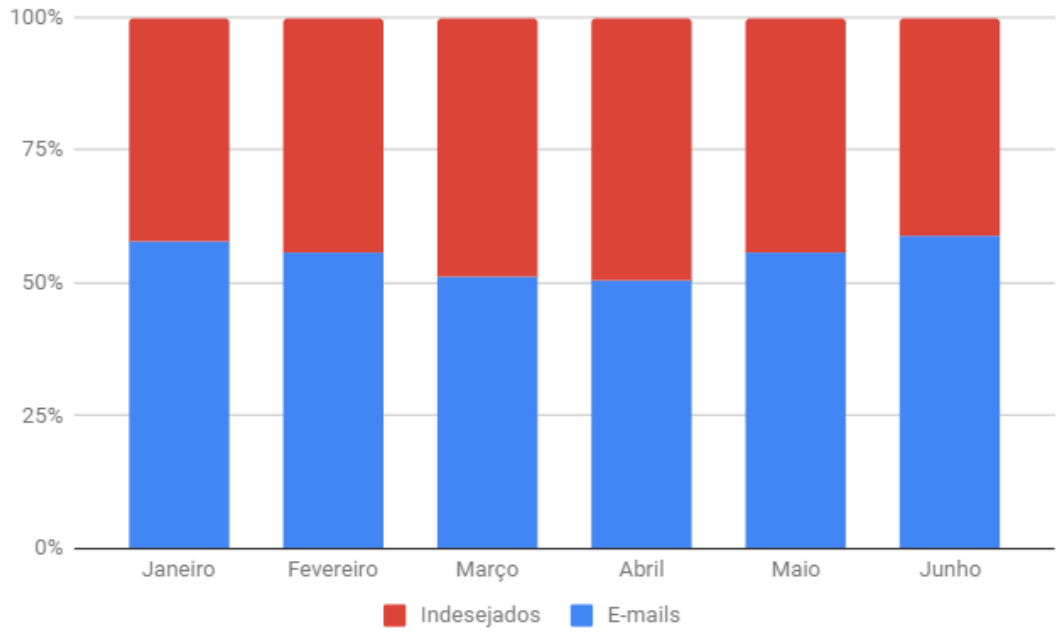
Como forma de facilitar a interpretação do cenário de cybersecurity na América Latina, a HSC Labs, através do levantamento realizado pela Equipe HSC Incident & Response, elaborou um relatório focado em ataques identificados em 2020 e suas principais características.

Da base de ataques consultada, foram analisados mais de 3,4 bilhões de mensagens sendo que em 2019 versus 2018, houve um aumento de 27% o que representou 67% do tráfego conforme relatório APWG 2018 e 2019. Já nos dados obtidos dos sensores da solução de proteção de e-mails Mail Inspector, apenas no primeiro semestre houve o registro de mais de 850 milhões de ataques, representando mais de 72% do tráfego filtrado.

A seguir, analisaremos os dados referentes a ameaças virtuais 2020, com foco em ataques de phishing e SPAM

Total de Mensagens vs SPAMs

Esta análise considerou os seis primeiros meses de 2020 e contou com 3,4 milhões de mensagens. Este primeiro gráfico traz uma visão generalista onde foi identificado como SPAM, vírus, e-mail marketing, malware phishing mais de 1,7 milhões de mensagens no primeiro semestre atingindo média superior a 53% de incidência de SPAM. Consideramos SPAM todas as mensagens não desejadas e limpas. Não foram considerados as conexões rejeitadas e que impediram de receber mais mensagens de origem maliciosa.

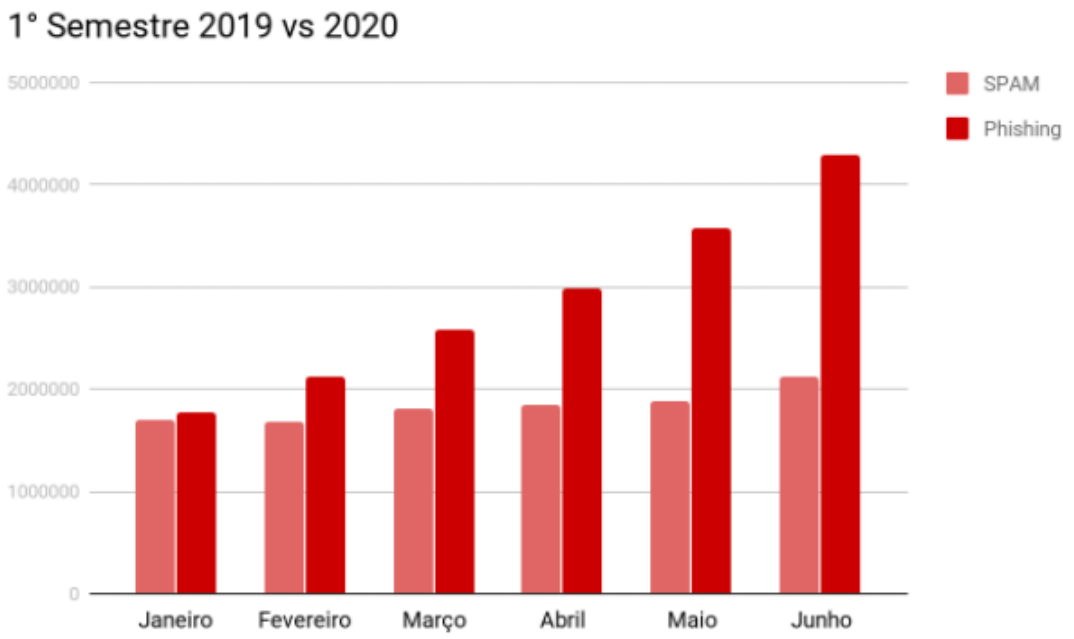


Na análise mensal, janeiro e fevereiro, apresentavam indicadores similares ao crescimento dos anos anteriores. Nos meses seguintes houve aumento nos ataques em relação às mensagens limpas, possivelmente pelo dinâmica trazida pelo Home Office. No final do primeiro semestre, sensível diminuição e aproximação à média anterior.

Comparativo: 1º semestre 2019 vs 2020

Segundo identificado pela equipe de Incident & Respond da HSC Labs, os meses de janeiro, fevereiro e março acompanhavam o crescimento anterior de envios de e-mails de phishing. Entretanto, ao final de março identificou-se um aumento considerável de 23% em campanhas de Spear Phishing, em que os usuários eram direcionados para páginas maliciosas onde eram facilmente ludibriados e informavam suas credenciais de acesso ao ambiente.

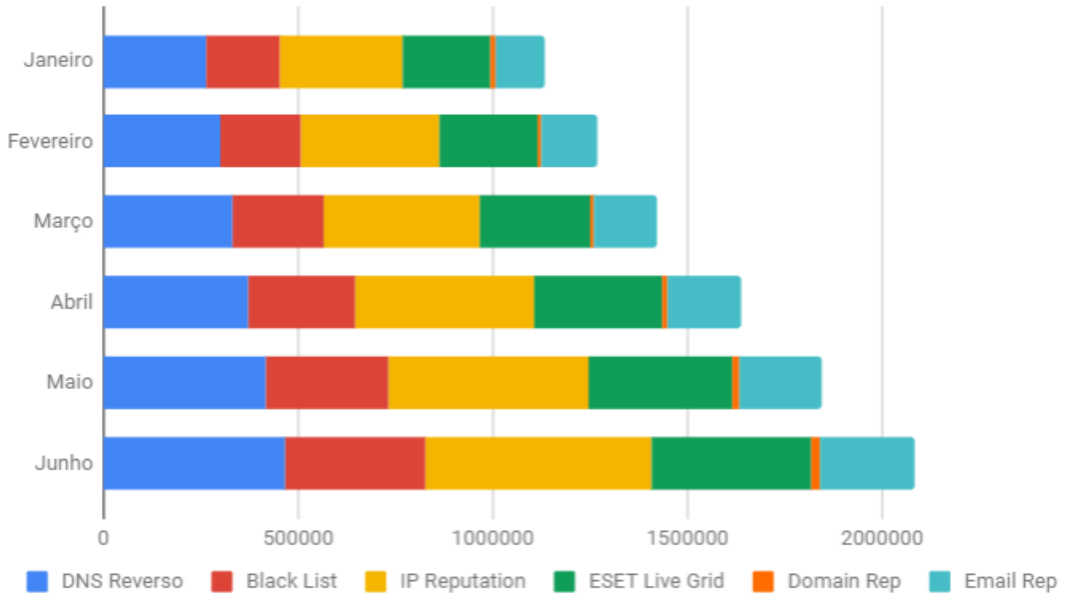
De posse do usuário e senha, os atacantes enviavam e-mails em nome do CEO (BEC) para colaboradores, clientes e fornecedores solicitando transferências em caráter de urgência, enviando boletos para pagamento ou documentos de uso cotidiano como listas de preços, catálogos e manuais para área comercial contendo código malicioso que realizava o download de um Backdoor.



O gráfico acima expressa o aumento dos ataques devido a pandemia Covid 19 e a facilidade de atacar os usuários desprotegidos trabalhando de casa, sem firewall, VPN e demais ferramentas de segurança cibernética que estão submetidos enquanto trabalhavam normalmente na empresa.

Conexões Rejeitadas

Concomitantemente com as mensagens acima, foram rejeitadas 2,7 bilhões de conexões de mensagens oriundas de servidores que não atendiam aos requisitos mínimos de segurança de e-mail ou apresentavam características de Spammers. As configurações de IP Reverso, Reputação de Host, Domínio, IP e E-mail Reputation, entre outras, interromperam o tráfego das mensagens, rejeitando suas conexões. Assim, não chegaram os ataques à infraestrutura da empresa, economizando recursos, como banda e processamento.



Neste contexto, o conteúdo da mensagem e anexos e não são recebidos e o processamento e tráfego é reduzido proativamente.

A ferramenta Mailinspector protege sua empresa antes que as ameaças cheguem, analisando a reputação em uma rede de Inteligência Artificial que avalia e monitora diversos serviços de e-mail. a cada conexão os servidores de origem são consultados e caso não sejam atendidos requisitos mínimos para garantir a propriedade do domínio e respectivas configuraçẽos do servidor de email, as mensagens são bloqueadas.

Adesão aos recursos de segurança SPF e DKIM

A implementação das tecnologias de legitimação de mensagens Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM) e Domain-Based Message Authentication Message Conformance (DMARC) foi iniciada em 2014, a partir da RFC 7208, que incrementou novos recursos que aumentaram a segurança da comunicação por e-mail. Entretanto, não foram adotados por parte das empresas até hoje.

O SPF informa através do DNS quais os servidores de e-mail autorizados a enviar mensagens. Esta consulta é feita por servidores de terceiros que, ao receber uma mensagem, validam se originou-se em um dos servidores de e-mail autorizados no DNS do domínio.

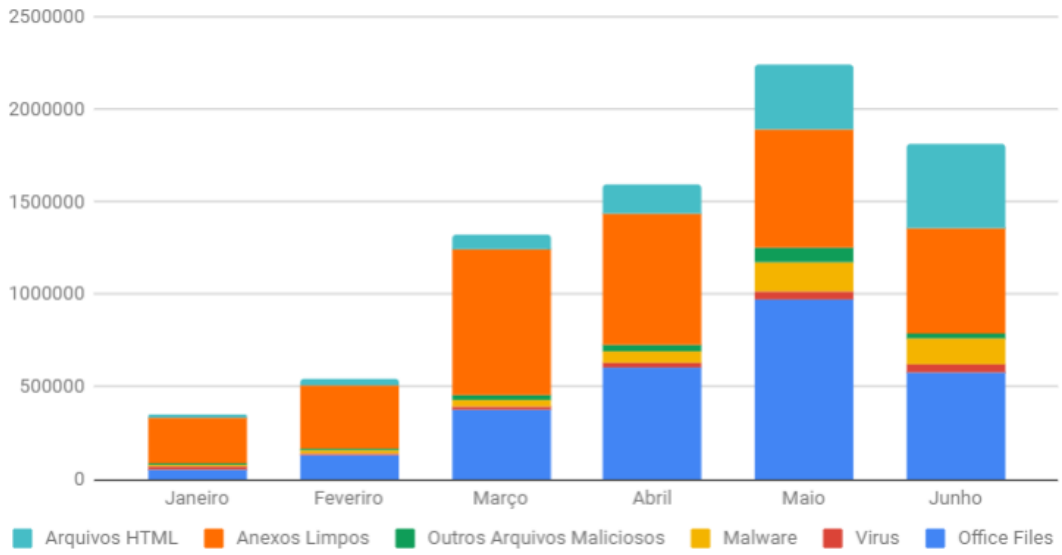
O DKIM é uma tecnologia que utiliza um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas, uso de hash e DNS. Este protocolo garante ao receptor a autenticidade de quem o escreveu e que o e-mail não foi alterado durante a transmissão.

Os protocolos acima não fornecem instruções para atuar proativamente contra um ataque. Já o DMARC consiste em um relatório de tráfego de mensagens que indica detalhes sobre o uso indevido de domínios por servidores não autorizados no registro SPF, ou mensagens alteradas durante o tráfego que não atendam ao hash gerado com uma chave no protocolo DKIM. A adoção do DMARC permite informar que, caso o SPF e DKIM não atendam, a mensagem deva ser rejeitada.

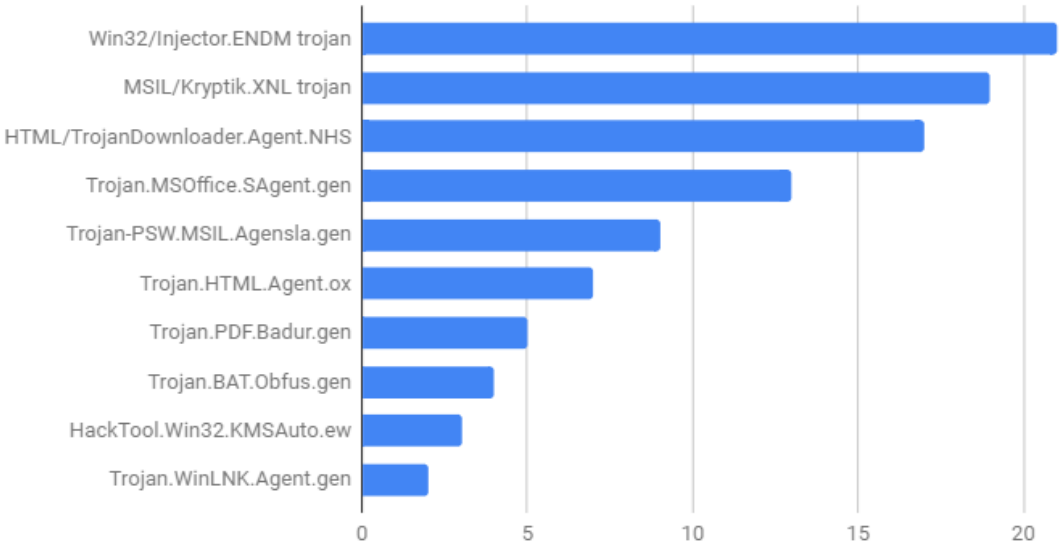
Caso os três protocolos obtenham maior aderência no mercado público e privado, aumentará seus resultados positivos diminuindo o tráfego indesejado.

Análise de Anexos Maliciosos

Ao analisar os anexos dos e-mails bloqueados, foi identificado pela equipe, que os arquivos mais comuns nos ataques continham documentos do pacote Microsoft Office com scripts maliciosos. Arquivos no formato PDF são comuns e estão considerados no grupo Office Files.



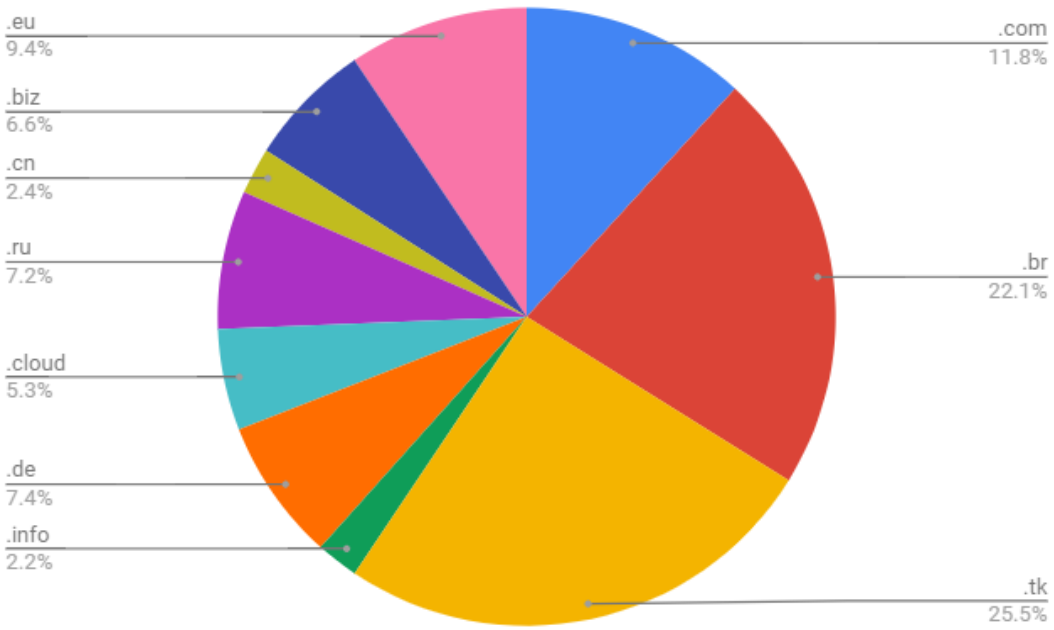
A relação com a pandemia neste âmbito foi relacionada a campanhas de phishing contendo programas falsos para rastrear o avanço da pandemia na América Latina.



Domínios de Topo mais utilizados para Ataques

Assim como é pertinente saber diferenciar a origem dos principais ataques, os gestores de segurança precisam conhecer os domínios de topo mais utilizados para ataques, buscando aumentar a segurança. Territórios independentes, como Tokelau, facilitam o registro de domínios com poucos requisitos burocráticos e baixos custos de aquisição.

Ao analisar os domínios usados nos ataques, verificamos que grande parte são oriundos de TLDs com tais características. veja a seguir os principais TLDs identificados:



Sistemas inteligentes utilizam a análise de TLDs em seus algoritmos e consideram em alguma camada seu bloqueio. A interação com nuvem de dados do HSC Smart Defender identifica os TLDs mais utilizados em ataques de e-mail e protege mais de 6 milhões de mailboxes em toda América Latina.

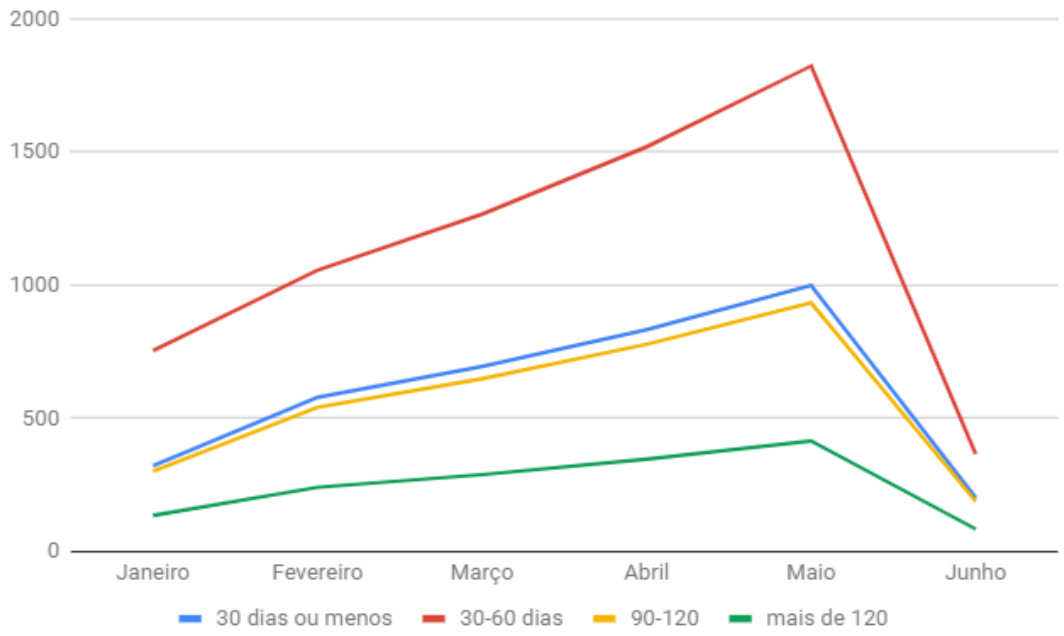
A origem dos Ataques

Países latinos também são alvos dos principais grupos de hackers, como Evil Corp, Calypso, Phosphorus e APT20, sediados em países como China, Rússia, Coreia do Norte e Irã. Muitos grupos são suportados pelos governos e contratados através da deep web, o que lhes garante o anonimato e segurança. Para dificultar o rastreamento dos contratantes, utilizam bitcoin e outras criptomoedas menos populares.

A análise do Range de IPs dos servidores de origem das mensagens é pertinente e utilizada por muitas ferramentas de proteção cibernética. O Mailinspector, identifica ataques de DDOS e pontua distintamente dependendo do país de origem e o idioma utilizado na mensagem. A partir disso, mapeia os países de origem das conexões e utiliza essa inteligência para impedir que mensagens maliciosas cheguem às caixas de e-mail de usuários protegidos.

Análise de tempo de registro de domínios

Ao trazer a luz para os domínios envolvidos em ataques, seja hospedando o site falso ou apenas utilizado como origem de e-mail, observamos que os Spammers aguardam para em média 40 dias para disparar os primeiros ataques. Na maioria das vezes, o tempo para remover o site malicioso do ar é maior.



É importante possuir ferramentas de segurança flexíveis, que compreendam como atuam os grupos criminosos e se adaptem rapidamente às práticas. As interações com outros sistemas de segurança entrega maior velocidade para bloquear um ataque e aumenta a precisão nas ações além de requerem menor administração da equipe de TI.

O Mailinspector possui um módulo que identifica a data de registro do domínio e aplica ações de classificação, conforme parametrizado, para compor uma pontuação atribuída à mensagem ou para bloqueá-la. Isso permite que a plataforma identifique domínios recém criados para um ataque ou criados há menos de 6 meses.

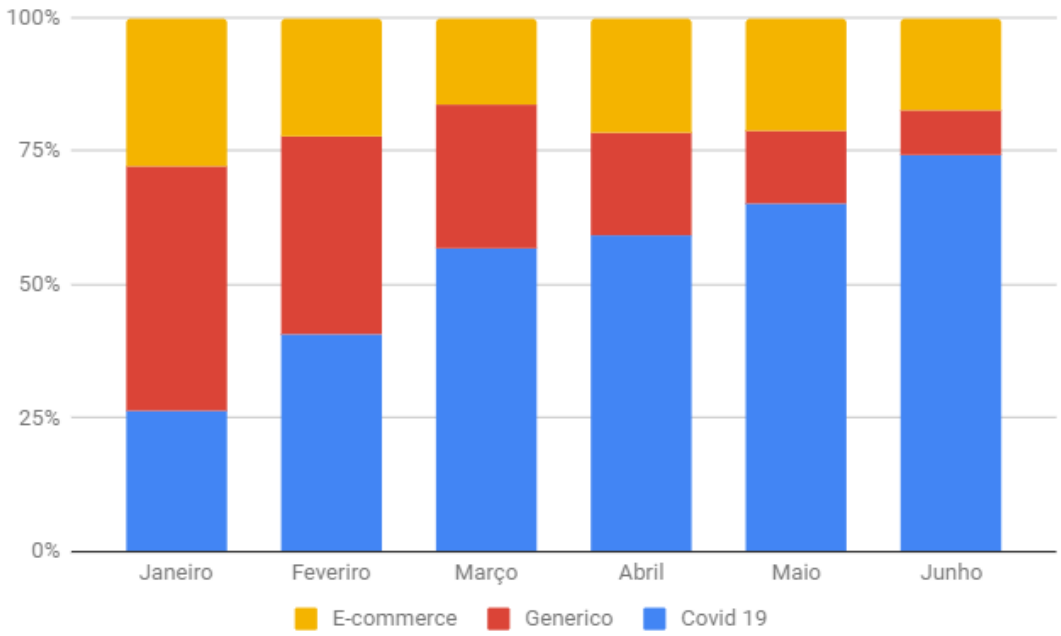
Aumento expressivo das campanhas de Phishing

A equipe de pesquisadores observou um aumento nos ataques de phishing, malwares e ransomwares relacionados ao COVID-19. Os ataques vinculados por e-mail fraudam marcas e as usam para atingir funcionários e clientes. Os arquivos e links analisados, baixam e executam ransomwares disfarçados de aplicativos legítimos.

É imperativo que as organizações tomem medidas proativas em seus ambientes e aumentem a segurança considerando o trabalho remoto. Aos usuários, é recomendado treinamento e aconselhamento para serem mais vigilantes e cautelosos, especialmente na abertura de links em emails, sites de conteúdo duvidoso obtidos por e-mail, sms, redes sociais, além de programas ou documentos relacionados ao COVID-19. Os sistemas de segurança devem interagir e diminuir a exposição que o trabalho remoto gerou nas organizações.

As campanhas de Phishing representam um método eficiente para atingir os usuários distribuídos em suas casas, sem firewall, proxies ou uso da VPN para proteção. Nesse cenário, a vulnerabilidade aumenta, pois o e-mail é a principal ferramenta de comunicação utilizada internamente e externamente pelas empresas, logo sua ampla utilização facilita ao atacante localizar o alvo final: o usuário. Esse cenário facilita a investida através de ataques de e-mail, por ter baixo custo de implementação. Além disso, o uso de novas temáticas é uma característica presente nos ataques atuais.

O gráfico abaixo reflete o aumento dos ataques relacionados a pandemia COVID19, ações governamentais de auxílio e afins, com objetivo de obter informações pessoais, credenciais de acesso para requererem e ou desviarem os valores oriundos de ações governamentais.



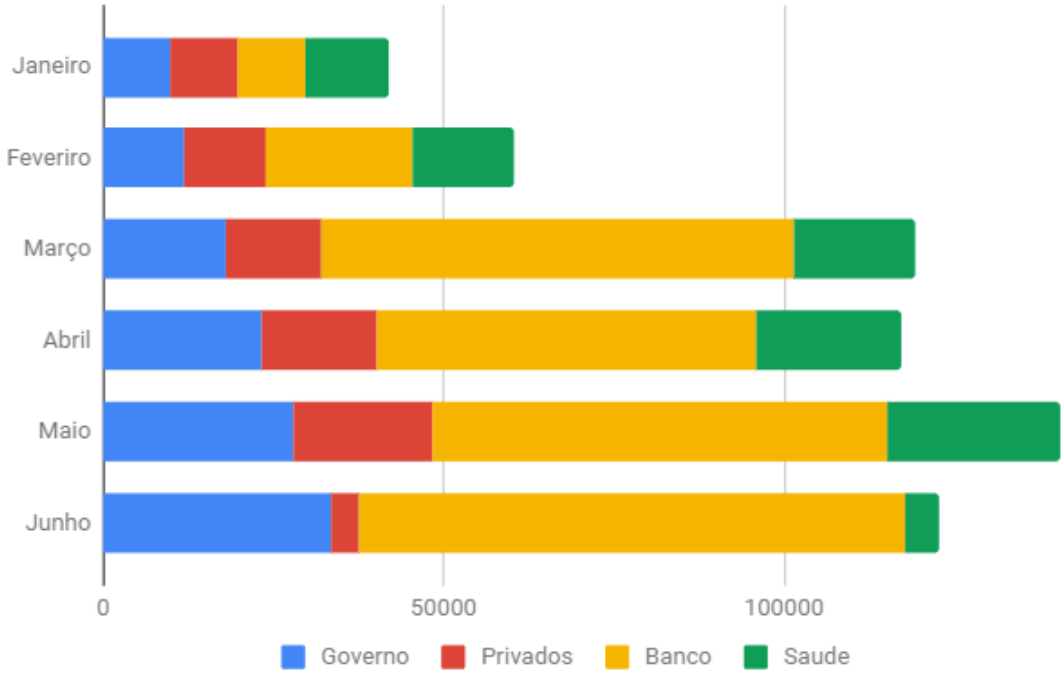
O estudo observou crescimento de mais de 800% em spam durante a pandemia, sobretudo relacionado à pandemia de Covid-19.

O conteúdo das mensagens leva o leitor a abrir anexos e acessar links oriundos de falsas entidades, privadas e públicas, que permite acesso ao dispositivo do usuário.

De posse das credenciais da empresa, pode realizar ataques utilizando o nome e os recursos, o que gera prejuízos a marca e financeiros, como ainda iremos abordar na análise de BEC. Ou ainda, permite criptografar o dispositivo e exigir pagamento para o resgate dos dados indicando carteiras de moedas digitais muitas vezes, ou contas sobre controle do cibercriminoso.

Segmentos mais atingidos por Ataques de Phishing

Analisando por segmento de atuação, identificamos que os usuários mais visados pelos atacantes foram do setor bancário e governo. Ao contrário de outras regiões em que instituições da área da saúde foram mais frequentes, na América Latina temos os bancos em primeiro lugar.

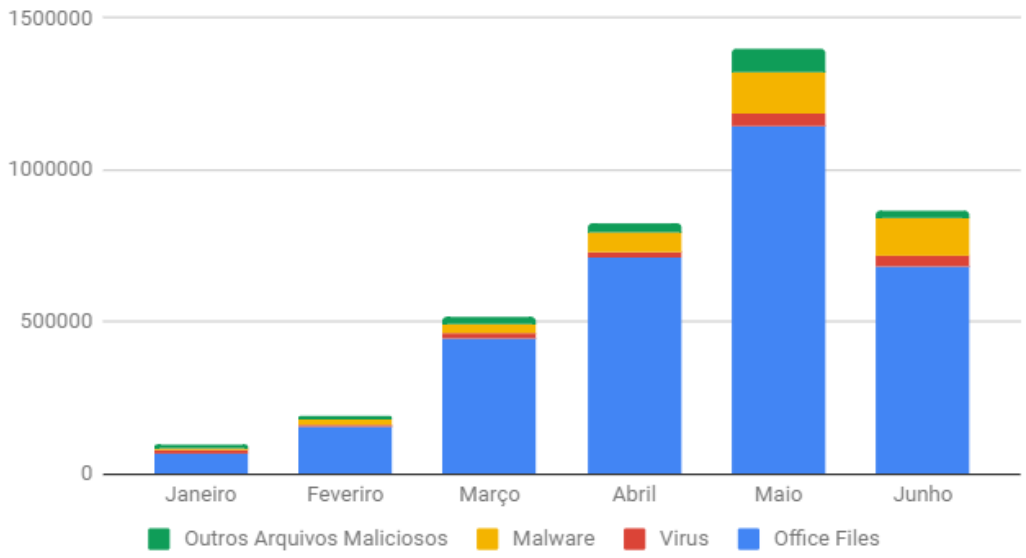


A busca por instituições de saúde e bancos é mais frequente devido ao fato das mesmas não serem tão protegidas como deveriam a principalmente a capacidade de contrapartida no caso de um ataque ser bem sucedido.

Anexos Maliciosos relacionados ao Covid-19

Anteriormente, neste relatório, analisamos os tipos de anexos maliciosos em mensagens de e-mail. No gráfico a seguir, analisamos os anexos contidos em ataques relacionados a Pandemia diretamente ou como reação à ações de governos ou organizações, como é o caso do auxílio emergencial no Brasil.

Os ataques de arquivos com Scripts em HTML e Office Files são os mais comuns. Entre os Malwares, o aumento de programas maliciosos com extensão .apk aumentaram nos meses de maio e junho.



Além do aumento de SPAMs e ataques relacionados ao COVID durante a pandemia, deve-se levar em conta o tráfego das informações de sua empresa pelas redes wireless sem segurança e computadores domésticos, que podem estar sendo usados durante expediente doméstico dos funcionários.

Para proteger as contas de e-mail contra ataques sofisticados, o Mailinspector emprega Inteligência Artificial e técnicas de SandBox para analisar a mensagem e seus anexos. Ao identificar um Link na mensagem, simula a navegação do usuário e categoriza o conteúdo do site. Caso o link realize download de um arquivo, o mesmo será executado e o ambiente da Sandbox irá identificar o comportamento deste arquivo.

Consequências do ataque bem sucedido: Business E-mail Compromise

Entender como ocorrem os ataques é imprescindível para evitá-los. Um dos ataques que gera maior impacto financeiro para as empresas é conhecido como Business E-mail Compromise. Este ataque consiste em adquirir as credenciais de um executivo de alto escalão, como diretoria geral ou financeira, para enviar solicitações falsas de transferências de valores.

Para isso, em um primeiro momento o ataque utiliza de Engenharia Social para obter dados sobre o quadro social da empresa e conseguir acesso a uma conta de e-mail. A partir dela, o atacante poderá conhecer o ambiente da empresa e identificar as pessoas com cargos mais representativos para direcionar o ataque a elas. De posse das credenciais de um executivo, o ataque é direcionado para um funcionário que seguirá as solicitações do e-mail sem questionar, efetivando uma transferência financeira. Caso não obtenha sucesso, irá direcionar para outras pessoas, como clientes ou fornecedores, a fim de obter seu objetivo.

Etapas do BEC

- Identifica o alvo: reúne informações disponíveis na internet, jornais, revistas e redes sociais da empresa e funcionários
- Prepara o ataque: o invasor usa uma variedade de ataques contra seu(s) alvo(s) a fim de manipulá-los e pressionar o alvo escolhido
- Troca de informações: o alvo é convencido que é uma comunicação legítima
- Pagamento: os fundos são transferidos para uma conta bancária administrada pelo invasor

BEC na prática

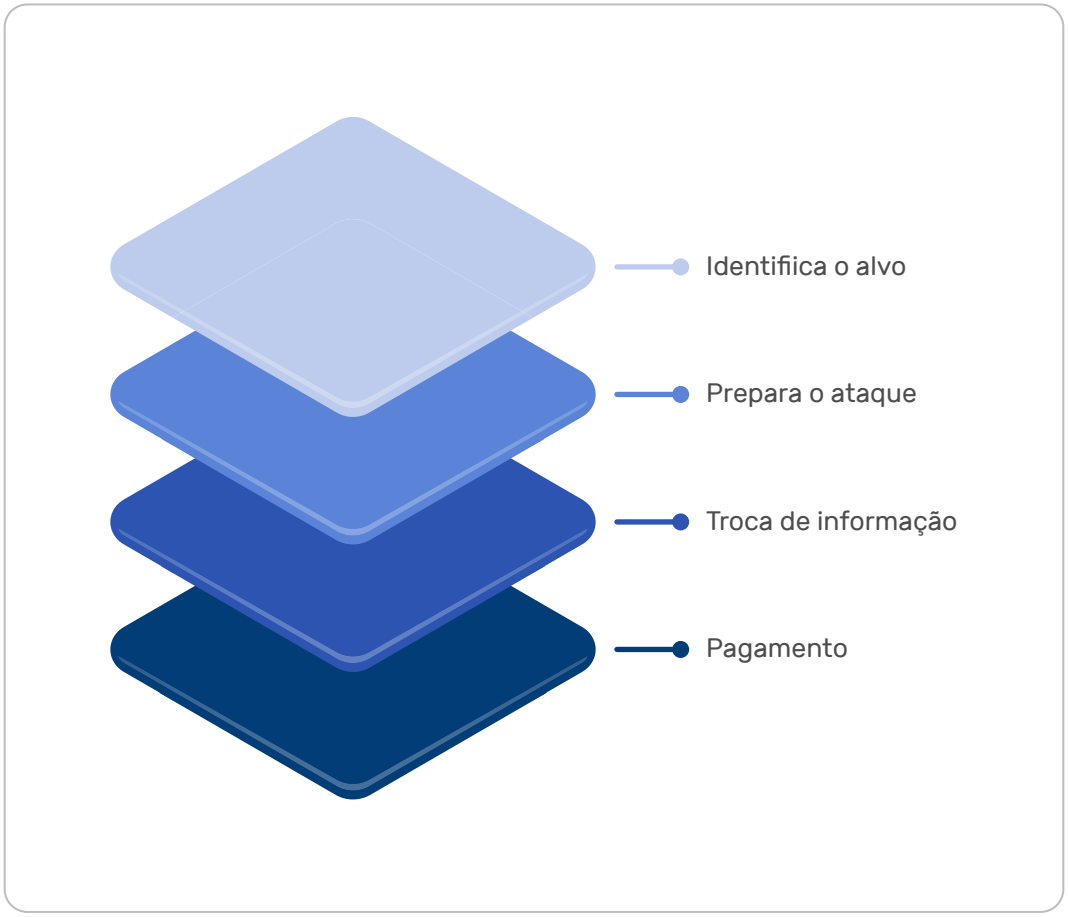
Um hacker invade uma conta de e-mail com senha fraca, através de um simples formulário que requer troca de senha, após a execução de um anexo malicioso que abre um backdoor e obtém acesso a uma conta da empresa.

Após analisar as trocas de mensagens e identificar os funcionários do alto escalão da empresa, compõem um e-mail falso e se faz passar pelo CEO ou CFO pedindo a um

funcionário do departamento financeiro que transfira fundos para uma nova conta. Este cenário é comum e ocorre com frequência pois a maioria dos funcionários não questionaria uma solicitação por escrito e documentada por e-mail oriunda do presidente da empresa.

Como essas contas de e-mail foram manipuladas e têm táticas bem ocultas, os ataques de BEC são difíceis de detectar e podem deixar as empresas expostas a grupos de cibercriminosos. Muitos sistemas de proteção de email não identificam ataques em mensagens internas. O Mail Inspector utiliza dados das comunicações legítimas usadas anteriormente, nome dos hosts e outros recursos para impedir que ataques BEC cheguem às contas de e-mail dos usuários da empresa.

O e-mail é o principal vetor de ameaças da atualidade, respondendo por 90% das ameaças avançadas. O desenho abaixo ilustra as 4 etapas citadas:

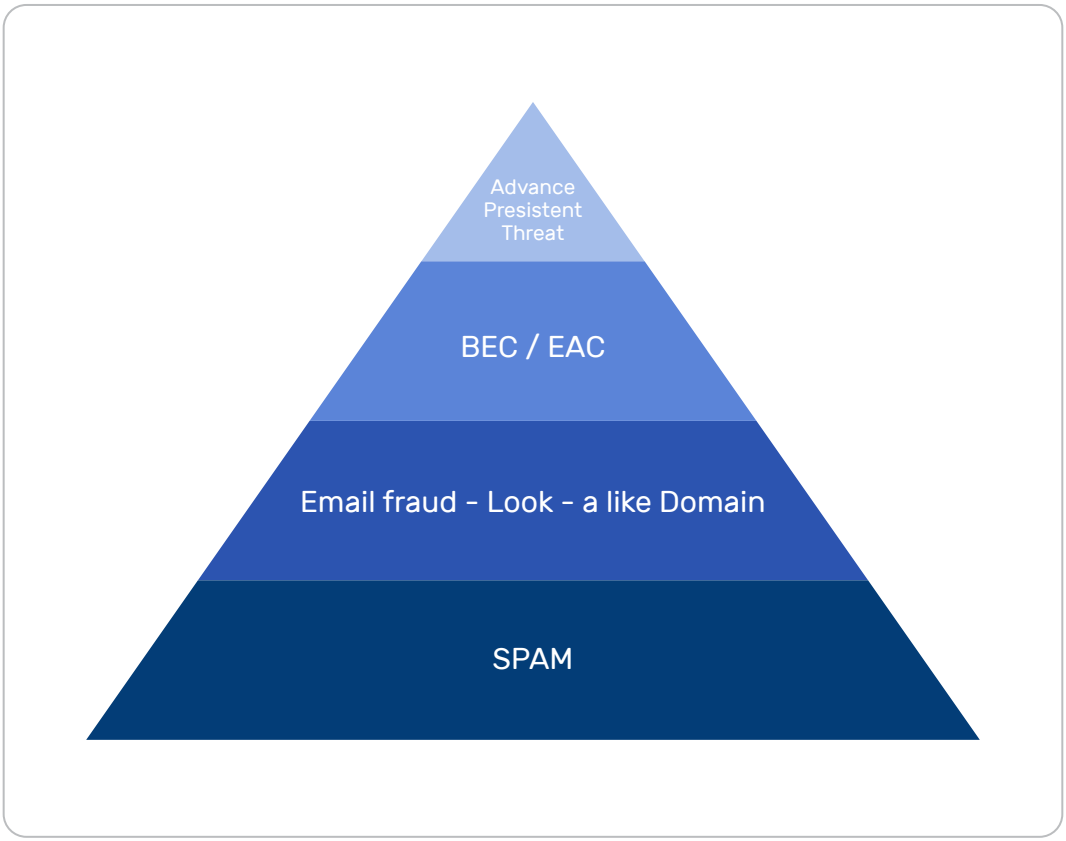


Aumento da sofisticação dos ataques por e-mail

Anteriormente, neste relatório, analisamos os tipos de anexos maliciosos em mensagens de e-mail. No gráfico a seguir, analisamos os anexos contidos em ataques relacionados a Pandemia diretamente ou como reação à ações de governos ou organizações, como é o caso do auxílio emergencial no Brasil.

Os ataques de arquivos com Scripts em HTML e Office Files são os mais comuns. Entre os Malwares, o aumento de programas maliciosos com extensão .apk aumentaram nos meses de maio e junho.

Com o passar dos anos os ataques por e-mail foram diversificando e mudando a abordagem utilizada. Anteriormente, era frequente mensagens contendo vírus entre os anexos. Atualmente os ataques são mais sofisticados não utilizam anexos e obtém sucesso quando atingem seu destino: os usuários da empresa.



Considerações finais

Como observado pelo estudo apresentado, o cenário atual requer que as empresas reconheçam os riscos relacionados à comunicação por e-mail, além de empregarem as tecnologias que proporcionem maior segurança, como o SPF.

É também imperativo que impeçam que atacantes utilizem da reputação da sua empresa para ludibriar clientes, analisando os relatórios de DMARC e tomando as ações legais em pouco tempo.

- mais de 65% das mensagens enviadas são SPAM no primeiro semestre de 2020.
- 89% das empresas já sofreram ataques de Spear Phishing entre 2019 e 2020
- usuários sem treinamento contra ataques cibernéticos são a principal vulnerabilidade
- CEO & CIO devem tomar ações de curto e longo prazo considerando as tendências de ataques atuais (hoje) e permanentes após a pandemia.

Para obtenção destes insights, foram analisados dados anônimos enviadas por mais de 1000 empresas, totalizando 2,6 milhões de contas de e-mail e 3,3 bilhões de mensagens analisadas no primeiro semestre de 2020.

Sobre a High Security Center

A HSC é uma empresa brasileira focada no desenvolvimento de soluções para segurança da informação. Utiliza tecnologias de Machine Learning e Behavior Analysis para proteger as empresas contra ameaças em tempo real, como ataques dirigidos e persistentes, ransomwares, phishing, mensagens indesejadas (SPAM) e muito mais. Entre seus principais produtos estão o MailInspector, uma solução para Security E-mail Gateway e o Internet Security Suite, solução para controle de conteúdo Web (Secure Web Gateway).

Sobre o autor do relatório

Ivan Szuhanszky faz parte do time de Incident & Response da High Security Center e é formado em Gestão de TI e Pós-Graduado em Perícia Digital Forense. Atua há mais de 10 anos com infraestrutura e segurança da informação.

Contato

(51) 3216-7007
negocios@hscbrasil.com.br
www.hscbrasil.com.br