O retorno do investimento da perspetiva do Ciber-Atacante

Por Rui Shantilal da INTEGRITY

O entendimento adequado da evolução do Cibercrime requer uma reflexão estratégica essencial para que se possa endereçar o tema de forma apropriada.

Atualmente a cibersegurança está tendencialmente na agenda dos gestores de praticamente todas as organizações, onde se procura de forma consistente avaliar as ameaças e definir estratégias de mitigação assentes em modelos de análise de risco, levando naturalmente em consideração o custo/benefício desses investimentos.

E quanto aos atacantes? Estes também terão uma abordagem de retorno de investimento à sua atividade? Quais são as variáveis a considerar, e mais importante: que lições devemos tirar desta análise?

Estarão as últimas tendências de crescimento e diversificação do cibercrime associadas a esta análise de retorno de investimento dos ciber-atacantes?

O que podemos esperar do futuro e quais as ações que devemos tomar?

Como pensa o atacante Variáveis a serem consideradas

Tal como acontece numa empresa, os atacantes também utilizam um modelo de custo/benefício e procuram obter o maior benefício possível dos seus investimentos.

Atuando maioritariamente em grupos organizados, estas são essencialmente as variáveis levadas em consideração pelos Cibercriminosos:

Receita líquida **–** É o resultado de quanto (ou o que) o atacante vai obter como resultado das suas ações. Esta variável calcula a projeção de potencial retorno considerando o cenário e alvo. Este valor terá que levar em consideração os custos de monetização da receita, que tipicamente envolve custos de branqueamento dos capitais obtidos de forma irregular.

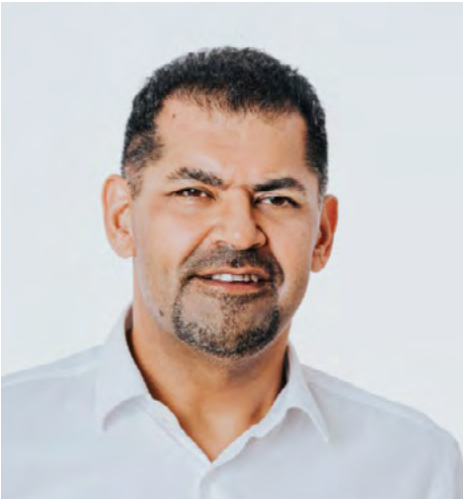
Investimento **–** O investimento do atacante é essencialmente os recursos humanos com expertise e os meios tecnológicos necessários para levar a cabo um ataque de forma bem-sucedida.

Outra dimensão a considerar é o ***risco***. Não só o risco de poderem ser apanhados, mas o risco de que, apesar de investirem tempo e recursos, o ataque não ser bem-sucedido. Nesse contexto os atacantes levam em consideração a probabilidade de sucesso e o risco que correm de serem apanhados.

Depois de avaliar o ROI potencial e os fatores de risco, o atacante decidirá se vale a pena seguir em frente. Estes vão evitar situações como investir recursos e não ter sucesso, assim como, em qualquer outro modelo de negócio.

A evolução da maturidade da cibersegurança

A segurança cibernética já não é um tópico novo. Pelo menos, desde o início do milénio, as grandes empresas e entidades e mais especificamente o setor financeiro têm se concentrado sobre este tema.



Após 20 anos, espera-se que a sua maturidade tenha evoluído consideravelmente e atualmente não são amadores os que conseguem atacar com sucesso tais organizações.

Nos últimos anos, estas empresas criaram departamentos dedicados especificamente, com pessoas formadas, em Cibersegurança. Atualmente, estas organizações têm uma série de políticas, procedimentos, tecnologia e equipas que lhes permitem prevenir, detetar e responder apropriadamente a ameaças e incidentes. Muitos destas também executam um programa consistente de conscientização para os seus recursos humanos, com o objetivo de reduzir a tendência a ataques combinados de Engenharia Social.

As implicações para o cenário de ameaça

O crescimento da maturidade no setor da Cibersegurança também representou mudanças significativas para o cenário de ameaça, principalmente porque as oportunidades de sucesso num ataque contra empresas robustas ou entidade financeiras ficaram consideravelmente reduzidas, resultando numa projeção de ROI negativa para os atacantes.

Desta forma, os atacantes também estão a mudar o seu comportamento, a saber:

Diversificação de Target:

Sempre que alguém disser: "Mas nós não somos um banco !!" recorde-lhes que os invasores também estão conscientes desse facto e como tal sabem que, outras entidades não possuem o mesmo nível de controlo que um banco possui, facilitando-lhes assim a sua intrusão. Apesar de o lucro ser potencialmente inferior, estes diversificam pelos setores porque sabem que o investimento em cibersegurança é menor e que a probabilidade de sucesso é maior e isso resulta num ROI melhor. Hoje, vemos setores sob ataque, que não eram o principal alvo dos atacantes, como saúde, educação, retalho, indústria, hotéis, PMEs e até mesmo utilizadores finais, todos sob ataque utilizando abordagens de ameaças, como Card Skimming, Ransomware, Ceo Fraud, APT, Phishing, entre outros.

Ataques combinados e complexos:

os atacantes estão cientes de que obter quantias mais avultadas não é uma brincadeira de criança. Assim, sempre que estão dispostos a correr o risco para alcançar este tipo de alvo, naturalmente, também têm ataques mais sofisticados. Ataques combinados utilizando mais do que uma abordagem de ataque, como combinação de ameaça interna com hacking ou conluio são formas de ataques sofisticados que foram observados nestes tipos de alvo.

Que medidas tomar

A mentalidade de que não somos um alvo interessante já não é aplicável. Todos que utilizamos tecnologia somos um alvo interessante. E a ideia de que já estávamos prontos há 10 anos também está muito longe da realidade.

Quer seja ou não uma grande empresa ou entidade, com base neste cenário, todos os que utilizam tecnologia precisam de estar conscientes e preparados, porque os atacantes estão permanentemente à procura de novas e criativas formas de diversificar e lucrar.

É claro que um utilizador final ou uma PME não pode investir o mesmo

nível de recursos que uma grande empresa ou entidade, mas um esforço equilibrado e adequado deve ser considerado na sua estratégia de segurança da informação.

Regularmente, as organizações (e pessoas) devem:

- Estar conscientes e informados sobre as tendências de ataques cibernéticos.
- Avaliar os riscos e nível de exposição.
- Definir controlos apropriados (técnicos e processuais) para mitigar riscos quando adequados.
- Treinar as equipas, disseminar conhecimento e conscientização aos utilizadores.
- Definir planos de deteção e resposta adequados para minimizar o impacto no caso de um ataque bem-sucedido.
- Monitorizar e adaptar consistentemente, porque a Cibersegurança é dinâmica e a capacidade de observação e adaptação é um elemento chave neste puzzle.

Por fim, devemos estar cientes de que grandes oportunidades vêm sempre acompanhadas de grandes riscos. O incremento do cibercrime está para as tecnologias da informação, assim como a sinistralidade automóvel está para indústria automotiva. Os riscos são reais e dinâmicos, há que estar consciente e atuar sobre os mesmos para que se possa tirar o máximo partido das oportunidades, com o mínimo de risco possível. CW