BOLETIM DE SEGURANÇA

Indústrias de petróleo e gás são alvos de ataques de phishing

heimdall
security research
A DIVISION OF ISH

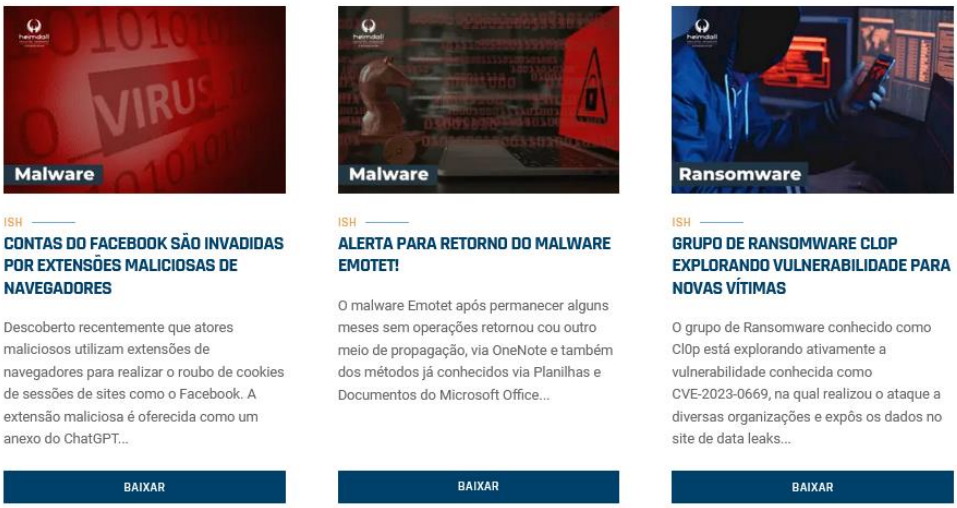
TLP: CLEAR

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

Em fevereiro de 2024, a Cofense Intelligence detectou uma sofisticada campanha de phishing voltada para a indústria de Petróleo e Gás. O objetivo era disseminar o Rhadamanthys Stealer, um sofisticado ladrão de dados disponibilizado como Malware-as-a-Service (MaaS). A campanha utilizou diversas táticas, técnicas e procedimentos (TTPs) complexos. Essa campanha ocorreu logo após várias atualizações do Rhadamanthys MaaS no mercado. Devido à singularidade da campanha e ao sucesso na entrega dos e-mails aos alvos, a Cofense Intelligence publicou um novo alerta Flash sobre a campanha de malware MaaS InfoStealer direcionada ao setor de petróleo e gás, juntamente com um relatório sobre ameaças ativas.

2 INFORMAÇÃO SOBRE A CAMPANHA

A campanha tem como foco principal o setor de Petróleo e Gás. A razão para a escolha deste setor não é clara, mas a campanha poderia ser aplicada a outros setores se os atores da ameaça optassem por mudar seus alvos. A campanha tem sido eficaz em atingir seus alvos através de e-mails, graças à utilização de uma série de TTPs (Táticas, Técnicas e Procedimentos) comuns que dificultam a análise. Ao combinar vários TTPs, como o uso de domínios confiáveis, múltiplos redirecionamentos e imagens clicáveis, os atores da ameaça conseguem aumentar a probabilidade de seus e-mails passarem pelos padrões de segurança de e-mail atuais e atingirem seus alvos. A figura abaixo ilustra a cadeia de infecção desta campanha, desde o ator da ameaça até o executável final do Rhadamanthys Stealer.

Figura 1 – Cadeia de infecção da campanha de phishing.

A ameaça é iniciada elaborando e-mails personalizados, cujo tema central é a implicação do veículo do destinatário em um incidente. O primeiro sinal de malícia é um link inserido no e-mail que explora um redirecionamento aberto, uma falha em um site que permite aos agentes de ameaça redirecionar as vítimas para um local mal-intencionado através de um caminho específico em um domínio legítimo. Os redirecionamentos abertos nesta campanha estão principalmente hospedados em domínios legítimos do Google, como Google Maps e Google Images. O link inserido leva a um encurtador de URL, que além de reduzir o tamanho do URL, ajuda a ocultá-lo. Este encurtador de URL serve como uma camada extra de evasão nesta campanha, pois os agentes de ameaça costumam adicionar mais redirecionamentos na cadeia de infecção para aumentar as chances de os e-mails maliciosos passarem despercebidos pelos SEGs.

Após o redirecionamento, as vítimas são levadas a um arquivo PDF clicável hospedado no domínio *docptypefinder[.]info*, que foi registrado no mesmo dia em que a campanha foi detectada pela primeira vez. O PDF, que é mostrado na Figura 4 mais adiante no relatório, é uma imagem clicável que imita o Departamento Federal de Transportes e menciona uma possível multa de US$ 30 mil pelo incidente. Ao clicar na imagem, é feito o download ou solicitado o download de um arquivo ZIP. Este arquivo contém um executável que, quando executado, descompacta e inicia o Rhadamanthys Stealer. O malware estabelece imediatamente uma conexão com um servidor de comando e controle (C2) que recolhe quaisquer credenciais roubadas, carteiras de criptomoedas ou outras informações sensíveis.

Embora possa parecer estranho utilizar acidentes de veículos como chamariz para phishing, os agentes de ameaça nesta situação se esforçam bastante para assegurar que seus e-mails e a cadeia de infecção correspondente atinjam seu destinatário. Cada e-mail tem um assunto e um corpo distinto, mas em geral, eles informam um funcionário sobre um incidente de trânsito, seja por meio de uma notificação ao empregador, possíveis ações judiciais ou até mesmo um aviso de contato com as autoridades. A seguir um exemplo de um dos e-mails de phishing observados nesta campanha. Apesar do assunto e do corpo serem diferentes dos outros e-mails, o tema geral é o mesmo, neste caso, uma notificação do empregador de que o funcionário esteve envolvido em um acidente de carro.

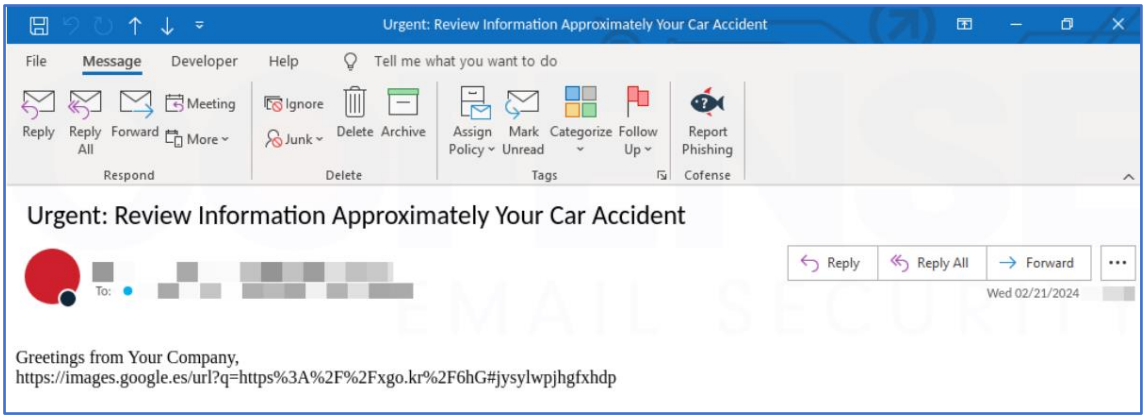


Figura 2 – E-mail de phishing com tema de incidente de veículo entregando Stealer.

Considerando o grande número de e-mails e a aparente aleatoriedade de cada um, na figura abaixo nos mostra uma visão geral de todas as palavras-chave empregadas durante a campanha. Palavras comuns como incidente, acidente, veículo, automóvel, carro e carruagem são facilmente identificáveis na nuvem de palavras, seguindo a temática da campanha. Além dessas, existem várias palavras adicionais usadas para provocar emoções no destinatário, como urgente, imediato, obrigatório, notificação, preocupante e importante. A ameaça de um ataque de phishing se torna significativamente maior quando os agentes de ameaça combinam TTPs conhecidos por ajudar a burlar a segurança com iscas cuidadosamente elaboradas e projetadas socialmente, como é o caso aqui.

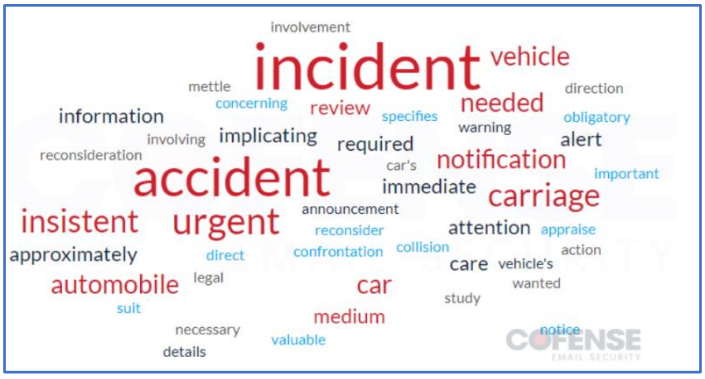


Figura 3 – Palavras-chaves utilizadas.

A campanha se destaca por sua singularidade, incluindo o uso de táticas sofisticadas de engenharia social e TTPs evasivos, com o propósito principal de infectar os alvos com o Rhadamanthys Stealer. Este malware, embora incomum, é avançado e é oferecido como um serviço (MaaS) para quem deseja adquiri-lo através de uma assinatura. Escrito em C++, o Rhadamanthys Stealer possui diversos recursos únicos, tornando-o a opção ideal para agentes de ameaças interessados em roubar credenciais, informações sensíveis e criptomoedas. O malware tem como alvo principalmente as credenciais armazenadas em vários aplicativos e navegadores. Uma vez infectada uma máquina, o malware se conectará a um C2, geralmente uma URL com um caminho de URL único; neste caso, a URL terminava com [.]gir3n.

O Rhadamanthys Stealer é menos comum em comparação com outros stealers frequentemente observados no cenário de ameaças de phishing. A súbita aparição de uma família de malware tão atípica levanta questionamentos sobre a escolha dos atores da ameaça por este malware específico, especialmente levando em conta os altos preços indicados. O Rhadamanthys Stealer recebeu diversas atualizações significativas, incluindo plug-ins adicionais, recursos de roubo e táticas evasivas para o malware. Isso provavelmente motivou a campanha, uma vez que ela surgiu pouco tempo após a implementação dessas atualizações.

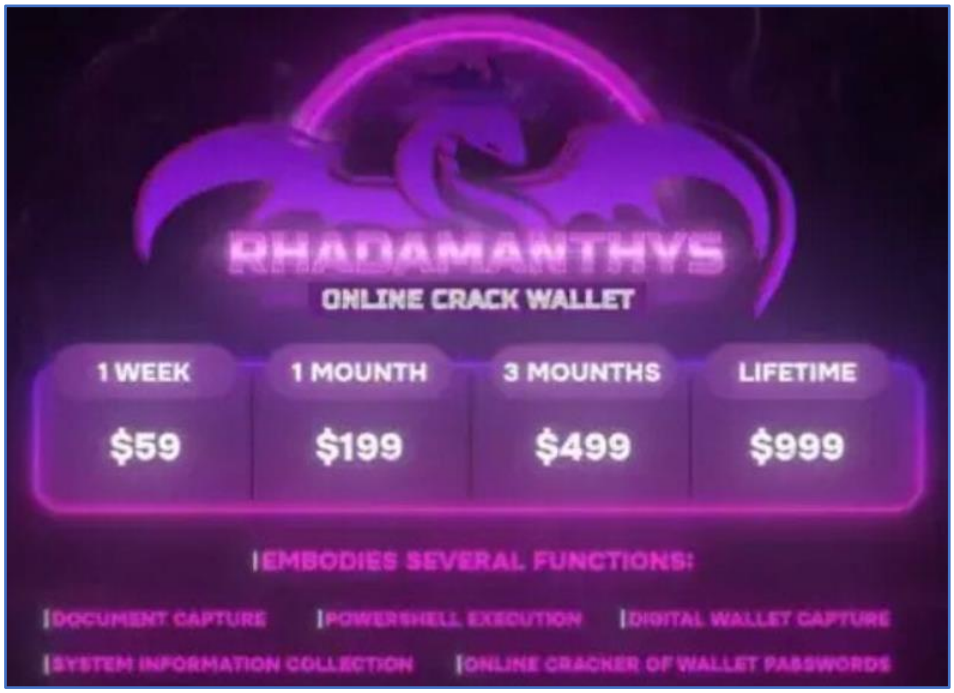


Figura 4 – Logotipo do Rhadamanthys Stealer.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Monitoramento e prontidão

- Mantenha um alto grau de monitoramento e prontidão, particularmente quanto à análise de logs de mudanças de IP e logins de geolocalizações suspeitas.

Atualizações de sistemas

- Mantenha os sistemas operacionais e aplicativos dos processos críticos ao negócio do órgão sempre atualizados.

Usuários administradores

- Utilize usuários administradores diferentes dos gestores de domínios.

Verificação de vulnerabilidades

- Verifique se seus sistemas estão vulneráveis à CVEs conhecidas, tomando as medidas de mitigação ou corretivas, conforme necessário.

Revisão de logs de tráfego

- Reveja os logs de tráfego de rede em busca de atividades relacionadas aos endereços IPs com tráfego HTTP.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Cofense
- Thehackernews

heimdall
security research
A DIVISION OF ISH