Resumo executivo

Hackers contra o sistema operacional humano

Raj Samani, CTO (EMEA)

Charles McFarland, engenheiro sênior de pesquisa do MTIS

intel Security

Muitos ciberataques envolvem um componente de engenharia social que tenta persuadir um indivíduo visado a realizar uma ação que cause uma infecção ou a divulgação de informações valiosas.

Embora o foco da correção do ataque seja de caráter técnico, o aspecto humano do ataque resulta na culpabilização do alvo e na demanda por mais conscientização quanto à segurança. Contudo, a verdade é que a maioria das organizações empenha-se pouco em compreender os motivos pelos quais o alvo foi explorado e, mais importante, o que fazer, além de promover maior conscientização, para reduzir o risco de mais ataques.

A expressão engenharia social pode ser definida como:

> *A aplicação deliberada de técnicas enganosas concebidas para induzir alguém a divulgar informações ou executar ações que possam resultar na liberação dessas informações.*

Durante um ataque de engenharia social, a vítima não tem discernimento de que suas ações são perigosas. O engenheiro social explora a ingenuidade do alvo, em vez de alguma propensão criminosa. Um ataque pode ser dividido em duas categorias:

- A caçada, que busca extrair informações utilizando o mínimo de interação com o alvo. Essa abordagem costuma envolver um único encontro. O atacante encerra a comunicação assim que a informação é obtida.
- O "farming" (cultivo), que busca estabelecer um relacionamento com o alvo e extrair informações deste ao longo de um período de tempo maior.

Os ataques de engenharia social que aproveitam o e-mail como canal de comunicação geralmente utilizam a caçada como principal forma de ataque. Existem exceções a essa regra, como as "fraudes nigerianas 419", que tentam prolongar a duração do ataque para poder extrair fundos adicionais. Os ataques de engenharia social dos tipos caçada e cultivo consistem, tipicamente, em quatro fases:

1. Pesquisa: essa fase opcional busca coletar informações sobre o alvo. O atacante busca informações que o ajudem a construir um "anzol" bem-sucedido, como os hobbies do alvo, seu local de trabalho ou fornecedor de serviços financeiros.
2. Anzol: o anzol tem como objetivo encenar um "enredo" bem-sucedido envolvendo o alvo e proporcionando um pretexto para interação. O psicólogo Robert Cialdini cita seis alavancas de influência que permitem tirar proveito do subconsciente do alvo:
   - Reciprocidade: as pessoas ganham alguma coisa, ficam agradecidas e sentem-se na obrigação de retribuir o favor.
   - Escassez: as pessoas tendem a obedecer quando acreditam que algo está em falta.
   - Consistência: uma vez que os alvos tenham prometido fazer algo, eles cumprem suas promessas por receio de parecerem pouco confiáveis.
   - Propensão: é mais provável que os alvos obedeçam quando o engenheiro social é alguém de quem eles gostam.
   - Autoridade: explora a tendência humana de obedecer quando a solicitação vem de alguma autoridade.
   - Validação social: a tendência de obedecer quando outras pessoas estão fazendo o mesmo.

3. Enredo: execução da parte principal do ataque. Esta pode envolver a divulgação de informações, um clique em um link, a transferência de fundos, etc.
4. Saída: a interação é encerrada. Embora talvez seja uma vantagem sair antes de despertar suspeitas de muitos ataques de cultivo, isso pode não ser necessário. Por exemplo, quando induzem os alvos a divulgar informações de cartões de pagamento, os atacantes geralmente não desejam levantar suspeitas que levem as vítimas a comunicar que seus cartões foram perdidos ou roubados e cancelá-los. Por outro lado, se os atacantes conseguirem roubar código-fonte ou outras informações pessoais, os alvos não poderão recuperar os dados roubados, mesmo que desconfiem de alguma coisa.

As tentativas de engenharia social não são necessariamente lineares. Um único ataque pode ser parte de uma campanha muito maior para coletar múltiplos fragmentos de informações relacionadas. Por exemplo, os atacantes podem realizar um ataque, obter informações e desaparecer. Alternativamente, eles podem realizar vários ataques de caçada e, com as informações coletadas, iniciar um ataque de cultivo.

Canais de ataque

Os engenheiros sociais podem utilizar vários caminhos em seus ataques.

- Sites: os ataques de engenharia social frequentemente aproveitam sites maliciosos como canal de ataque. Segundo o Relatório de investigações de violações de dados de 2014 da Verizon (2014 Verizon Data Breach Investigations Report), "20% dos ataques motivados por espionagem utilizam um site estratégico na Web para fornecer malware".
- E-mail: as formas mais comuns de engenharia social via e-mail são o "phishing" e o ainda mais direcionado "spear phishing". O e-mail é um método eficaz para os cibercriminosos porque "18% dos usuários visitam links em e-mails de phishing", segundo o relatório da Verizon.
- Telefone: este é um canal popular para os traficantes de informação.
- Cara a cara: um funcionário pode ser abordado e ludibriado ou coagido a fornecer informações.
- Correio: embora esse canal pareça menos predominante que os demais, ainda há relatos de ataques de engenharia social pelo correio.
- Fax: como exemplos podemos citar e-mails que se apresentam como mensagens de serviços de pagamento on-line.

Defesa contra engenharia social

Os controles seguintes podem ser utilizados para minimizar o risco da engenharia social. Eles se dividem em três categorias: pessoas, processos e tecnologia. Esses controles não abrangem todos os casos e podem não se aplicar a todas as organizações.

Pessoas

- Estabeleça limites claros: toda a equipe deve estar plenamente consciente das políticas relacionadas à divulgação de informações e ter caminhos de escalonamento claramente definidos caso uma solicitação esteja fora de sua área de responsabilidade.
- Educação contínua: implemente um programa de conscientização sobre segurança para educar consistentemente os funcionários ao longo do tempo. Use ferramentas como o Quiz da McAfee sobre phishing para destacar táticas específicas frequentemente utilizadas nos ataques.
- Permissão para verificar: ofereça à equipe a confiança de questionar até mesmo solicitações aparentemente inócuas. Um exemplo disso é questionar pessoas que tentam se infiltrar junto com pessoas autorizadas.

- Ensine a importância da informação: até mesmo informações aparentemente inócuas, como números de telefone (informações capacitadoras) podem ser utilizadas para orquestrar um ataque.
- Crie uma cultura de inculpabilidade: os alvos dos engenheiros sociais são vítimas. Punir funcionários específicos que tenham sido enganados torna toda a equipe menos propensa a admitir a liberação de informações. Uma vez enganados, eles podem ficar sob o controle do engenheiro social, o qual pode usar de chantagem.

Processo

- Relatórios de chamadas falsas: quando ocorrer uma atividade suspeita, a equipe deve fazer um relatório que descreva detalhadamente a interação. Isso ajuda nas investigações.
- Páginas informativas de bloqueio: quando os funcionários chegarem a uma página da Web maliciosa, use uma página de bloqueio para informá-los porque não devem prosseguir. Isso fará com que eles reflitam sobre sua ação anterior, o que pode ajudar a identificar fontes de ataques.
- Notificação ao cliente: caso informações sejam negadas aos interlocutores, a organização deve notificar a todos e verificar se o interlocutor tinha direito às informações. As organizações também devem avaliar como se comunicam com os clientes. Por exemplo, o PayPal inclui uma orientação para os usuários que ajuda a identificar se os e-mails recebidos são legítimos: "Um e-mail verdadeiro enviado por nós nunca pede o número da sua conta, o número do seu cartão de crédito ou de débito, etc. Também nunca perguntamos o seu nome completo, a senha da sua conta ou as respostas às perguntas de segurança do PayPal em um e-mail."
- Caminho de escalonamento: uma linha de relatório claramente definida na qual a equipe da linha de frente possa escalonar quaisquer dúvidas que tenham sobre interação com mensagens potencialmente fraudulentas.
- Testes de penetração: teste rotineiramente a equipe quanto à sua susceptibilidade a ataques de engenharia social pelo uso de múltiplos canais de comunicação. Isso proporciona uma ferramenta com a qual medir a eficácia dos programas de treinamento.

Tecnologia

- Gravação de chamadas: grave rotineiramente as chamadas telefônicas recebidas para auxiliar nas investigações.
- Linhas falsas: encaminhe para um número monitorizado as chamadas que parecerem suspeitas.
- Filtragem de e-mail: remova e-mails fraudulentos que contenham malware conhecido ou nunca antes visto.
- Filtragem da Web: bloqueie o acesso a sites maliciosos e detecte malware in-line com acesso à Internet.
- Autenticação forte: embora o uso de uma autenticação de múltiplos fatores não elimine o risco de que os usuários sejam induzidos por engenharia social a fornecer suas credenciais de autenticação, a tarefa se torna mais difícil para possíveis atacantes.

Siga o McAfee Labs

Resumo

A ameaça da engenharia social é bastante real. Os cibercriminosos a utilizam para extrair, de maneira ilegal, informações para vários fins maliciosos. Para enfrentar melhor esse problema, precisamos compreender a natureza dos ataques de engenharia social. Isso significa definir os responsáveis mais prováveis pelas ameaças, seus métodos de ataque e seus recursos — e aplicar os controles relevantes para reduzir o risco de um ataque bem-sucedido.

Uma cópia do relatório completo pode ser encontrada em **www.mcafee.com/hacking-human-os.**

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com