HACK3R_
RANGERS

Os impactos financeiros do phishing

Embora seja uma fraude relativamente antiga, o phishing continua sendo uma das formas mais eficazes pelas quais os cibercriminosos entregam malwares e roubam dados sigilosos das empresas.

O que você provavelmente não sabe é que eles também são altamente lucrativos para os meliantes digitais — e, de forma proporcionalmente inversa, também trazem prejuízos financeiros preocupantes para companhias de todos os portes e segmentos comerciais.

De acordo com o The Ponemon 2021 Cost of Phishing Study, um estudo que analisou o impacto do phishing em centenas de corporações ao redor do mundo ao longo de 2021, o prejuízo médio causado por um ataque do tipo chegou na marca de incríveis US$ 14,8 milhões em empresas de grande porte — o triplo do valor registrado em 2015.

Entre as perdas, incluem-se o comprometimento de credenciais, a infecção por diversos tipos de malwares (incluindo ransomwares) e até a deterioração reputacional da marca após um vazamento de dados.

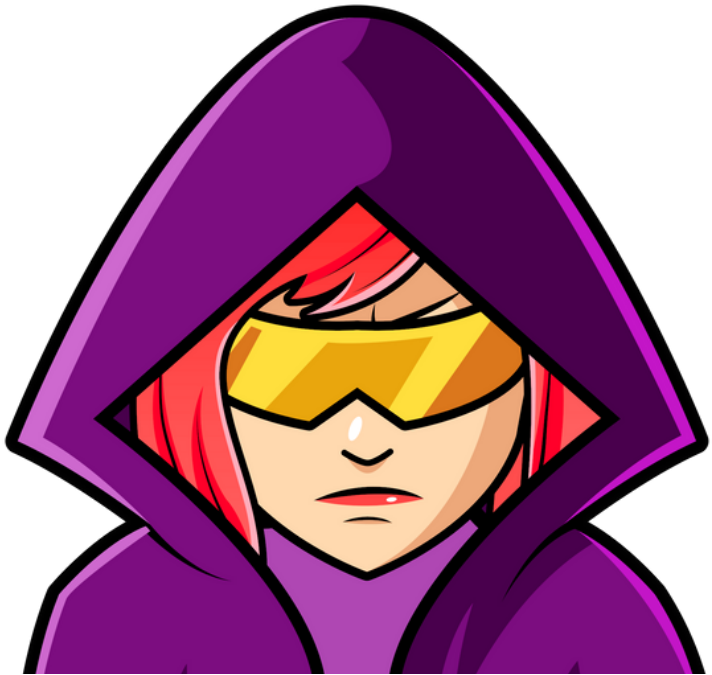
Dissecando os impactos

Uma das maiores causas dos prejuízos são as fraudes de Business Email Compromise (BEC), ataque no qual os criminosos cibernéticos personificam um executivo de alto escalão da companhia no intuito de extorquir outros colaboradores.

De acordo com o mais recente relatório do Internet Crime Complaint Center (IC3) do Departamento Federal de Investigação dos EUA (FBI), só em 2021, foram registrados 19.954 casos desse tipo de ataque. Juntos, eles somam um prejuízo de quase US$ 2,4 bilhões.

"O golpe acontece quando um cibercriminoso invade um e-mail corporativo legítimo por meio de engenharia social ou técnicas de invasão de computadores. Então, o fraudador incentiva os colaboradores a realizar transferências não autorizadas", explica o órgão federal. "Essas transferências fraudulentas geralmente são imediatamente direcionadas para carteiras de criptomoedas e rapidamente dispersas, tornando os esforços de recuperação mais difíceis."

O instituto Ponemon calcula que os ataques de BEC causaram danos de, em média, US$ 5,96 milhões para cada empresa, com um teto máximo de US$ 8,12 milhões.



HACK3R_
RANGER5

E os ransomwares?

Como citamos anteriormente, o phishing continua sendo uma das formas mais eficazes de entrega de malwares, e os ransomwares são, sem dúvida alguma, o tipo de software malicioso mais ameaçador do momento. Só no primeiro semestre de 2021, o pagamento médio de resgates subiu 82% em comparação com o ano anterior e 17,6% das infecções foram ocasionadas por cliques em e-mails fraudulentos.

De acordo com o relatório Unit 42 Ransomware Threat Report 2021, o maior valor de resgate pago por uma empresa em 2020 foi de US$ 10 milhões — o dobro do registrado em 2019, que foi de US$ 5 milhões. Vale observar, porém, que essas são as quantias efetivamente desembolsadas pelas empresas aos cibercriminosos. Se analisarmos os pedidos iniciais dos meliantes (que são sempre negociados), a maior demanda registrada foi de absurdos US$ 30 milhões.

Credenciais roubadas

Já os ataques de comprometimento de credenciais (que roubam logins através de páginas falsas) também são aplicados via phishing e causaram um prejuízo de US$ 2,1 milhões para as empresas em 2021. Estima-se que cada corporação gaste cerca de US$ 700 mil para remediar os danos de cada ataque desse gênero.

A solução: conscientização!

Por fim, não poderíamos deixar de falar sobre os vazamentos de dados, que são os incidentes mais caros e danosos que podem decorrer de um phishing bem-sucedido. De acordo com a mais nova edição do tradicional relatório da IBM, Cost of a Data Breach Report 2022, o phishing é o segundo maior vetor de vazamentos de dados, respondendo por 16% dos incidentes.

Após entrevistar 550 empresas, foi constatado que o custo de um vazamento de dados aumentou para US$ 4,35 milhões em 2022, um salto de 2,6% em comparação com 2020.

Felizmente, investir em programas de conscientização com foco no fator humano pode reduzir as despesas com phishing em aproximadamente 53%, de acordo com os participantes do estudo da Ponemon. Uma vez que o colaborador saiba identificar um e-mail malicioso e reportá-lo para a área de segurança, as chances de a empresa ser vítima desse tipo de ataque caem drasticamente.

No fim das contas, quando o assunto é phishing, o condicionamento do comportamento humano é mais valioso do que o investimento em soluções automatizadas.

HACK3R_ RANGER5

Bibliografia
What are the top 10 costs of phishing? (Hoxhunt, dezembro de 2021)
The Ponemon 2021 Cost of Phishing Study (Proofpoint, agosto de 2022)
2021 Internet Crime Report (FBI, março de 2022)
Cost of Data Breach 2022 (IBM, julho de 2022)