BOLETIM DE SEGURANÇA

Violação de segurança no aplicativo Authy da Twilio compromete milhões de números de telefone

heimdall
security research
A DIVISION OF ISH

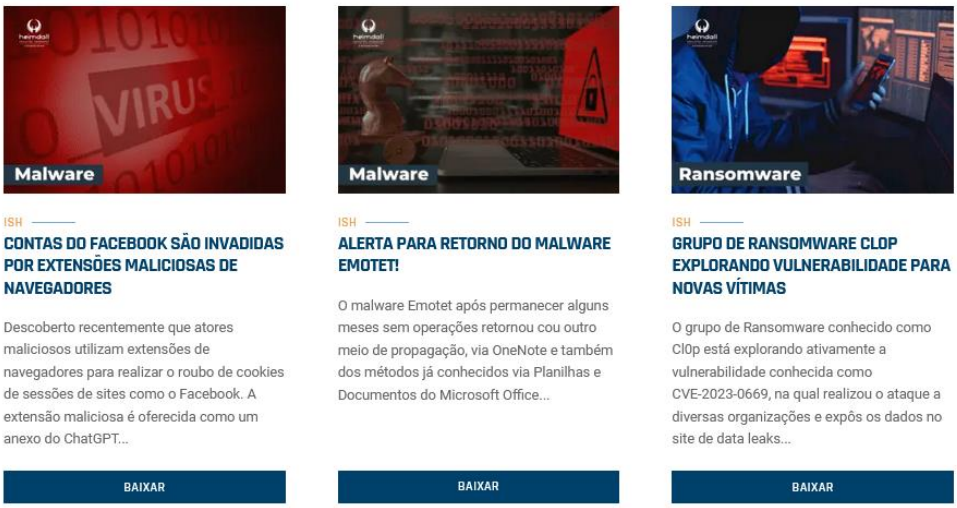
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Recentemente a empresa de comunicações em nuvem Twilio revelou que agentes de ameaças desconhecidos exploraram um endpoint não autenticado no Authy para acessar dados vinculados às contas do Authy, incluindo números de celular dos usuários, a mesma informou que tomou medidas para proteger o endpoint e impedir novas solicitações não autenticadas.

Esse evento ocorreu poucos dias após um ator de ameaça conhecido como ShinyHunters ter divulgado no BreachForums um banco de dados contendo 33 milhões de números de telefone supostamente obtidos de contas Authy. A Authy, que pertence à Twilio desde 2015, é um aplicativo popular de autenticação de dois fatores (2FA) que oferece uma camada extra de segurança para contas.

2 RISCOS ASSOCIADOS

A Twilio também informou que, não foram observadas evidencias que os agentes da ameaça obtiveram acesso aos sistemas da Twilio ou outros dados confidenciais. Porém ela recomenda que os usuários atualizem seus aplicativos **Android** (**versão 25.1.0 ou posterior)** e **iOS** (**versão 26.1.0 ou posterior**) para a versão mais recente. Também alertou que os agentes de ameaças podem tentar usar o número de telefone associado às contas Authy para ataques de phishing e smishing, e pede cuidado aos usuários.

3 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referido *ameaça*, como por exemplo:

Phishing

- Verificação de remetente: Sempre verifique o endereço de e-mail do remetente. E-mails de phishing frequentemente utilizam endereços que parecem legítimos, mas possuem pequenas variações.
- Desconfiança de anexos: Não abra anexos de e-mails suspeitos ou de remetentes desconhecidos. Eles podem conter malware.
- Avisos de segurança: Configure alertas de segurança para detectar e-mails suspeitos e avisar os usuários sobre possíveis ataques.
- Não fornecer informações pessoais: Nunca forneça informações pessoais ou financeiras em resposta a um e-mail. Empresas legítimas não solicitam esse tipo de informação por e-mail.
- Uso de filtros de spam: Utilize filtros de spam robustos para reduzir a quantidade de e-mails de phishing que chegam às caixas de entrada.

Smishing

- Desconfiança de mensagens de texto: Seja cauteloso com mensagens de texto que solicitam informações pessoais ou financeiras, especialmente se a mensagem criar um senso de urgência.
- Verificação de links: Evite clicar em links em mensagens de texto não solicitadas. Verifique o link digitando-o diretamente no navegador, se necessário.
- Bloqueio de números: Bloqueie números que enviam mensagens de smishing e reporte-os ao seu provedor de serviços.
- Utilização de aplicativos de segurança: Use aplicativos de segurança que possam detectar e bloquear mensagens suspeitas.
- Confirmação independente: Verifique a autenticidade de mensagens suspeitas diretamente com a empresa ou pessoa através de um canal de comunicação oficial.

Recomendações para empresas

- Implementação de políticas de segurança: Crie e implemente políticas claras sobre como lidar com e-mails e mensagens suspeitas.
- Monitoramento contínuo: Monitore continuamente os sistemas de TI para detectar atividades suspeitas.

- Respostas rápidas: Tenha um plano de resposta a incidentes para lidar rapidamente com ataques de phishing e smishing.
- Simulações de phishing: Realize simulações de ataques de phishing para treinar os funcionários a identificar e evitar esses ataques.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Twilio
- Thehackernews

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH