BOLETIM DE SEGURANÇA

Dados de 70 milhões de clientes são vazados afirma AT&T, em violação de dados

heimdall
security research
A DIVISION OF ISH

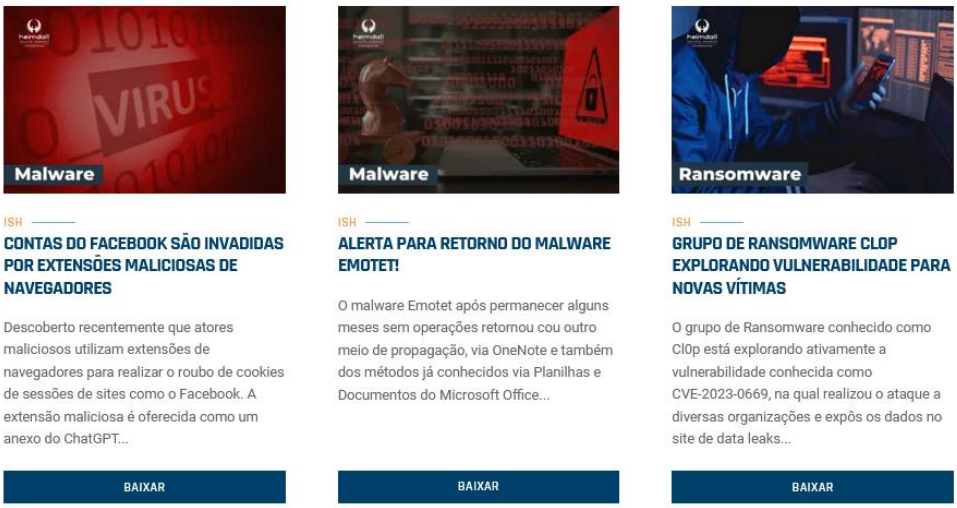
TLP: CLEAR

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

Após negar inicialmente, a AT&T admitiu que foi vítima de uma violação de dados. A violação afetou 73 milhões de seus clientes, tanto atuais quanto antigos. A empresa passou as últimas duas semanas negando que os dados vazados tivessem se originado de seus sistemas. No entanto, agora confirmou que a origem do vazamento de uma grande quantidade de dados de clientes era de fato de seus sistemas.

Figura 1 – Logo AT&T.

2 INFORMAÇÕES SOBRE O INCIDENTE

A AT&T reconheceu que os dados vazados são de 73 milhões de seus clientes, tanto atuais quanto antigos. Segundo uma análise preliminar da empresa, os dados parecem ser de 2019 ou antes, afetando cerca de 7,6 milhões de titulares de contas atuais e aproximadamente 65,4 milhões de ex-titulares de contas. Além disso, a AT&T também confirmou que as senhas de segurança usadas para proteger as contas vazaram para 7,6 milhões de clientes.

Em 2021, Shiny Hunters, um conhecido agente de ameaças, afirmou estar comercializando dados de 73 milhões de clientes da AT&T que teriam sido roubados. Esses dados abrangem nomes, endereços, números de telefone e, para muitos, números de segurança social e datas de nascimento. Naquele momento, a AT&T refutou a ocorrência de qualquer violação ou que os dados provinham de seus sistemas. Avançamos para 2024, e um novo agente de ameaças divulgou esse vasto conjunto de dados em um fórum de hackers, alegando serem os mesmos dados que Shiny Hunters havia roubado.

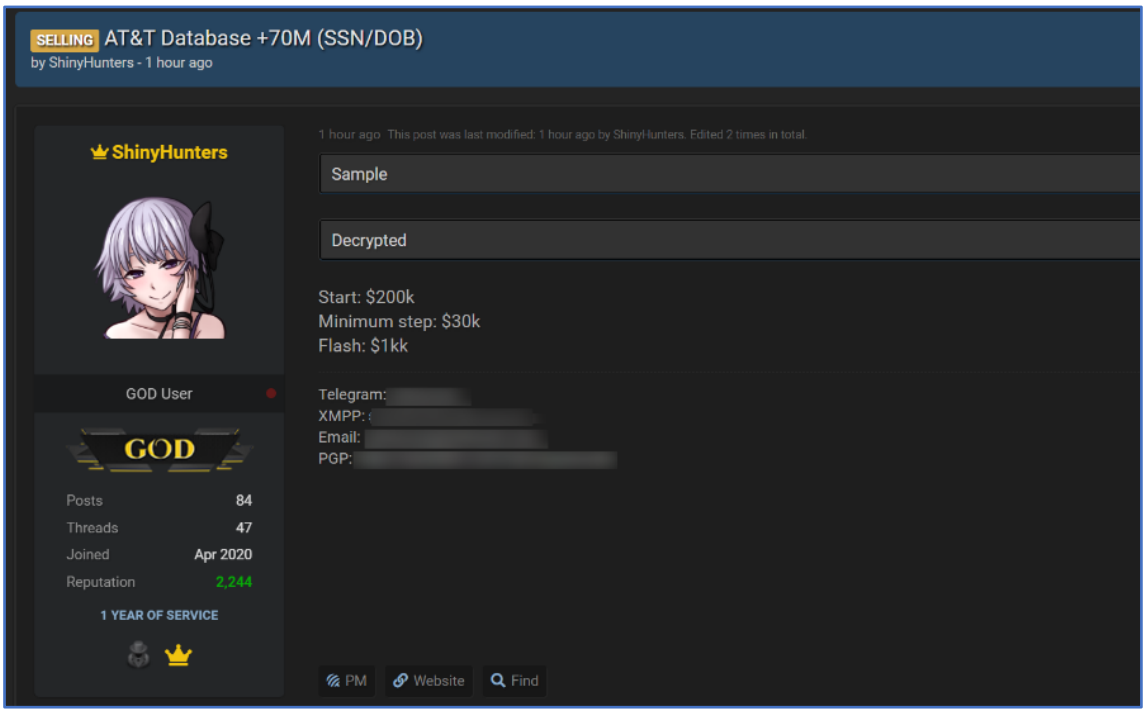


Figura 2 – ShinyHunters tentando vender supostos dados da AT&T.

Foi realizada uma análise dos dados e concluiu que eles continham as mesmas informações sensíveis que Shiny Hunters afirmou ter roubado. Contudo, nem todos os clientes tiveram seus números de segurança social ou datas de nascimento revelados neste incidente.

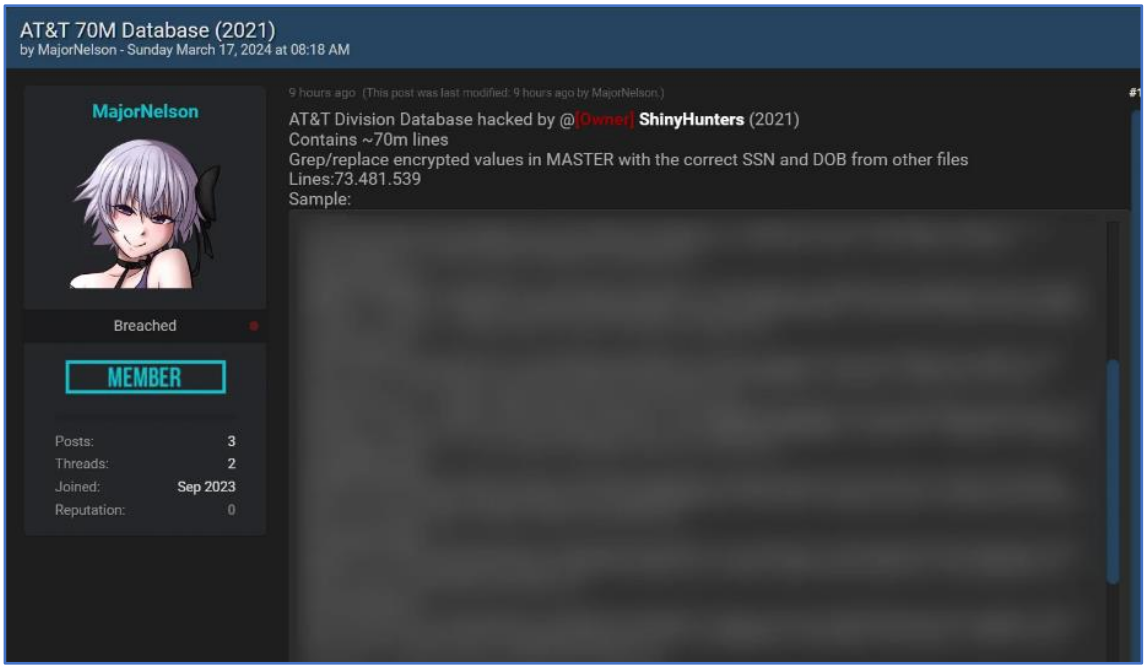


Figura 3 – Fórum com supostos dados vazados da AT&T em 2021.

Embora a AT&T tenha reiterado que não foi vítima de uma violação de dados, evidências sugerem o contrário. Após uma conversa com mais de 50 clientes da AT&T e DirectTV, descobriu-se que os dados vazados incluíam informações exclusivas para suas contas da AT&T. Os clientes revelaram que utilizaram recursos de e-mail descartável do Gmail e do Yahoo para criar endereços de e-mail específicos para a DirectTV ou AT&T, usados apenas ao se inscreverem no serviço. Isso sugere que os dados vazados provavelmente se originaram da DirectTV ou AT&T, pois esses endereços de e-mail não foram usados em outras plataformas.

Além disso, foi confirmada informações semelhantes após os dados serem adicionados ao serviço de notificação de violação de dados *Have I Been Pwned*. No entanto, apesar de várias tentativas de contato com a AT&T sobre essas informações, a empresa não respondeu a mais e-mails até o momento. A DirectTV, em resposta, indicou que quaisquer perguntas adicionais deveriam ser direcionadas à AT&T, pois os dados em questão são de um período anterior à sua separação e eles não têm mais acesso aos sistemas da AT&T para verificação. A AT&T, por sua vez, informou que apenas divulgaria mais detalhes sobre a violação em sua declaração oficial e em uma nova página dedicada à segurança das contas da AT&T.

Essa página de segurança revelou que as senhas de 7,6 milhões de clientes da AT&T foram comprometidas durante a violação e, consequentemente, foram redefinidas pela empresa. As senhas são usadas pelos clientes para adicionar uma camada extra de proteção às suas contas da AT&T, sendo necessárias para receber suporte ao cliente, gerenciar contas em lojas físicas ou acessar suas contas online.

A AT&T divulgou em um comunicado que várias de suas senhas foram comprometidas. A empresa está tomando medidas para entrar em contato com todos os 7,6 milhões de clientes afetados e já redefiniu suas senhas. Além disso, a AT&T planeja se comunicar com os titulares de contas atuais e antigos cujas informações pessoais confidenciais foram comprometidas. Foi o *TechCrunch* que primeiro relatou sobre as senhas comprometidas, após ser contatado por um pesquisador que afirmou que os dados vazados incluíam senhas criptografadas de milhões de usuários.

A AT&T esclareceu que os dados comprometidos parecem ser de 2019 ou anteriores e não incluem informações financeiras pessoais ou históricos de chamadas. Também planeja informar todos os seus 73 milhões de clientes, tanto antigos quanto atuais, sobre a recente violação de segurança e orientá-los sobre as medidas a serem tomadas. Além disso, os clientes têm a opção de usar o serviço "*Have I Been Pwned*" para verificar se seus dados foram comprometidos neste incidente específico.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bleepingcomputer**
- **Prnewswire**

heimdall
security research
A DIVISION OF ISH