



BOLETIM DE SEGURANÇA

Entenda como funciona o golpe de SIM swap e seus riscos a organizações e pessoas



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

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

 Malware	 Malware	 Ransomware
ISH CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT... BAIXAR	ISH ALERTA PARA RETORNO DO MALWARE EMOTET! O malware Emotet após permanecer alguns meses sem operações retomou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office... BAIXAR	ISH GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS O grupo de Ransomware conhecido como CLOP está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks... BAIXAR

Sumário

1	Sumário Executivo	5
2	SIM SWAP	6
3	Golpes conhecidos.....	8
4	Como se proteger?	9
5	Referências.....	10

Lista de Figuras

Figura 1 – Diagrama de ataque de SIM swap.....	5
--	---

1 SUMÁRIO EXECUTIVO

O SIM Swap representa uma ameaça significativa para organizações. Criminosos podem obter acesso a contas e dados sensíveis através da troca do chip telefônico. Empresas, especialmente de telecomunicações e terceirização de processos, são alvos principais. Medidas de segurança são essenciais para proteger contra esse tipo de ataque.

Desta forma, a ISH Tecnologia detalha como funciona o golpe de SIM swap, bem como alguns detalhes de ataques identificados e outros detalhes de como se proteger.

A seguir, apresentamos o diagrama de um ataque de SIM swap, mencionando de forma detalhada posteriormente em seção o referido golpe.

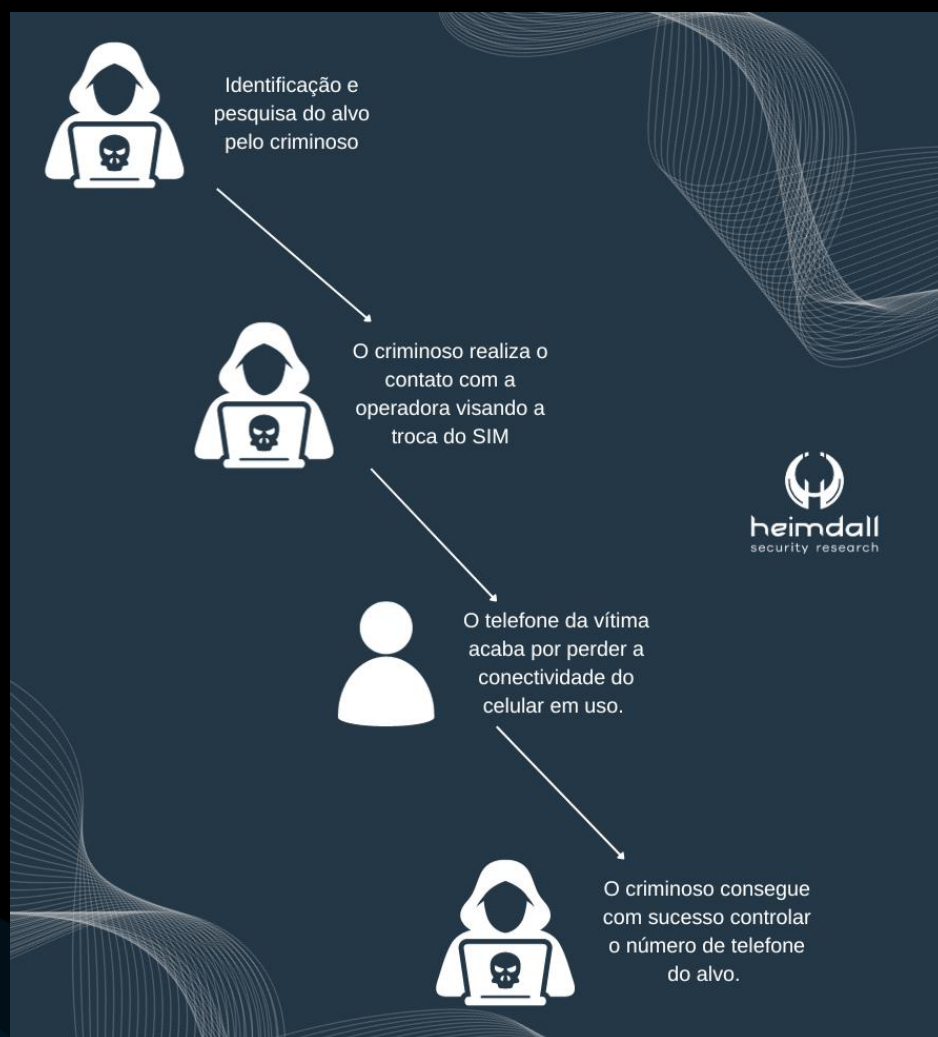


Figura 1 – Diagrama de ataque de SIM swap.

2 SIM SWAP

O SIM Swap, também conhecido como "clonagem de chip", é uma tática empregada por indivíduos mal-intencionados com o intuito de obter acesso a contas de e-mail, redes sociais e outros serviços que utilizam o número de telefone como meio de verificação. É importante ressaltar que esse tipo de ataque é frequentemente empregado para aquisição indevida de informações pessoais, realização de compras online ou até mesmo para assumir a identidade da vítima.

Como funciona?

O golpe de SIM swap começa quando um criminoso entra em contato com a operadora de telefonia da vítima e se passa por ela. O criminoso fornece informações pessoais da vítima, como nome, CPF e data de nascimento, visando solicitar a troca do SIM card.

Após a troca do SIM card, o criminoso passa a ter acesso a todas as mensagens SMS enviadas para o número da vítima, incluindo os códigos de verificação enviados por serviços como Instagram, Facebook e WhatsApp e, na sequência realiza a solicitação da troca de senhas de contas pessoais, já que muitas dessas contas são utilizadas o serviço de SMS como forma de autenticação de segurança.

Grupos de atores identificados utilizando o golpe?

Um dos atores da qual foram mapeados utilizando esta técnica são os atores denominados como "Scattered Spider" (UNC3944/ Scatter Swine e Muddled Libra) os quais existem desde maio de 2022.

Os atores realizam o SIM swap, ataques de phishing por e-mail e SMS e, por vezes realizam o envio de phishing em outras pessoas dentro de uma organização depois de invadirem bancos de dados de funcionários.

De acordo com a Mandiant e Trellix, os alvos do grupo de ameaças geralmente são empresas de telecomunicações e terceirização de processo de negócios (BPO) porém, outras pesquisas identificaram que o grupo possui o foco em outros segmentos, como o ICS.

Declaração da ANATEL

Em 28 de Agosto de 2023, a Anatel teria afirmado que entrariam em vigor novas regras para prevenção e fraudes e portabilidade numérica, sendo que agora, o usuário terá que responder a um SMS confirmando o processo de troca de operadora mantendo o número telefônico. Essas regras de acordo com a agência, é para barrar os golpes de trocas de SIM (SIM swap).

3 GOLPES CONHECIDOS

Um dos golpes mais comuns que são praticados pelos criminosos é após conseguir realizar o golpe do SIM swap, realizar o acesso junto a uma conta do Instagram da vítima e na sequência, inicia a prática do golpe do PIX.

Neste tipo de golpe, os criminosos acabam realizando publicações, enviam mensagens para os seguidores e oferecem um suposto investimento com determinado retorno, de até 1.000%, além claro de fazer rifas falsas. Tais atos levam os seguidores a acreditar que realmente é autêntico.

Recentemente, um indivíduo na Flórida foi preso após realizar o golpe de SIM swap e teria roubado aproximadamente quase US\$ 1 milhão em criptomoedas de dezenas de vítimas.

Outro golpe foi reportado pelo cofundador da Ethereum, Vitalik Buterin, o qual teria confirmado que teria sido vítima de SIM swap. Um dos tipos de métodos utilizados pelos atores foi a publicação no X sobre uma oferta falsa de NFTs, levando os usuários a clicar em um link malicioso que teria resultado na perda coletiva de mais de US\$691.000 pelas vítimas.

4 COMO SE PROTEGER?

Os usuários podem adotar algumas medidas para se proteger e evitar de cair no golpe de SIM swap, como:

1. Não utilize a verificação de duas etapas via SMS.

Caso o cibercriminoso consiga realizar a troca de SIM, é possível realizar o "reset" em suas contas que estiverem habilitadas as opções de recuperações via SMS.

2. Ative a verificação de duas etapas no WhatsApp

Após habilitar o código PIN de seis dígitos no WhatsApp é importante também que seja definido um endereço de e-mail para recuperar este PIN.

3. Ative os códigos PIN e PUK do seu chip SIM

Os códigos PIN e PUK são a última linha de defesa do seu chip SIM, já que toda vez que ele for colocado em um novo celular ou aparelho for reiniciado, o PIN será solicitado para ser liberado. O código PUK serve para desbloquear o chip caso o PIN seja inserido errado várias vezes, sendo a chave mestra do chip.

Caso o PUK seja digitado errado 10 vezes, o chip é bloqueado definitivamente; o usuário terá que ir até a loja da operadora para resgatar o número em outro chip.

5 REFERÊNCIAS

- Heimdall *by* ISH Tecnologia



heimdall
security research

A DIVISION OF ISH