BOLETIM DE SEGURANÇA

Usuários de IPhone em 92 países são alvos de spyware mercenário.

heimdall
security research
A DIVISION OF ISH

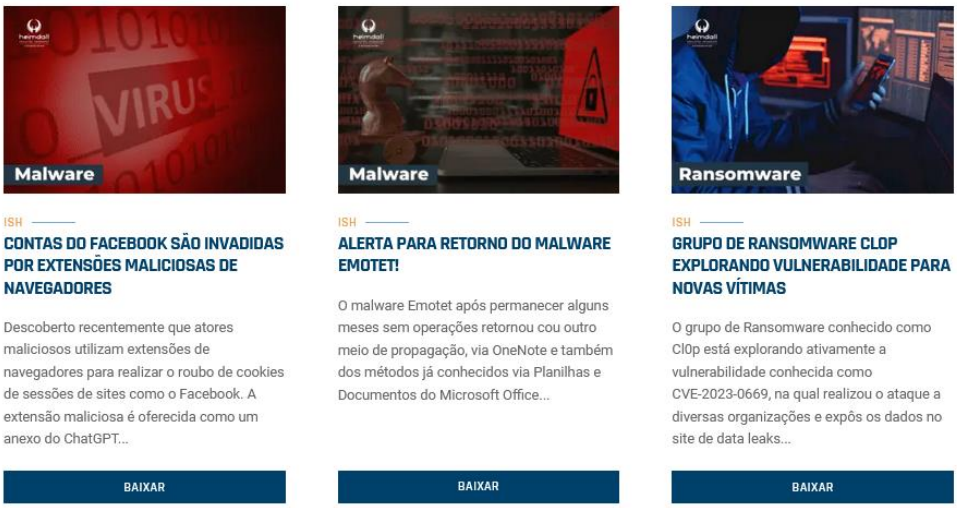
TLP: CLEAR

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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Apple está alertando usuários de iPhone em 92 países a respeito de um “ataque de spyware mercenário”. Este ataque visa invadir os dispositivos de forma remota. De acordo com a empresa, este ataque provavelmente tem como alvo usuário especificamente por causa de quem é ou do que faz. Embora nunca seja possível obter certeza absoluta ao detectar esses ataques, a Apple está muito confiante em suas suspeitas e que seus usuários levem a sério.

2 INFORMAÇÕES SOBRE A AMEAÇA

A Apple informa que esses ataques são muito mais complexos do que a atividade cibercriminosa normal, uma vez que os atacantes de spyware mercenário aplicam recursos excepcionais para atingir um número muito pequeno de indivíduos específicos e seus dispositivos. Esses ataques custam milhões de dólares e muitas vezes têm uma vida útil curta, tornando-os muito mais difíceis de detectar e prevenir.

De acordo com relatórios públicos e pesquisas realizadas por organizações civis, empresas de tecnologia, ataques direcionados individualmente de custo e complexidade tão excepcionais têm sido historicamente associados a atores estatais, incluindo empresas privadas que desenvolvem spyware mercenário em seu nome, como o Pegasus da NSO Group. Embora sejam utilizados contra um número muito pequeno de indivíduos, muitas vezes jornalistas, ativistas, políticos e diplomatas, os ataques de spyware mercenário são globalmente contínuos. Desde 2021, foi enviado notificações de ameaças à Apple à medida que foram detectados esses ataques e, até o momento, os usuários foram notificados em mais de 150 países no total. O custo extremo, a sofisticação e a natureza mundial dos ataques desta ameaça fazem deles algumas das ameaças digitais mais avançadas existentes atualmente. Como resultado, a Apple não atribui os ataques ou notificações de ameaças resultantes a invasores ou regiões geográficas específicas.

Caso seu iPhone seja comprometido por este tipo de ameaça, a Apple enviará alertas através de e-mail e iMessage para os contatos associados ao seu ID Apple. Além disso, uma notificação de segurança aparecerá no portal Apple ID quando você acessar sua conta, servindo como uma verificação adicional de autenticidade.

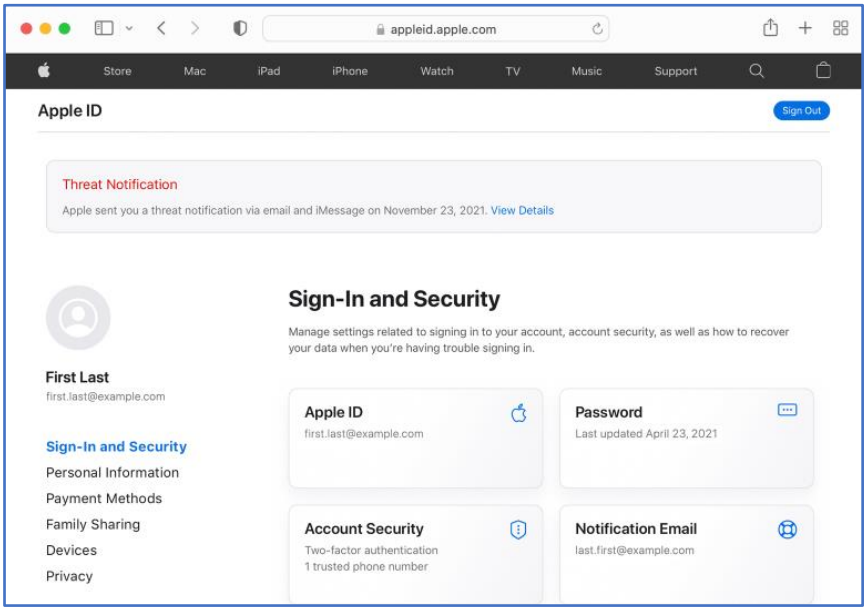


Figura 1 – Portal da Apple ID.

Os sofisticados ataques de spyware, com financiamento robusto e em constante evolução, são monitorados pela Apple através de métodos próprios de inteligência de ameaça e investigação. As notificações de ameaças emitidas pela empresa são indicativos confiáveis de que um usuário pode ter sido alvo de tais softwares maliciosos. É importante tratar esses avisos com seriedade, embora a Apple não revele os critérios específicos para sua emissão, a fim de não fornecer vantagens aos atacantes. É fundamental estar ciente de que a Apple não pedirá ações como clicar em links, abrir arquivos, instalar apps ou fornecer senhas via e-mail ou telefone em suas notificações de ameaças. Para confirmar a autenticidade de um alerta, o usuário deve acessar diretamente o site appleid.apple.com, onde as notificações legítimas estarão visíveis após o login.

3 RECOMENDAÇÕES

A Apple recomenda que todos os usuários realizem nesse caso são as seguintes:

- Entre em contato com a Linha Direta de Segurança Digital em Access Now para obter ajuda e conselhos sobre segurança de emergência.
- Ative o Modo Lockdown para proteção adicional contra spyware, reduzindo significativamente a superfície de ataque.
- Atualize aplicativos de mensagens e de nuvem para as versões mais recentes disponíveis.
- Atualize todos os outros dispositivos Apple (Mac, iPad) que você usa e habilite o Modo Lockdown neles também.
- Use autenticação de dois fatores e uma senha forte para Apple ID.

Siga boas práticas gerais, como aplicar as atualizações mais recentes, usar senhas, ativar a autenticação de dois fatores, baixar aplicativos apenas da App Store, usar senhas fortes e exclusivas e evitar abrir links ou anexos suspeitos.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Support.Apple**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH