Os hackers armarem os códigos QR com links maliciosos para roubar dad

Data: 2025-08-21 21:42:17

Autor: Inteligência Against Invaders

O Quishing, uma forma poderosa de phishing que usa hiperlinks maliciosos contidos nos códigos QR

para expor as credenciais do usuário e dados sensíveis, surgiu no campo em constante mudança de

ameaças de segurança cibernética.

Diferentemente do phishing tradicional, que depende de links clicáveis ??ou e -mails enganosos, a realização explora a opacidade inerente aos códigos QR, que não são legíveis ao olho humano e, portanto, evitam suspeitas imediatas.

Os invasores favorecem esse método porque os códigos QR podem contornar as defesas de segurança convencionais, como gateways de email e scanners de URL, parecendo inócuos em trânsito.

Além disso, a necessidade de os usuários digitalizar esses códigos por meio de dispositivos móveis geralmente muda a interação fora dos perímetros de segurança corporativa, expondo vítimas a riscos sem as camadas de proteção de firewalls corporativos ou sistemas de detecção de terminais.

À medida que os atores de ameaças refinam suas táticas, as inovações recentes levaram a Quishing a territórios mais avançados, incorporando técnicas que desafiam até as ferramentas de segurança adaptativas.

Essa progressão ressalta a necessidade de as organizações entenderem os fundamentos técnicos desses ataques, desde a codificação da carga útil até os mecanismos de evasão, para reforçar suas posturas defensivas de maneira eficaz.

Táticas avançadas de evasão

Um dos mais recentes avanços em Quishing envolve dividir Códigos QRuma técnica recentemente adotada pela plataforma Gabagool Phishing-As-A-Service (PHAAS) para melhorar a furtividade e a evasão de detecção.

Nesta abordagem, os adversários dividem um único código QR malicioso em vários segmentos de imagem, incorporando -os separadamente nos e -mails de phishing.

Quando digitalizados pelas soluções tradicionais de segurança de email, esses fragmentos parecem visuais benignos e não relacionados, impedindo que o sistema reconstrua e analise o código completo.

Por exemplo, em uma campanha recente observada pelos analistas de ameaças, os operadores de

Gabagool implantaram códigos QR divididos em um golpe de redefinição de senha do Microsoft simulado, provavelmente precedido por uma conversa que sequestrava exploração para personalizar a atração e aumentar a credibilidade.

Após uma inspeção mais detalhada da estrutura HTML do email, o código QR se revela como um composto de duas imagens distintas que, quando digitalizadas juntas pelo dispositivo de um usuário, redirecionam para um site de phishing de colheita de credenciais.

De acordo com Barracuda relatórioesse método explora as limitações dos scanners estáticos de imagem, que não conseguem correlacionar elementos díspares sem renderização contextual.

Complementando isso, os códigos QR aninhados representam outra estratégia de evasão inovadora, como visto em implantações pelo TYCOON 2FA Kit Phaas.

Aqui, um código QR malicioso está em camadas dentro ou ao redor de um legítimo, criando ambiguidade em processos de detecção automatizados.

Em um ataque documentado, o código QR externo direcionou as vítimas para um URL fraudulento projetado para a exfiltração de dados, enquanto o código interno apontou benignas para um domínio confiável como o Google.

Essa estrutura dupla confunde scanners, produzindo resultados mistos durante a análise, pois a presença de um código interno válido pode mascarar a carga útil externa maliciosa, reduzindo assim a pontuação geral da ameaça nas avaliações baseadas em heurísticas.

Fortalecendo as defesas com IA multimodal

Para combater essas ameaças de Quishing rapidamente mutantes, os especialistas em segurança cibernética recomendam uma estratégia de defesa multifacetada que integra tecnologias avançadas às práticas fundamentais.

As medidas essenciais incluem treinamento abrangente de conscientização sobre segurança para educar os usuários sobre os riscos de código QR, juntamente com a autenticação multifatorial para mitigar roubo de credenciais e filtros robustos de spam para interceptar e -mails maliciosos no gateway.

No entanto, dada a sofisticação dos códigos QR divididos e aninhados, as organizações devem priorizar os sistemas de proteção de email de várias camadas aprimorados pela inteligência artificial multimodal.

Essas soluções acionadas por IA se destacam na detecção de ameaças, renderizando visualmente anexos para identificar códigos QR por meio de reconhecimento de caracteres ópticos (OCR) e processamento de imagens profundas, seguido pela decodificação do conteúdo incorporado para examinar URLs de destino ou cargas úteis.

Além disso, links suspeitos podem ser detonados em ambientes isolados de caixa de areia para observar comportamentos maliciosos em tempo real, enquanto os modelos de aprendizado de máquina analisam padrões de pixel e anomalias estruturais sem extração direta de conteúdo.

Tais abordagens integradas, combinando o processamento de linguagem natural para análise

contextual com visão computacional para ameaças baseadas em imagem, fornece uma barreira resiliente contra variantes de quishing que dependem apenas dos códigos QR para entrega.

Ao adotar essas salvaguardas técnicas, as empresas podem reduzir significativamente a superfície de ataque, garantindo que, mesmo que os adversários inovem, os mecanismos defensivos evoluem em conjunto para proteger ativos de dados sensíveis.

Encontre esta notícia interessante! Siga -nos Google News**Assim,**LinkedIn**e**X**Para obter atualizações instantâneas!**