Novo kit de ferramentas MatrixPDF transforma PDFs em iscas de phishing

Data: 2025-10-01 00:20:39

Autor: Inteligência Against Invaders

Um novo kit de ferramentas de distribuição de phishing e malware chamado MatrixPDF permite que os invasores convertam arquivos PDF comuns em iscas interativas que ignoram a segurança de e-mail e redirecionam as vítimas para roubo de credenciais ou downloads de malware.

A nova ferramenta foi detectada por pesquisadores da Varonis, que disseram ao BleepingComputer que o MatrixPDF foi detectado pela primeira vez em um fórum de crimes cibernéticos. O vendedor também usa o Telegram como um meio adicional de interagir com os compradores.

O desenvolvedor do MatrixPDF promove a ferramenta como uma ferramenta de simulação de phishing e blackteaming. No entanto, o pesquisador da Varonis, Daniel Kelley, disse ao BleepingComputer que foi visto pela primeira vez sendo oferecido em fóruns de crimes cibernéticos.

“MatrixPDF: Document Builder – Advanced PDF Phishing with JavaScript Actions é uma ferramenta de elite para criar PDFs realistas de simulação de phishing adaptados para equipes negras e treinamento de conscientização sobre segurança cibernética”, diz um anúncio compartilhado com o BleepingComputer.

“Com importação de PDF de arrastar e soltar, visualização em tempo real e sobreposições de segurança personalizáveis, o MatrixPDF oferece cenários de phishing de nível profissional.”

“Proteções integradas, como desfoque de conteúdo, mecanismo de redirecionamento seguro, criptografia de metadados e desvio do Gmail, garantem autenticidade e entrega confiável em ambientes de teste.”

A ferramenta é oferecida em vários planos de preços, variando de US$ 400 por mês a US$ 1,500 por um ano inteiro.

[IMAGEM REMOVIDA]novo relatório da Varonis explica que o construtor MatrixPDF permite que invasores carreguem um PDF legítimo como isca e, em seguida, adicionem recursos maliciosos, como conteúdo desfocado, prompts falsos de “Documento Seguro” e sobreposições clicáveis que levam a um URL de carga útil externa.

[IMAGEM REMOVIDA]

Um teste da Varonis demonstra como os PDFs maliciosos puderam ser enviados para uma conta do

Gmail, ignorando os filtros de phishing. Isso ocorre porque os PDFs gerados não contêm binários maliciosos e apenas links externos.

“O visualizador de PDF do Gmail não executa PDF JavaScript, mas permite links/anotações clicáveis”, explica Varonis.

“Assim, o PDF do invasor é criado para que o pressionamento do botão simplesmente abra um site externo no navegador do usuário. Esse design um tanto inteligente funciona em torno da segurança do Gmail: qualquer verificação de malware do PDF em si não encontra nada incriminador, e o conteúdo malicioso real só é buscado quando o usuário clica ativamente, aparecendo no Gmail como uma solicitação da web iniciada pelo usuário.

Outra demonstração mostra como simplesmente abrir o PDF malicioso tenta abrir um site externo. Esse recurso é um pouco limitado, pois os visualizadores de PDF modernos alertarão o usuário de que o PDF está tentando se conectar a um site remoto.

Varonis adverte que os PDFs são um veículo popular para ataques de phishing porque são comumente usados e as plataformas de e-mail podem exibi-los sem aviso prévio.

A empresa diz que a segurança de e-mail orientada por IA, que analisa a estrutura do PDF, detecta sobreposições borradas e prompts falsos e detona URLs incorporados em uma sandbox, pode ajudar a impedir que esses arquivos cheguem à caixa de entrada do alvo.

Lawrence Abrams

Lawrence Abrams é o proprietário e editor-chefe da BleepingComputer.com. A área de especialização de Lawrence inclui Windows, remoção de malware e computação forense. Lawrence Abrams é coautor do Guia de campo de desfragmentação, recuperação e administração do Winternals e editor técnico do Rootkits for Dummies.

Você também pode gostar: