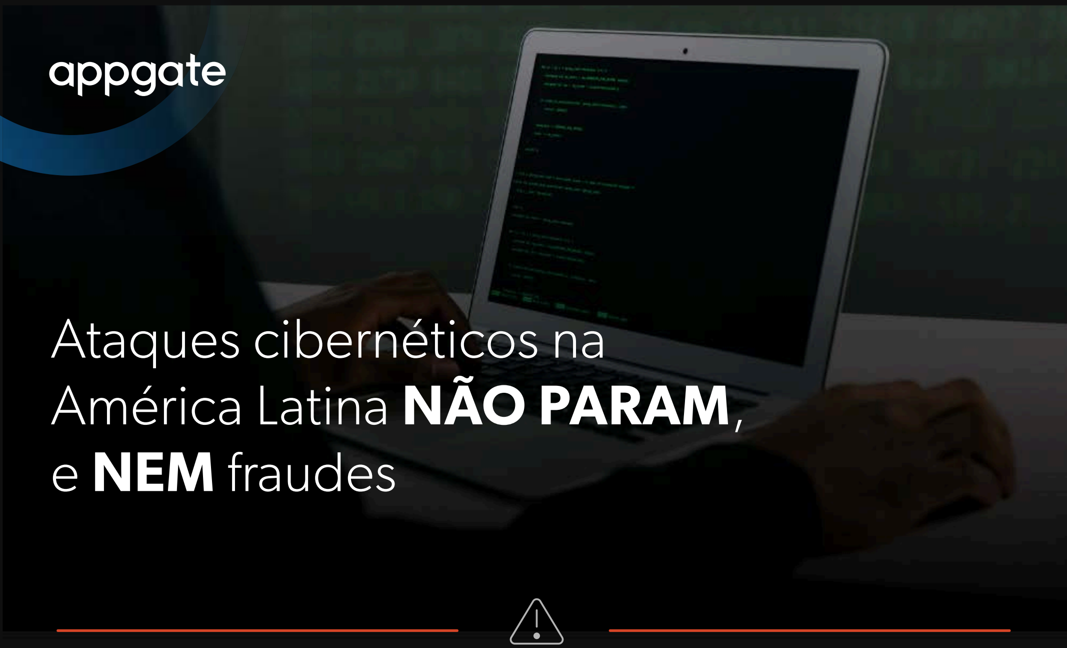


Ataques cibernéticos na América Latina **NÃO PARAM**, e **NEM** fraudes

O crime está sempre em busca de novas vítimas para atacar

com técnicas tradicionais que provaram funcionar muito bem, explorando ou desenvolvendo novos mecanismos para executar e massificar seus ataques.

Agora é a hora de pensar e entender **como esses desafios de segurança cibernética e fraude se moldam no próximo ano.**

ATAQUES DE ENGENHARIA

Continuam a se posicionar como um dos mecanismos mais eficazes, massificáveis e lucrativos quando se trata de monetizá-los.

Não é o único mecanismo, mas ***"o rei dos reis é o phishing".***

É assim que **Carlos Rubio**, Líder de Engenharia de Pré-vendas da Appgate, descreve.

As diferentes variantes que estão sendo exploradas para massificar e ter mais alcance ao seu objetivo, no caso da América Latina, temos um crescimento exponencial de ataques:

Smishing

Phishing por mensagens de texto SMS

QRishing

Phishing através de códigos QR

Vishing

Phishing por voz, ou phishing através de chamadas telefônicas

Explorando Assim A **Corrida Digital Que Diferentes Indústrias Da Região Vêm Desenvolvendo.**

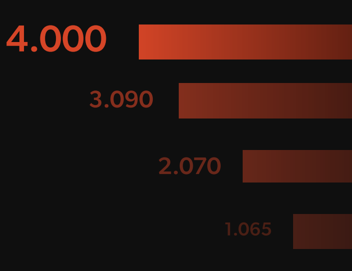
Os ataques de engenharia social tornaram-se o **vetor de origem** dos principais incidentes de segurança cibernética e fraude que ocorreram na região **durante 2022.**

Nesse período, a **equipe do SOC da Appgate** apresentou um aumento na detecção e desmontagem de ***4290%*** dos sites de phishing na América Latina, em comparação com o ano anterior, principalmente aqueles que utilizam plataformas gratuitas.

RANSOMWARE

As credenciais comprometidas dos usuários de uma organização implicam em um risco de acesso aos seus recursos críticos, o que levou a um crescimento acelerado dos ataques de ransomware:

Durante 2022 encontramos uma média de ataques por dia na região (Kaspersky).



Os cibercriminosos criaram uma indústria organizada que **cria perfis, projeta e lança ataques direcionados.**

O CONTI, uma variante de ransomware operando como Ransomware as a Service (RaaS)

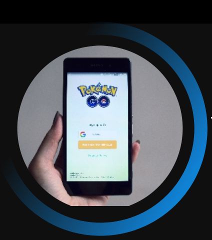
É um exemplo claro do impacto que esse tipo de ataque trouxe para a América Latina. **O alvo dos atacantes se espalhou para diferentes verticais da indústria com grande sucesso**

- Governo
- Saúde
- Educação
- Serviços Financeiros

Cada violação ou intrusão gera exfiltração de informações sensíveis que podem ser facilmente encontradas para venda ou, em alguns casos, gratuitamente na :

Dark Web

Fóruns Especializados Em Crimes Cibernéticos



Em muitos casos escondidos em fóruns de tecnologia, jogos on-line, entre outras atividades legais

Plataformas de Mensagens

sendo esta última para a **América Latina a principal fonte de mercado de credenciais.**

OUTROS TIPOS DE FRAUDE

A materialização desses ataques está gerando um forte impacto sobre os consumidores de diferentes setores econômicos e com isso **vemos um crescimento da fraude através do:**

Roubo de Identidade

Registro em serviços e produtos digitais

Identidades Sintéticas

Aquisição de produtos de crédito

Contas Mule

Destinatários de fundos de fraude

Fraude em um Ambiente Não Presente

Com cartões de crédito e débito

Durante o ano de 2022, a Appgate detectou um crescimento das transações anómalas de mais de 150%, sendo as transferências de fundos (interbancárias e locais), os pagamentos de serviços e a abertura de produtos digitais o maior risco, sem deixar de lado o crescimento do roubo de identidade através de carteiras digitais associadas à administração de moedas virtuais.

Aplicativos móveis

É provável que os aplicativos móveis continuem a ser um bom negócio para os criminosos, especialmente quando os usuários continuarem a baixar e usar aplicativos móveis obtidos de lojas de aplicativos desonestos ou baixá-los de links na Internet.

AS MAIORES FRAQUEZAS DAS EMPRESAS

Manuel Giraldo
Gerente Sênior De Serviços De Prevenção De Fraudes Da Appgate,
destaca que os criminosos hoje exploram diferentes fraquezas na gestão de fraudes para iniciar sua orquestração.

1 **Falta de visibilidade das organizações frente aos riscos digitais,** que possam apresentar, perdendo a proatividade na gestão de ataques de phishing, personificação de marca e até mesmo a publicação de aplicações maliciosas em sites não oficiais, comprometendo a segurança da organização e de seus usuários.

2 **A maturidade dos processos de autenticação (Fluxos e esquemas)** na região permanece baixa, verificamos que ainda há uma falta de sincronia entre os processos de autenticação em canais digitais e outros canais de distribuição, em muitos casos esses canais de distribuição tornam-se a entrada do atacante.

3 **A análise de risco transacional é tendenciosa e não tem uma visão 360° do cliente.**

NOVOS DESAFIOS

INTELIGÊNCIA ARTIFICIAL

As novas tendências da Inteligência Artificial abriram as portas para ferramentas de código generativo, como o **Copilot** do Github ou o **ChatGPT** da OpenAI.

Estes são uma faca de dois gumes, pois podem melhorar a velocidade e a eficiência dos projetos, mas usá-los sem considerar potenciais riscos de segurança **pode introduzir sérias vulnerabilidades ao código,** bem como trazer problemas de propriedade intelectual

Camilo Gómez
vice-presidente de engenharia da Appgate.

"Usar IA (Inteligência Artificial) para gerar código é como convidar um estranho para a equipe de desenvolvimento, é importante entender seus limites e riscos, especialmente nos estágios iniciais dessas ferramentas"

SEGURANÇA NA NUVEM

Não podemos deixar de lado os desafios de segurança na nuvem, onde a operacionalidade, as ferramentas obsoletas, a expansão da superfície de ataque, as vulnerabilidades do DevOps e a pouca visibilidade com **controles limitados tornam as implantações na nuvem um desafio diante da construção de uma verdadeira postura de segurança.**

Nesse sentido, Appgate recomenda trabalhar no desafio de proteger conexões **para, de e entre** usuários e cargas de trabalho sob o **modelo Zero Trust.**

MALWARE COMO SERVIÇO (MAAS)

Atualmente, **há um grande número de plataformas de malware como serviço** que permitem que até mesmo invasores não qualificados lancem rapidamente suas próprias campanhas a preços muito acessíveis.

Devido ao aumento na adoção e criação desses serviços este ano, essas plataformas aumentarão suas capacidades e provavelmente farão parcerias com outros tipos de empresas de "cibercrime como serviço".

Esse cenário é perfeito para agentes de ameaças mais perigosos, como grupos de ransomware, que poderiam facilmente comprar seu acesso inicial a dispositivos comprometidos e realizar ataques maiores.

Marcela Nestler
Gerente de negócios da immune (parte da appgate).

"Se houver uma recessão, as empresas provavelmente reduzirão seus orçamentos de segurança cibernética e manutenção, e isso pode levar a mais vulnerabilidades e exposição"