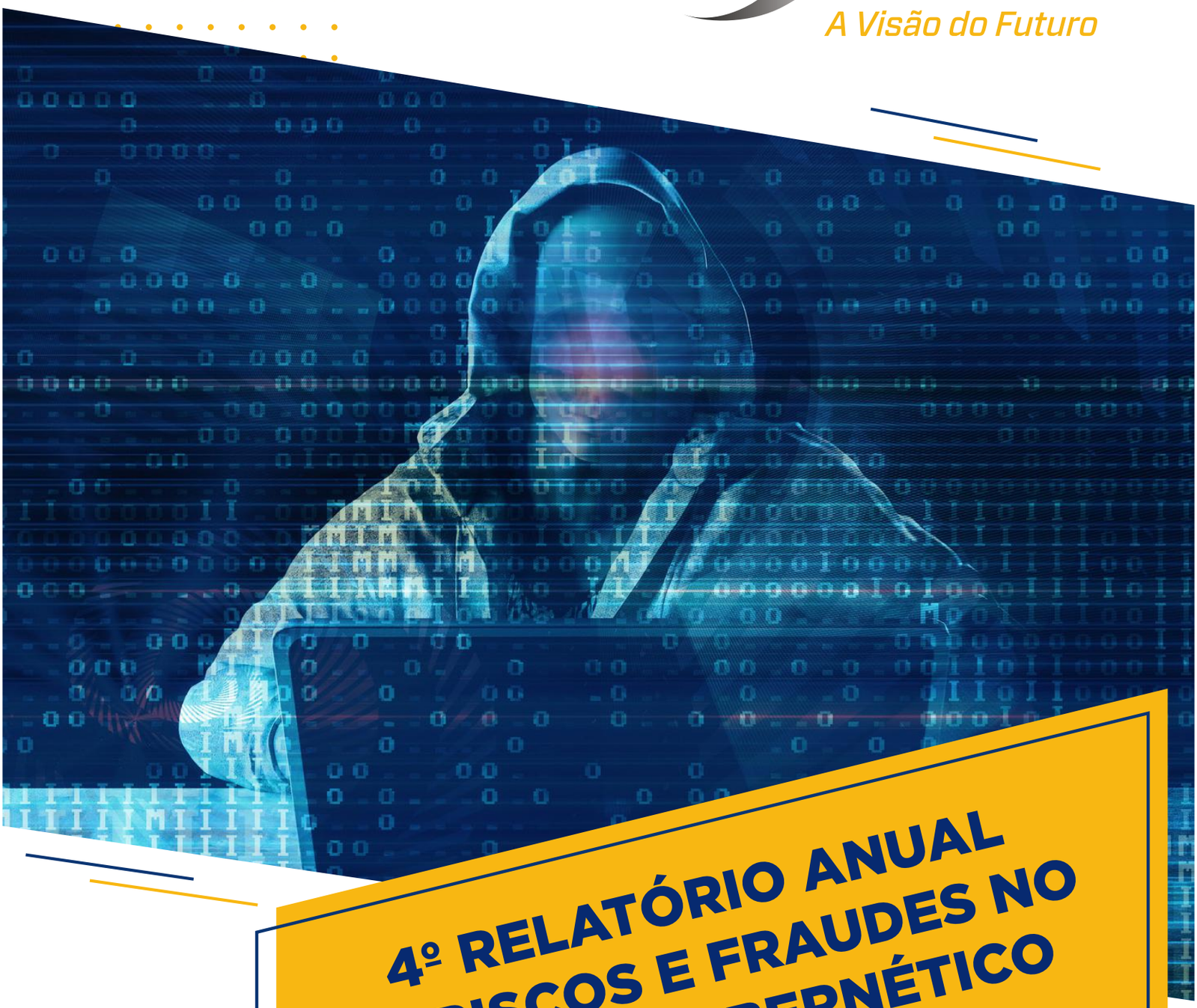
GRUPO NEW SPACE®
A Visão do Futuro



# 4º RELATÓRIO ANUAL DE RISCOS E FRAUDES NO CENÁRIO CIBERNÉTICO

// JUNHO DE 2019 //

# ÍNDICE

# INTRODUÇÃO

Mais uma vez, o **Grupo New Space** divulga o seu Relatório Anual de Riscos e Fraudes no Cenário Cibernético. Com uma visão analítica sobre a história recente, episódios de destaque e demandas globais de cibersegurança, o documento ressalta tendências e apresenta considerações preditivas para o curto e para o médio prazo.

A edição de 2019 foi realizada em parceria com o Grupo DARYUS, especialista em Gestão de Riscos, Governança e Compliance. A expertise do núcleo DARYUS Consultoria contribuiu para enriquecer o material, pois possibilitou ampliar a abrangência do anuário com dados e reflexões complementares aos apontamentos da NS Prevention.

Boa leitura!

Produzido por: Silvana Tavares, Paula Guerra e Thiago Bordini do Grupo New Space; Jeferson D'Addario, Nadia Guimarães e Vanessa Oliveira do Grupo DARYUS.

# CONTEXTO GLOBAL CIBERNÉTICO

Mundialmente, os cenários cibernéticos são discutidos com o intuito de compreender o âmbito no qual as empresas estão inseridas, principalmente frente aos riscos dos negócios, interações e serviços digitais. Desde o início da Revolução Digital, com destaque para a 4ª Revolução Industrial, as empresas avançam, exponencialmente, no uso da internet e dos recursos derivados dos processos de digitalização. Com isso, a vulnerabilidade às fraudes e aos ataques dos cibercriminosos demandam cada vez mais atenção.

O caminho para adaptar-se à hipercomplexidade atual, visando proteção e segurança, passa invariavelmente por uma trilha de conscientização da realidade dos riscos, assim como por tomadas de decisão e posicionamentos dos gestores que orientem a construção e o aprimoramento das condições de cibersegurança e da mitigação dos riscos. Nesse sentido, observar criticamente os acontecimentos recentes é fundamental para assimilar o contexto e identificar as tendências.

O **4º Relatório Anual de Riscos e Fraudes no Cenário Cibernético** apresenta os resultados de estudos realizados em 2018 como base para a indicação de tendências para 2019 e 2020,

destacando o ataque por malwares direcionados. Contrariando as expectativas do quadro internacional de eficácia da GDPR - General Data Protection Regulation -, em 25/05/2018, e do quadro nacional de sanção da LGPD - Lei Geral de Proteção de Dados -, em 14/08/2018, o ano anterior à divulgação deste relatório concentrou diversos casos de violação de dados e de segurança.

Mesmo imersas nas discussões e preparações para as leis sobre privacidade e proteção de dados, inclusive nos meios físicos, em 2018, muitas empresas sofreram violações, como vazamentos e acessos indevidos. Em linhas gerais, as motivações dos infratores foram desde ataques direcionados, para atingir a imagem da organização, até obtenção de dados para comercialização. Ocorreram casos de grande repercussão com empresas dos mercados tecnológico e hoteleiro, por exemplo. No circuito nacional, destacaram-se e-commerces, financeiras, varejistas e empresas de grande relevância de vários segmentos, incluindo líderes de setor.

## CRIMES CIBERNÉTICOS E OS CIBERCRIMINOSOS

Os cibercriminosos atuam de forma ilícita, via internet, em ambientes comuns para qualquer cidadão, como as redes sociais, websites de compartilhamento de informações, chats, dentre outros. Valendo-se de identidades falsas e do anonimato digital, mantêm-se camuflados. Porém, mesmo utilizando técnicas sofisticadas de camuflagem de endereços de IP ou de outros registros, em algum momento acabam sendo rastreados e descobertos. Aliás, os processos de identificação tendem a ser mais comuns em ataques que derivam de fraudes financeiras ou se há monetização por parte do atacante.

## FRAUDES COM CREDENCIAIS DE ACESSO

Grande parte das estratégias dos grupos de fraudadores consiste em transformar as vulnerabilidades do ambiente empresarial em produtos de comercialização ou troca, como é o caso da doação e/ou venda de credenciais. Usando os dados desviados, criminosos digitais podem usar os acessos para tentar inva-

**EM 2018, MUITAS EMPRESAS SOFRERAM VIOLAÇÕES, COMO VAZAMENTOS E ACESSOS INDEVIDOS. EM LINHAS GERAIS, AS MOTIVAÇÕES DOS INFRATORES FORAM DESDE ATAQUES DIRECIONADOS, PARA ATINGIR A IMAGEM DA ORGANIZAÇÃO, ATÉ OBTENÇÃO DE DADOS PARA COMERCIALIZAÇÃO. OCORRERAM CASOS DE GRANDE REPERCUSSÃO COM EMPRESAS DOS MERCADOS TECNOLÓGICO E HOTELEIRO, POR EXEMPLO. NO CIRCUITO NACIONAL, DESTACARAM-SE E-COMMERCES, FINANCEIRAS, VAREJISTAS E EMPRESAS DE GRANDE RELEVÂNCIA DE VÁRIOS SEGMENTOS, INCLUINDO LÍDERES DE SETOR.**

dir contas dos mesmos usuários em diversos serviços, aproveitando o fato de que muita gente repete suas palavras-chaves em múltiplos canais. Com as informações necessárias para adentrar um sistema, ao acessar dados sensíveis, tanto pessoais como corporativos, o cibercriminoso pode cometer diversos outros tipos de violações cibernéticas.

## ATAQUES MAIS COMUNS:

• **Spoofing:** é um tipo de falsificação tecnológica com a intenção de mascarar uma rede ou uma pessoa, levando a acreditar que a fonte de uma informação é confiável, quando a realidade é bem diferente;

• **Phishing:** ataque no qual cibercriminosos enganam o usuário, fazendo com que ele revele informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Isso é feito por meio do envio de e-mails falsos ou direcionamento do usuário para websites falsos;

• **Ataques** diretos com acesso ao sistema da organização.

Esses três tipos de ataque são aplicados para auxiliar, no caso de uma possível fraude, ou para servir de insumo para invasões que resultam em vazamentos.

## ATAQUE COM USO DE ENGENHARIA SOCIAL

Os ataques direcionados, ou seja, aqueles com alvo determinado, utilizam o método de Engenharia Social como input para o

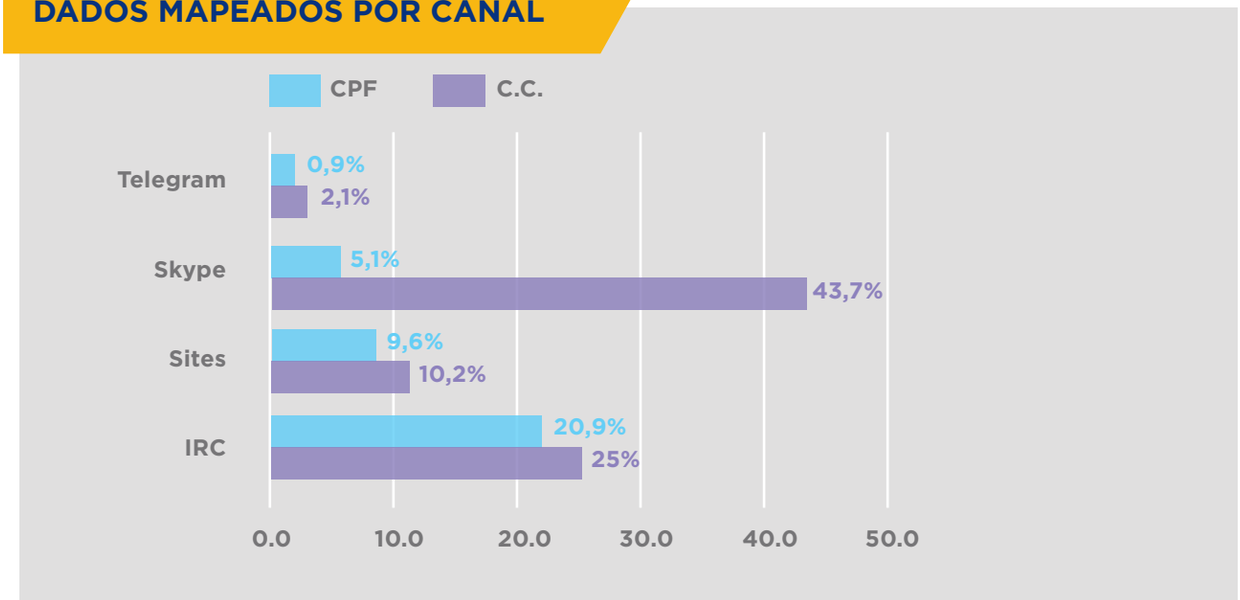

**Práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou da exploração da confiança das pessoas.**

# PESQUISA ANUAL NS PREVENTION

**PESQUISA REALIZADA PELA NS PREVENTION, EMPRESA DE SERVIÇOS DE SEGURANÇA CIBERNÉTICA DO GRUPO NEW SPACE**

Para maior compreensão do cenário de comercialização, a **NS Prevention** realizou uma pesquisa por meio dos seus serviços de segurança cibernética, no período de junho de 2018 a maio de 2019.

## DADOS MAPEADOS POR CANAL



A pesquisa identificou que o maior percentual de vazamento de dados de cartão de crédito ocorreu por meio do canal de comunicação Skype (43,7%), seguido por:

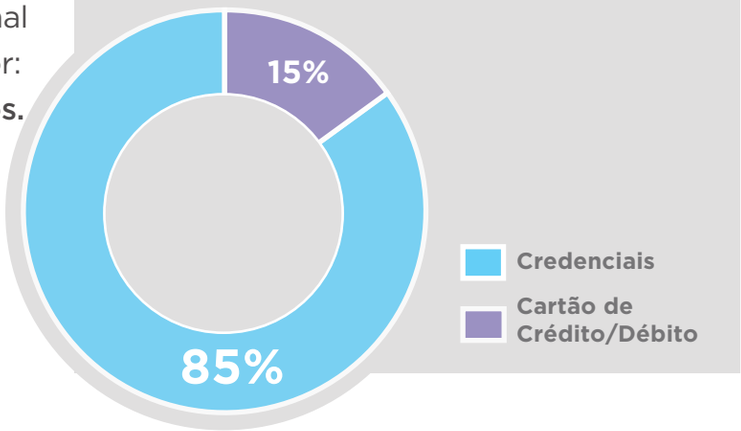
- **25% em salas de IRC.**
- **10,2% em sites de compartilhamentos.**
- **2,1% em grupos de Telegram.**

Já com relação a dados como CPF, temos como maior concentrador o canal IRC, com 20,9% de dados, seguido por:

- **9,6% em sites de compartilhamentos.**
- **5,1% em grupos de Skype.**
- **0,9% em grupos de Telegram.**

A pesquisa revelou também os percentuais de cartões de crédito e de credenciais vazados, considerando o período de junho de 2018 a maio de 2019, apontados por meio dos serviços de segurança cibernética.

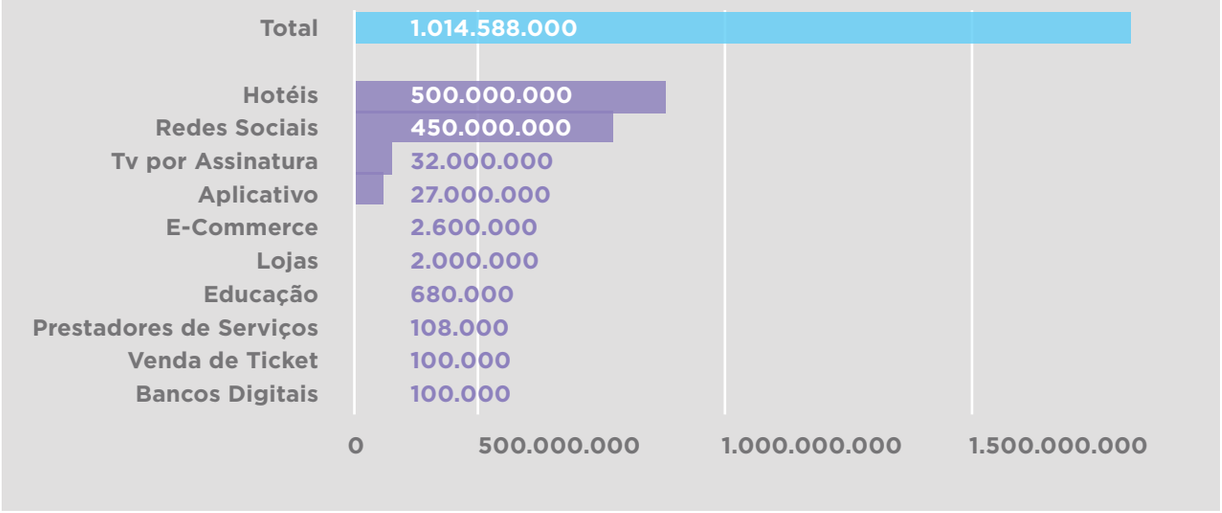
**MONITORAMENTO FRAUD MONITOR 2019**




A análise foi realizada por meio do **Fraud Monitor**, ferramenta de antifraude da **NS Prevention**, e nos revela que 85% dos vazamentos consistem em dados de credenciais, variando entre CPF e e-mail ou e-mail e senha, seguido por 15% de cartões de crédito, o que evidencia que ano passado foi promissor para os vazamentos.

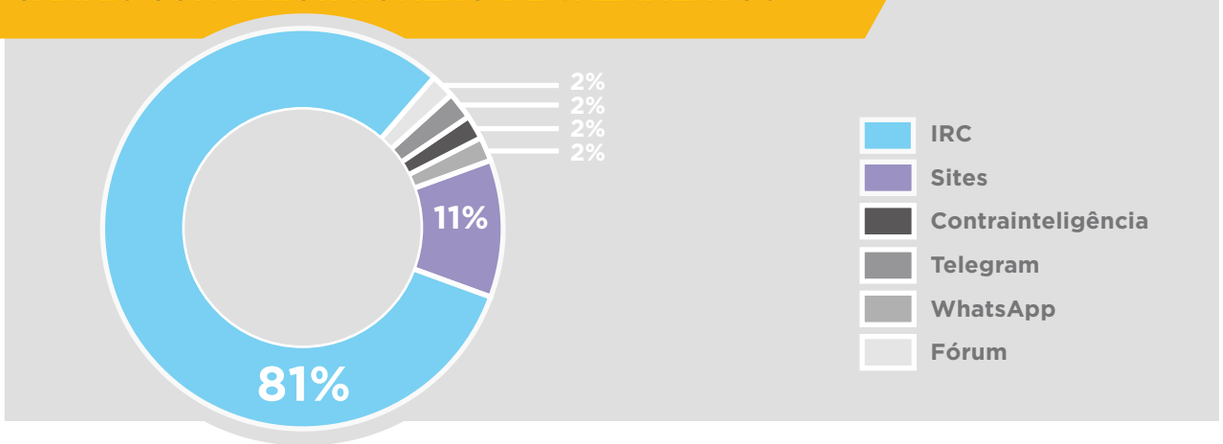
Na pesquisa com uso do **Fraud Monitor**, observa-se uma diferença de 70% entre vazamento de credencial e vazamento de cartão de crédito em 2019, evidenciando mais uma vez que os dados de credenciais são os mais utilizados pelos fraudadores afetando diretamente a imagem da empresa. A pesquisa ainda destaca quais os segmentos mais afetados com os vazamentos ocorridos no ano passado pelo volume total de dados vazados: 1.014.588.000.

## QUANTIDADE DE DADOS VAZADOS POR SEGMENTO



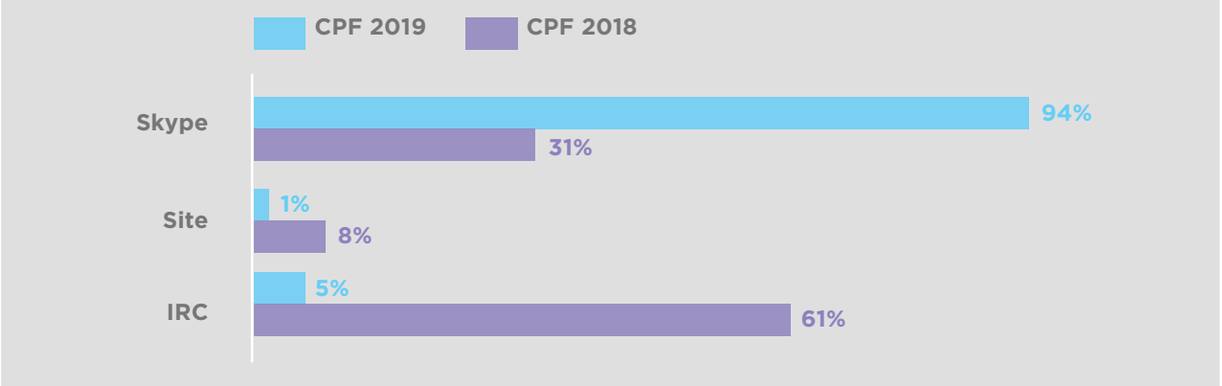

A análise também identificou quais os canais que mais tiveram vazamentos para cartões de crédito, destacando 81% para canais IRC, seguido de 11% para sites de compartilhamento.

## CANAIS COM MAIOR NÚMERO DE VAZAMENTOS




Comparando o cenário anterior e vislumbrando nitidamente a mudança de canal de atuação, principalmente o avanço dos vazamentos, a análise de 2018 tem como destaque os dados de CPF.

## QUANTIDADE DE DADOS VAZADOS POR CANAL



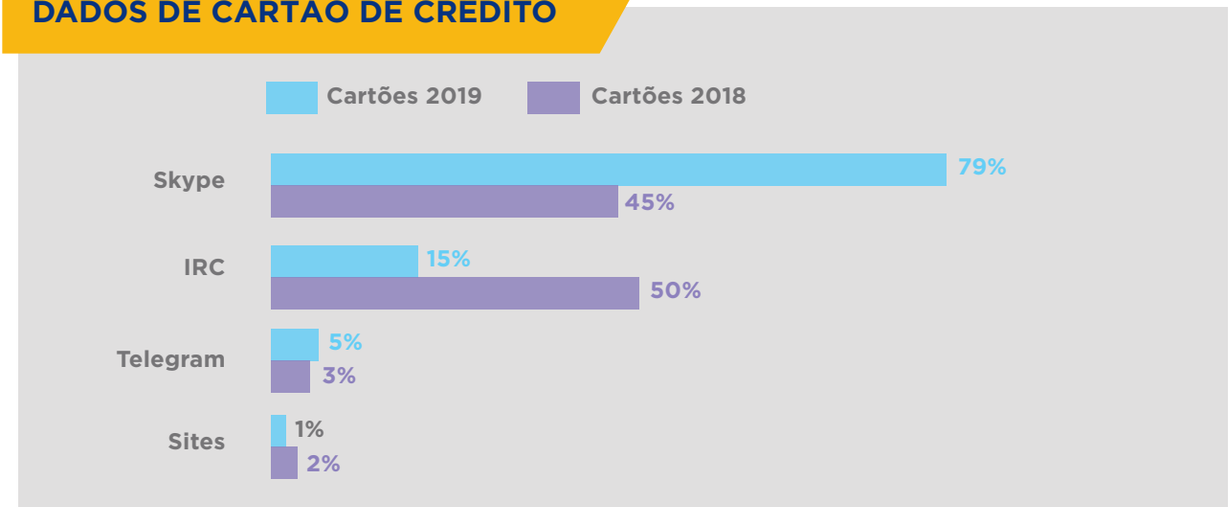

Dados de 2018, retirados da pesquisa de 2018 no período de junho de 2017 a 2018

Na pesquisa, é possível observar a mudança de cenário de "mercado", ficando evidente a migração da comercialização para IRC em 2019, como uma estratégia dos fraudadores por se tratar de um canal mais propício para comércios ilegais e ataques.

Com relação a dados de credenciais, temos, em 2019, 94% de dados vazados por Skype, enquanto que, em 2018, esse número era de apenas 31%.

No gráfico a seguir, que aborda especificamente dados sobre perda ou vazamento de cartões de crédito, temos, em 2018, em 1º lugar os canais IRC, com 50%. Já em 2019, o canal com maior número foi o Skype, com 79%.

## DADOS DE CARTÃO DE CRÉDITO




Há uma crença no mercado de que os cibercriminosos buscam apenas os dados pessoais dos clientes, o que não afetaria o negócio. Porém, o vazamento de dados pode causar danos tecnológicos e financeiros nas operações de uma organização, afetar a sua imagem e, ainda, consumir lentamente a sua reputação, bem como as estruturas organizacionais e administrativas. Além disso, a LGPD, lei que entrará em vigor no Brasil em agosto de 2020, responsabiliza tanto controladores, quanto operadores.

• Controlador: pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais.
• Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Além das questões legais, as organizações devem buscar constantemente melhorias tecnológicas e processuais e a contratação de serviços especializados de empresas de segurança, que permitam concentrar os esforços no core business e também que mantenham a credibilidade no mercado e tornem suas operações mais seguras. As ações preventivas e os serviços de contrainteligência cibernética fornecem melhorias contínuas para evitar ataques.

Fonte: LGPD, art. 5º.

# PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

**PARA ENTENDER COM PROFUNDIDADE A REALIDADE DO CENÁRIO NACIONAL DE SEGURANÇA DA INFORMAÇÃO, O GRUPO DARYUSS REALIZOU UMA PESQUISA EM AGOSTO DE 2018.**

## PÚBLICO PARTICIPANTE: 176 PESSOAS

- 80% envolvidos nas tomadas de decisão.
- 67% pós-graduados.
- 54% em posições de direção e gerência.
- 33% certificados em Segurança da Informação.

## SOBRE AS EMPRESAS PARTICIPANTES:

- 23% da área de tecnologia.
- 49% acima de 1.000 colaboradores.
- 27% das empresas com faturamento superior a R$ 300 MM/ano.
- 70% possuem Gestão de Segurança da Informação (SI).
- 60% possuem, no máximo, 5 colaboradores de SI.

Com o intuito de demonstrar as mudanças e os avanços da segurança da informação nas corporações, a pesquisa de 2018 foi comparada com a realizada em 2014.

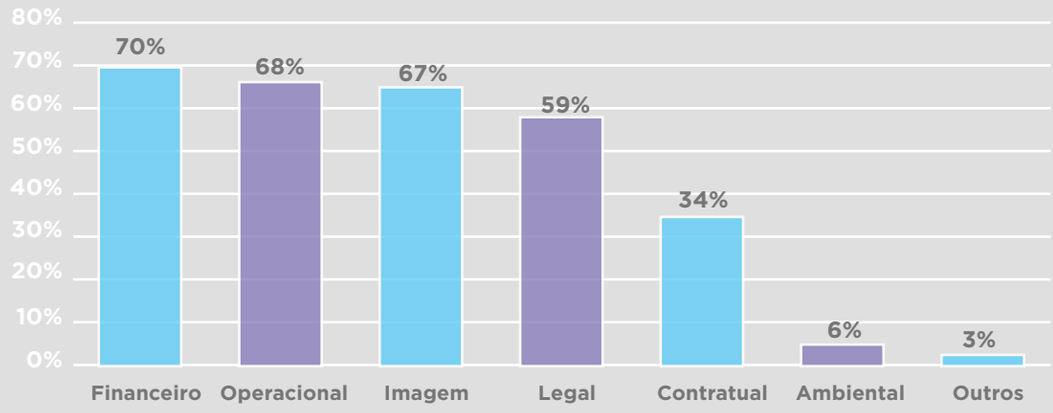
- Em 2018, 66% das empresas informaram possuir Política de Segurança da Informação implementada, indicando aumento na comparação com 2014, quando eram 44,75%.
- Em 2018, 44% das empresas afirmaram ter Comitê de SI.

Analisando especificamente as questões gerenciais, a pesquisa revelou que:

- 14% das empresas ainda não investem em SI.
- 40% dos respondentes desconhecem o % investido por suas empresas em SI.
- 50% dos respondentes não possuem nenhuma certificação internacional.
- Em 50% das empresas, a responsabilidade de SI é da TI.

Em linha com as considerações prévias deste relatório, a Pesquisa Nacional de Segurança da Informação apontou que os impactos mais preocupantes estão concentrados nos riscos financeiro, operacional e de imagem.

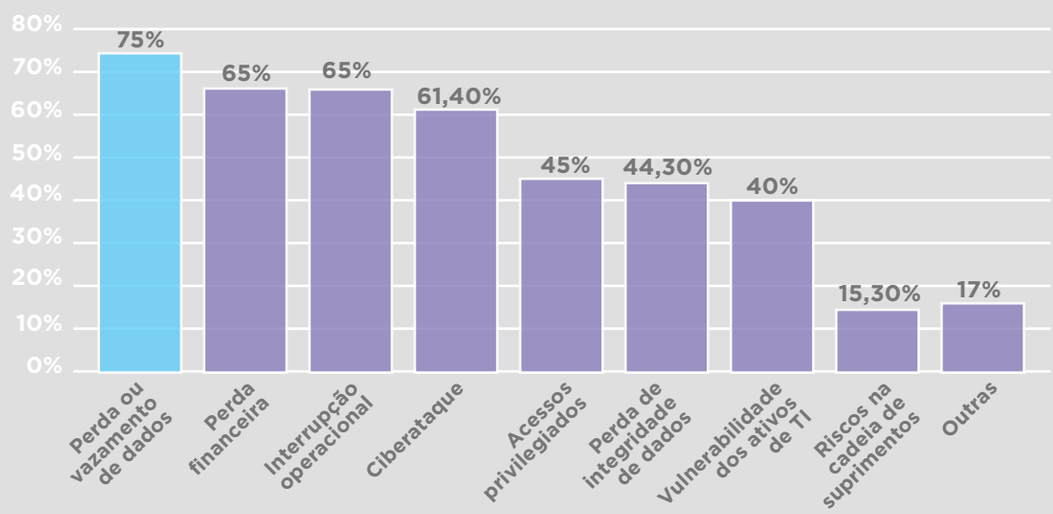
## IMPACTOS MAIS PREOCUPANTES




Fonte: DARYUS. Pesquisa Nacional de Segurança da Informação 2018.

Já no caso das preocupações com incidentes, o item perda ou vazamento de dados ocupa o topo da lista para 75% dos respondentes. Na sequência, a perda financeira e a interrupção operacional dividem o 2° lugar (65%) e os ciberataques aparecem em 3° lugar (61,40%).

## PRINCIPAIS PREOCUPAÇÕES FRENTE A INCIDENTES

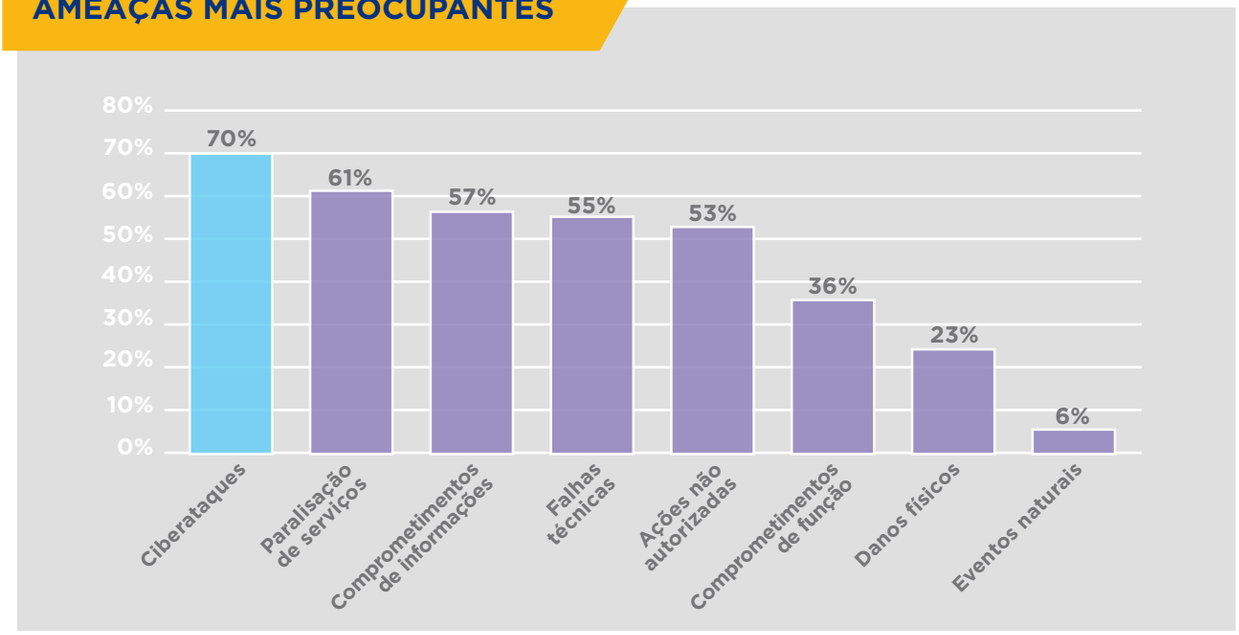



Fonte: Grupo DARYUS. Pesquisa Nacional de Segurança da Informação 2018.
Fonte: 2018 Cost of a Data Breach Study.

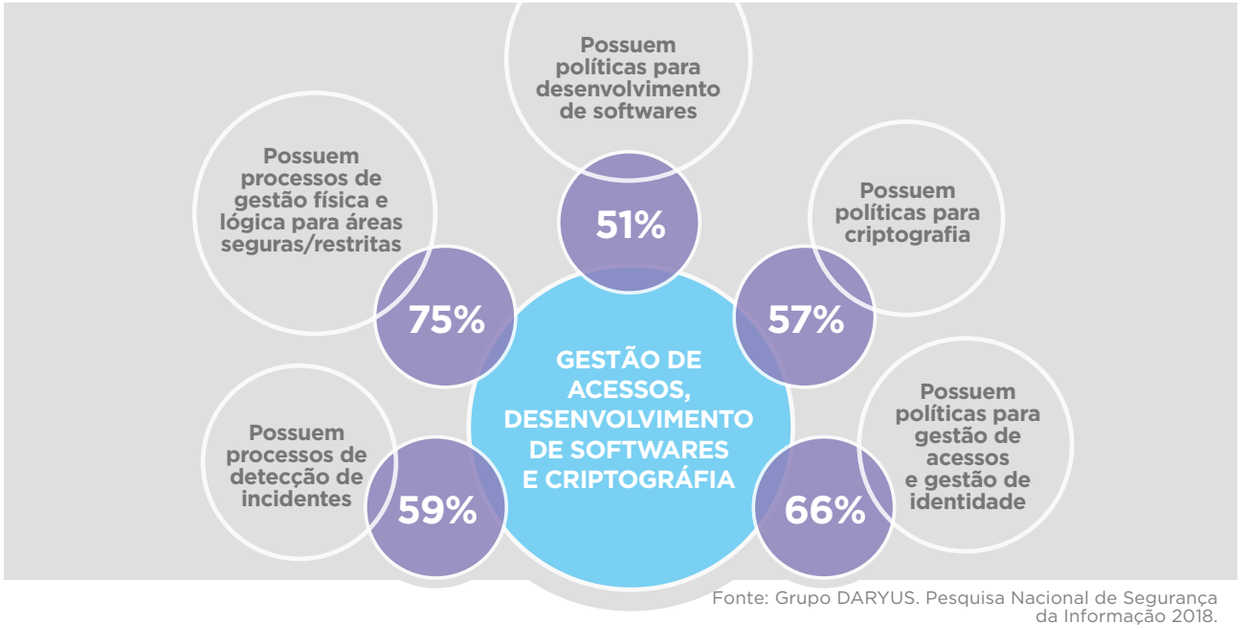
A Pesquisa Nacional de Segurança da Informação ainda traz dados de estudos complementares para expandir a análise. Segundo o Ponemon Institute, o custo médio de violação de dados no Brasil é de R$ 1,24 milhão para empresas. Além disso, o país é o mais propenso a sofrer violações de segurança, com um risco de 43% de uma empresa sofrer um ataque cibernético.

No tocante às ameaças, a pesquisa revelou que os ciberataques estão no topo das preocupações das empresas.

## AMEAÇAS MAIS PREOCUPANTES



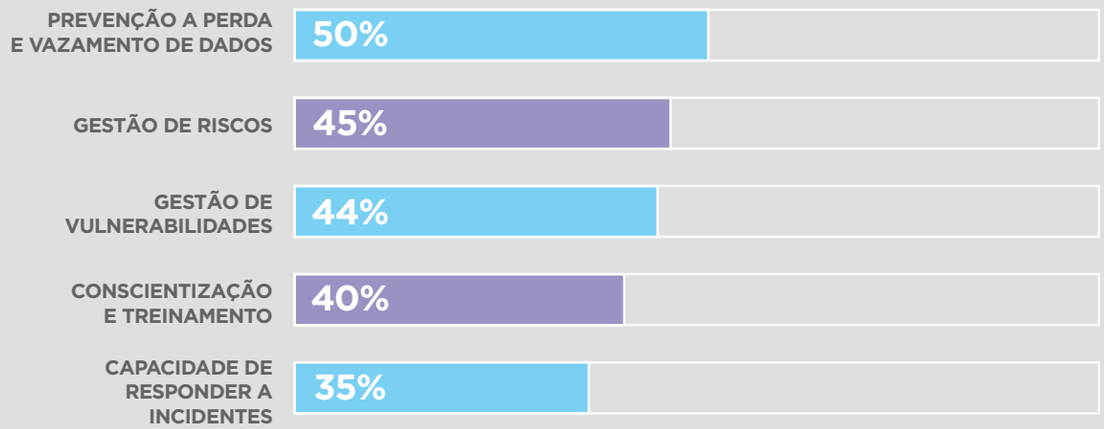

Fonte: Grupo DARYUS. Pesquisa Nacional de Segurança da Informação 2018.




Fonte: Grupo DARYUS. Pesquisa Nacional de Segurança da Informação 2018.

Assim como este **4º Relatório Anual de Riscos e Fraudes no Cenário Cibernético**, a Pesquisa Nacional de Segurança da Informação também visava entender o passado, o presente e o futuro e, para isso, questionou os entrevistados sobre quais seriam as prioridades para os próximos 12 meses.

**PRIORIDADES PARA OS PRÓXIMOS 12 MESES**




Fonte: Grupo DARYUS. Pesquisa Nacional de Segurança da Informação 2018

## VIOLAÇÃO DE DADOS: O DANO INVISÍVEL

É público o quanto uma empresa pode perder com violação de dados pessoais e corporativos, visto o exemplo de um dos maiores bureaux de crédito americano que teve, em março de 2018, um enorme prejuízo. Outras empresas dos segmentos financeiro, de entretenimento e de tecnologia também tiveram ações em queda brusca após terem seus nomes envolvidos com vazamentos. Entretanto, há danos incalculáveis e invisíveis por longos períodos decorrentes de vulnerabilidades não tratadas, que podem se tornar um incidente.

É de conhecimento geral que o prejuízo com uma violação de dados vai além das perdas financeiras, envolvendo comprometimento da reputação, ações civis e até sanções mínimas. Diversas pesquisas citam que empresas perdem cerca de 1 milhão de dólares desde 2017 com roubos de dados e danos oriundos de vazamentos. A falha de correção pode

tornar a empresa menos competitiva e com imagem fragilizada no mundo dos negócios. No relatório de 2018, foi abordado o dilema da comunicação de uma violação. Para este ano e para 2020, a questão foi ampliada para a esfera legal. As empresas que optavam por manter o caso em sigilo por questões de credibilidade e de imagem da marca precisarão cumprir a Lei Geral de Proteção de Dados, que determina:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Logo, é importante que a empresa reflita sobre as consequências na imagem da marca, porém, o mais importante é construir um ambiente estrategicamente seguro, que proteja as informações dos negócios e dos titulares envolvidos nas operações.

**VIOLAÇÃO DE DADOS: O VAZAMENTO DE DADOS E/OU O ACESSO NÃO AUTORIZADO PODEM SER ARMAS QUASE LETAIS. EM CONTRAPARTIDA, SE A EMPRESA APLICA RECURSOS E REALIZA AÇÕES DE FORMA PREVENTIVA, A SEGURANÇA ATUA COMO UMA ESPINHA DORSAL, VIABILIZANDO QUE TODA A CONSTRUÇÃO SEJA FORTALECIDA. ALÉM DISSO, A COMPLEXIDADE DE MENSURAÇÃO DE DANOS À IMAGEM COLABORA PARA O ENTENDIMENTO DE QUE É SEMPRE MENOS ONEROSO INVESTIR EM MECANISMOS E METODOLOGIAS DE PREVENÇÃO E SEGURANÇA DO QUE FICAR À MERCÊ DOS PREJUÍZOS E POTENCIAIS CONSEQUÊNCIAS DE UMA VIOLAÇÃO DE DADOS.**

# LGPD E VIOLAÇÃO DE DADOS

## POR JEFERSON D'ADDARIO, CEO DO GRUPO DARYUS

Uma das perguntas da Pesquisa Nacional de Segurança da Informação (mencionada neste relatório) foi se as empresas estavam preparadas para a Lei Geral de Proteção de Dados (LGPD). 15% afirmaram que sim, 40% declararam que não e 44% informaram estar em desenvolvimento. Na época da coleta das respostas (14 a 27 de agosto de 2018), a lei estava recém-sancionada. Porém, o contexto temporal não é plausível para justificar que apenas 15% das empresas estivessem preparadas. Antes da sanção e da publicação da LGPD, em agosto de 2018, o tema já havia sido discutido por 2 anos no Congresso e por mais de uma década na comunidade.

Provavelmente, você sabe que estou correto em afirmar que a lei é importantíssima, mas que não traz efetivamente tantas novidades. Certificações e ISO's já abordavam a segurança das informações e as questões de privacidade. A regulação, que entrará em vigor em agosto de 2020, define diversas obrigatoriedades, mas muitas delas já eram recomendações previstas nas ISO 27001 e ISO 29100, por exemplo.

Além disso, o cenário internacional também corroborava com o entendimento de que a SI vivia transformações importantes e que as organizações que ainda não haviam dado a devida importância à área precisavam expandir a visão tecnológica, de riscos e de segurança da informação. Acima de tudo, a atmosfera já inspirava ação. Meses antes da coleta das respostas da Pesquisa Nacional de Segurança da Informação, o GDPR havia entrado em plena eficácia (25/05/2018). Mesmo sendo uma legislação da União Europeia, as obrigatoriedades da lei eram - e continuam sendo - extraterritoriais. Ou seja, aplicáveis às empresas fora da União Europeia, se estas oferecerem serviços para os países da UE e/ou tratarem dados de europeus, respeitando os eventuais casos de exceção.

Entrando nos pormenores da LGPD, as violações de dados pessoais e incidentes cibernéticos estão, em sua grande titularidade, diretamente ligados. Aliás, os episódios públicos de violações e comprometimentos da segurança de dados de usuários e clientes de diversas empresas mundo afora foram um dos motivos para pressionar as legislações, tanto no Brasil, quanto na Europa. Para demonstrar a relação da LGPD com as violações, listamos alguns pontos da lei diretamente conectados à questão:

• A comunicação de ocorrência de incidente de segurança deverá ser feita em prazo razoável, conforme definido pela autoridade nacional.
• É preciso comunicar à ANPD (Autoridade Nacional de Proteção de Dados) a natureza dos dados pessoais afetados; informações dos titulares envolvidos; indicação das medidas utilizadas para a proteção dos dados; riscos relacionados ao incidente; motivos da demora, no caso de a comunicação não ter sido imediata; e medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Depois de tudo que este relatório trouxe até aqui, peço licença para refazer a pergunta da Pesquisa Nacional de Segurança da Informação a você. Sua empresa está preparada para a LGPD?

Dedicar-se ao conhecimento dos riscos e das fraudes no cenário cibernético é um começo promissor, mas me permita uma recomendação: é fundamental que você vá além da leitura deste relatório e que evolua a SI da sua organização com suporte especializado. Em pouco mais de um ano (agosto/2020), a LGPD entrará em plena eficácia e a ausência de processos azeitados e de uma Gestão de Segurança da Informação adequada farão com que as violações de dados sejam ainda mais comprometedoras para o negócio.■

## ENGENHARIA SOCIAL: O PRIMEIRO PASSO

A articulação usada no método de Engenharia Social é a mais eficaz para obter dados de alvos específicos, principalmente quando se trata da intenção de criar ataques direcionados. Aqui, não estamos falando de ataques comuns, como spam e phishing, mas sim de ataques estrategistas, como:

• Skimming: ataque direcionado para obter informações privadas sobre o cartão de crédito usado em uma transação normal. O cibercriminoso obtém dados dos cartões, recibos, fotocópias, entre outros por meio de dispositivos eletrônicos implantados em dispositivos bancários: ATM, POS e PIN PAD.
• Spear Phishing: o alvo é um número menor de pessoas, contudo, a elaboração é tão convincente que o usuário acredita que se trata de algo legítimo.

Diante de qualquer ataque, elaborado ou não, o uso de Engenharia Social é o pontapé para compreender todo o processo, sistemas e métodos das transações para permitir que os golpes tenham eficácia, além de precisar qual ponto seria o alvo, isso é, onde há maior chance de ganho.

Além de, obviamente, incentivar que medidas prévias sejam tomadas com o intuito de evitar incidentes, a lei também determina como devem ser tratadas as violações de dados. É importante frisar que as decisões de ocultar os episódios serão passíveis de sanções, como advertência, multa simples e multa diária.


**APESAR DE A LEI BRASILEIRA AINDA NÃO ESPECIFICAR O PRAZO PARA COMUNICAÇÃO, AS 72H DEFINIDAS PELO GDPR SERVEM COMO REFERÊNCIA PARA A NECESSIDADE DE AGILIDADE NESSES PROCESSOS.**

# MALWARE: TENDÊNCIA EM CONSOLIDAÇÃO

POR THIAGO BORDINI, DIRETOR DE INTELIGÊNCIA CIBERNÉTICA DA NS PREVENTION.

A cada dia, presenciamos mais e mais notícias sobre malwares, ransomwares, entre outros. Na maior parte dos casos, são ataques genéricos, entretanto, no último ano, presenciamos uma mudança significativa nos ataques de malwares direcionados a aplicações específicas, literalmente feitos sob medida.

Participamos de algumas investigações nas quais foi perceptível que o atacante estudou toda a aplicação do alvo de modo a realizar uma engenharia reversa com o intuito de entender a manipulação de parâmetros, variáveis, entrypoint, dentre outras características, criando, assim, um artefato malicioso específico para esta aplicação, o que torna o ataque mais efetivo e silencioso para as ferramentas de defesa.

Enganam-se os que pensam que estamos falando de grupos estrangeiros; em todos os casos analisados, os artefatos haviam sido desenvolvidos por brasileiros. Outro ponto interessante das análises foi a crescente utilização de domínios dinâmicos usados pelos artefatos na exfiltração dos dados, bem como no estabelecimento do comando e do controle, o que dificulta o processo investigativo e de resposta ao incidente.

Percebemos, durante o nosso monitoramento um aumento significativo de novos malwares, os " criadores" desses artefatos estão criando malwares mais direcionados. A oferta de serviço no ambiente cibernético é grande, o que nos leva a crer que a demanda pela contratação desse tipo de serviço também esteja em alta tornando se um forma de monetização para cibercriminosos, que consequentemente atingirá as empresas alvos desses malwares.

Não é difícil entender os motivos da migração, uma vez que a indústria de soluções de defesa tem aperfeiçoado os processos de identificação e de mitigação desses ataques. Por exemplo, uma das formas que adotamos junto aos nossos clientes é a utilização de técnicas de inteligência e de contrainteligência cibernética para mapear os indicadores de comprometimento de forma efetiva, eliminando não o artefato identificado, mas sim o modus operandi por completo. ■

## MALWARE E ATMS

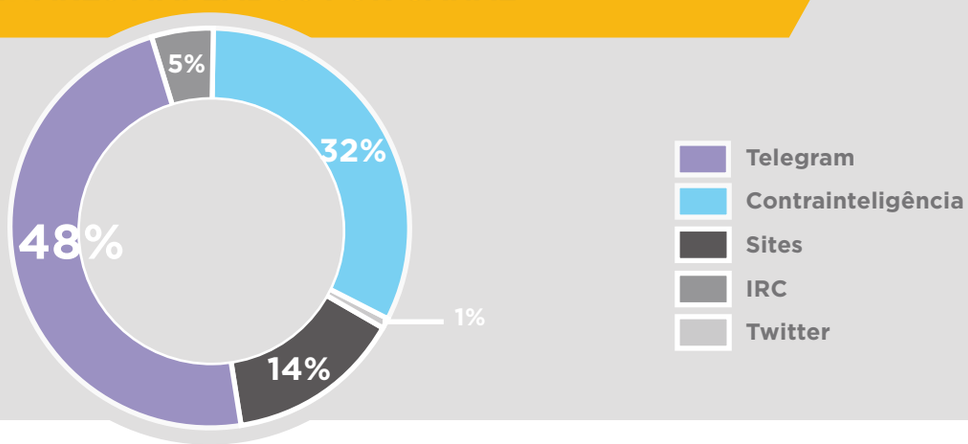
Malwares que atacam ATMs são abertamente comercializados nos mercados da Darknet, onde também é possível encontrar instruções detalhadas de uso.

Os malwares são os melhores hospedeiros para ataques como skimming, SSL-Strip e outros métodos atrelados, que ocasionam grandes danos e cuja rastreabilidade é quase nula. Notadamente, o problema de riscos cibernéticos e segurança da informação está em constante crescimento, o que requer orçamentos mais robustos para as áreas. As organizações possuem capacidades limitadas de monitoramento de segurança cibernética e inteligência de ameaças, áreas fundamentais no cenário de digitalização dos negócios e de ameaças emergentes.

Nossos serviços de inteligência cibernética mapeou 2093 malwares, onde destacarmos como os canais mais usados como distribuição ou repositório:

- **Grupos de Telegram: 48%**
- **Serviços de contrainteligência: 32%**
- **Sites de compartilhamento: 14%**

**MALWARES MAPEADOS POR CANAL**




**O PRINCIPAL OBJETIVO DO MALWARE PARA ATM É CONECTAR E CONTROLAR DISPOSITIVOS PERIFÉRICOS DENTRO DO CAIXA ELETRÔNICO A FIM DE RETIRAR O DINHEIRO ARMAZENADO E/OU DE COLETAR INFORMAÇÕES DOS CLIENTES DO BANCO.**

## RISCOS E FRAUDES NO CENÁRIO CIBERNÉTICO

Como demonstrado neste relatório, o cenário de riscos e fraudes avança em complexidade de forma exponencial, demandando Gestão de Segurança da Informação e Gestão de Riscos atentas às necessidades do negócio da organização, atuação do board e investimentos orientados para a criação de medidas preventivas e corretivas, de fato, robustas.

No curto horizonte, 2019 e 2020, o período de preparação (vacatio legis) e a previsão de entrada em vigor da Lei Geral de Proteção de Dados são importantes destaques. As exigências legais demandam dedicação das áreas de TI, Riscos, Compliance, entre outras, assim como oportunizam melhorias e fomentam avanços, que podem contribuir imensamente para a maturidade das empresas que, efetivamente, assimilarem a relevância de observação e entendimento do cenário cibernético, de todos os personagens envolvidos e dos impactos corporativos. Logo, uma postura ativa, dinâmica e consciente é de suma importância para todos os negócios com implicações tecnológicas, independentemente do nível de profundidade.

GRUPO NEW SPACE®
A Visão do Futuro

## SOBRE A NS PREVENTION

A **NS Prevention** é a vertical de soluções de prevenção a fraudes com uso de inteligência e contrainteligência cibernética do Grupo New Space, um dos líderes em serviços de tecnologia para o setor financeiro no Brasil.

Em 2017, a **NS Prevention** recebeu o selo de empresa estratégica de defesa e o nosso serviço de inteligência cibernética foi catalogado como Produto Estratégico de Defesa, ambos concedidos pelo Ministério da Defesa a um grupo seleto e homologado de empresas nacionais, garantindo uma segurança a mais para os nossos clientes e parceiros no que tange a qualidade e a seriedade de nossos serviços. Com mais de 30 anos de mercado, atuamos na gestão de serviços de crédito, RH, cartões e retaguarda bancária.

A **NS Prevention p**ossui um centro de competência operacional para meios de pagamento, desenvolve soluções e consultoria em alta e baixa plataformas e dispõe de equipes especializadas em inteligência cibernética, prevenção a fraudes e análise de riscos. O Grupo **New Space**também oferece serviços de custódia e armazenagem de mídias, documentos, código-fonte e destruição segura de informações confidenciais.

DARYUS

## SOBRE O GRUPO DARYUS

Fundado em 2005, o Grupo DARYUS atua nas áreas de consultoria, educação e tecnologias para apoio à gestão empresarial, estratégica e de riscos. O núcleo DARYUS Consultoria dedicase às frentes de Continuidade de Negócios, Governança e Gestão de TIC, Segurança da Informação e Gestão de Processos e Qualidade. Além disso, o grupo é idealizador dos eventos GRC International, Driday Latin America e GRM – Global Risk Meeting.

As informações, pesquisas e análises apresentadas
no **4º Relatório Anual de Riscos e Fraudes**
no Cenário Cibernético foram obtidas por meio
dos serviços realizados pela **NS Prevention**,
do Grupo **New Space**, e pelo Grupo **DARYUS**,
além de dados colhidos na imprensa e em pesquisas
de institutos reconhecidos, conforme indicações
ao longo do documento.


GRUPO
NEW SPACE
A Visão do Futuro
DARYUS