TLP: CLEAR

BOLETIM DE SEGURANÇA

Plataforma de Phishing Sniper Dz facilita mais de 140.000 ataques cibernéticos em busca de credenciais de usuários

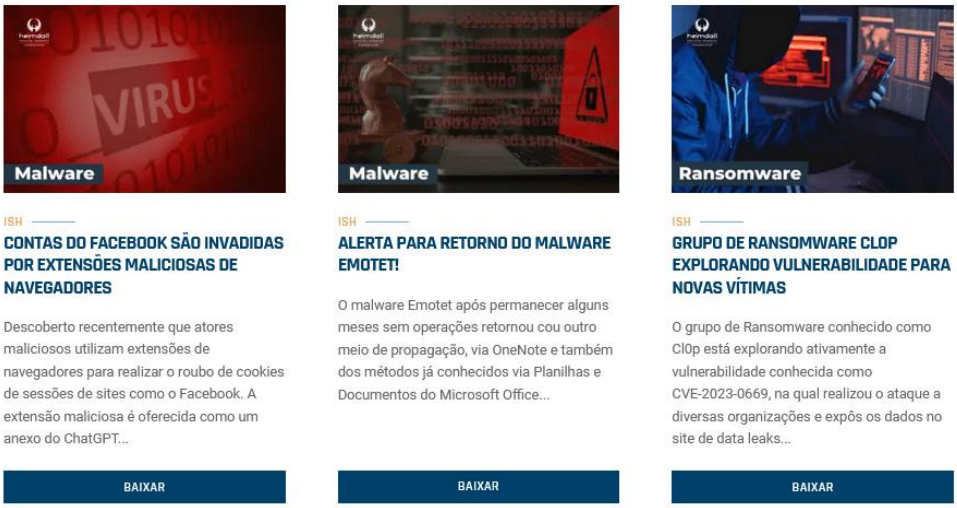
heimdall
security research
A DIVISION OF ISH

Acesse a nossa nova comunidade através do WhatsApp!

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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

No último ano, foram identificados mais de 140.000 sites de phishing associados à plataforma de phishing como serviço (**PhaaS**) Sniper Dz. Isso revela que a plataforma está sendo amplamente utilizada por criminosos cibernéticos para o roubo de credenciais de usuários.

2 INFORMAÇÕES SOBRE A AMEAÇA

O Sniper Dz adota uma estratégia inovadora ao ocultar o conteúdo de phishing por trás de um servidor proxy público, permitindo a realização de ataques de phishing em tempo real. Os criminosos que operam essa plataforma configuram automaticamente o servidor proxy para carregar o conteúdo de phishing hospedado em seus servidores. Essa técnica pode ser eficaz para proteger a infraestrutura contra detecção. A plataforma oferece um painel de administração online com um catálogo de páginas de phishing, que podem ser hospedadas na infraestrutura do Sniper Dz ou baixadas para servidores próprios dos phishers. Notavelmente, o Sniper Dz PhaaS disponibiliza esses serviços gratuitamente, possivelmente porque também coleta credenciais roubadas para compensar os custos operacionais.

Os criminosos que utilizam o Sniper Dz frequentemente exploram plataformas legítimas de software como serviço (SaaS) para hospedar seus sites de phishing. Ao configurar sua infraestrutura, esses phishers utilizam nomes de marcas conhecidas, tendências atuais e tópicos sensíveis como palavras-chave para atrair vítimas. Após obter as credenciais de uma vítima, a infraestrutura pode redirecioná-la para anúncios maliciosos, incluindo a distribuição de aplicativos ou programas potencialmente indesejados (PUA ou PUP), como instaladores de navegadores suspeitos.

O Sniper Dz é uma plataforma de Phishing-as-a-Service (**PhaaS**) que facilita a realização de ataques de phishing por phishers em potencial. A plataforma oferece um painel de administração para a criação de páginas de phishing. Para acessar esse painel, é necessário criar uma conta utilizando um endereço de e-mail. Após o registro, os usuários (ou phishers) podem acessar uma ampla gama de páginas de phishing voltadas para marcas conhecidas.

O ator disponibiliza dois métodos para lançar ataques de phishing ao vivo como, páginas de phishing hospedadas em sua própria infraestrutura e modelos de phishing para download, que podem ser hospedados na infraestrutura do usuário.A plataforma pode hospedar páginas de phishing em sua própria infraestrutura e fornecer links personalizados para essas páginas. O painel de administração do Sniper Dz, que compartilha links temporários para páginas de phishing ativas, personalizadas para o usuário registrado. Dessa forma, um phisher não precisa configurar um servidor web para hospedar sites de phishing, podendo utilizar a infraestrutura do Sniper Dz para realizar os ataques.

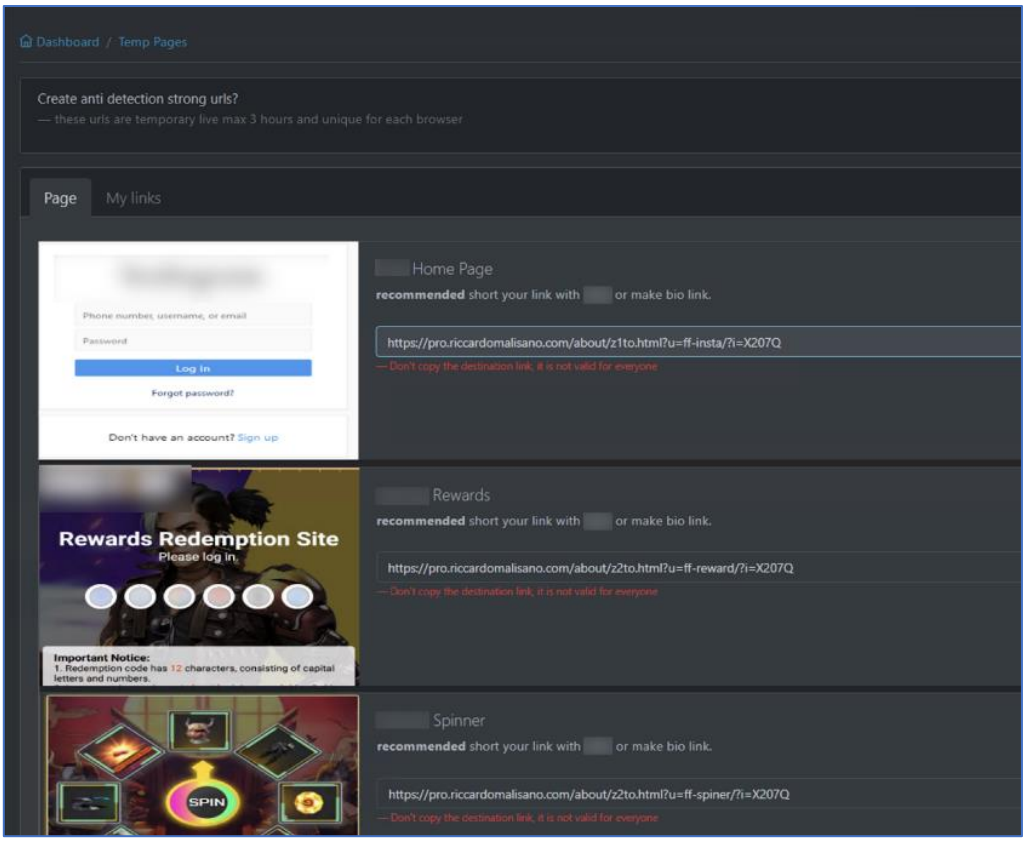


Figura 1 – Painel de administração do Sniper Dz.

O Sniper Dz oferece aos phishers a possibilidade de baixar modelos de páginas de phishing offline em formato HTML, permitindo que eles hospedem essas páginas em seus próprios servidores. Os phishers interessados podem selecionar uma marca-alvo, baixar a página de phishing correspondente e implantá-la em seus servidores pessoais.

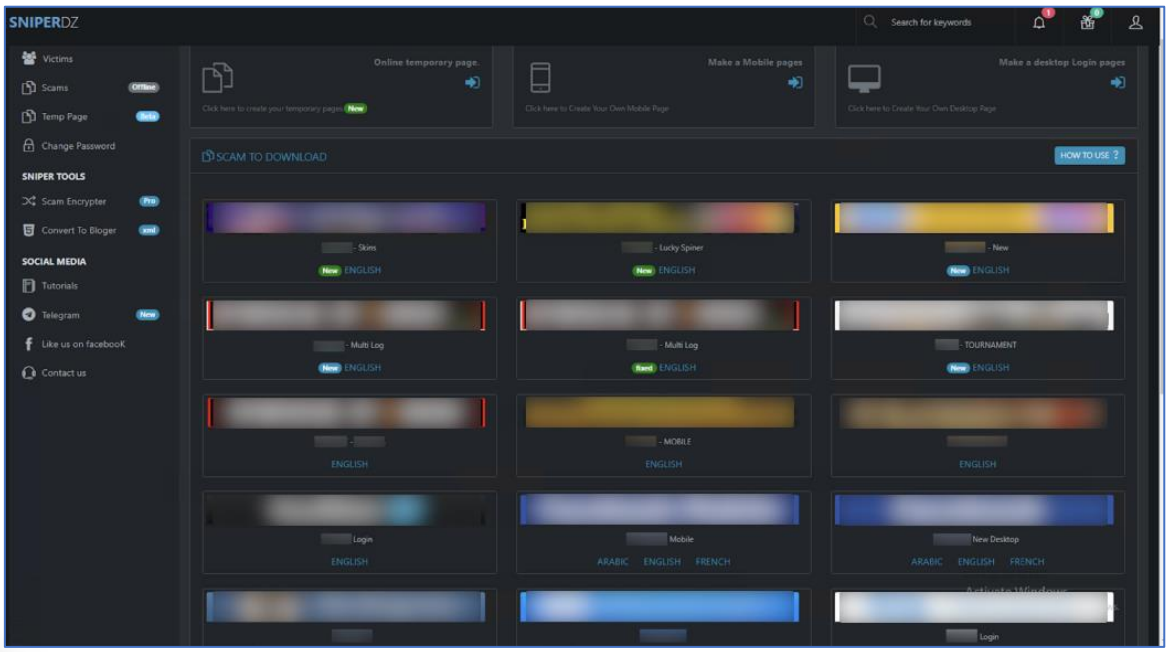


Figura 2 – Lista de páginas de modelos de phishing para download do site Sniper Dz.

O Sniper Dz faz uso de um servidor proxy público legítimo (**proxymesh[.]com**) para esconder seu conteúdo de phishing. Agentes de ameaças frequentemente abusam de produtos legítimos para fins maliciosos, o que não significa que esses produtos sejam falhos ou maliciosos. O grupo responsável pelo ator configura esse servidor proxy para carregar automaticamente o conteúdo de phishing de seu próprio servidor, sem comunicações diretas. Essa técnica pode ajudar o Sniper Dz a proteger seus servidores backend, pois o navegador da vítima ou um rastreador de segurança verá o servidor proxy como o responsável por carregar o payload de phishing.

O Sniper Dz utiliza um servidor proxy público para ocultar solicitações ao seu servidor web (**dev-cdn370[.]pantheonsite[.]io**), que hospeda conteúdo de phishing. O ponto de entrada é uma página de phishing descartável que os invasores podem distribuir às vítimas por e-mails ou redes sociais. Quando uma vítima acessa essa página, ela retorna um script que configura automaticamente o servidor proxy.

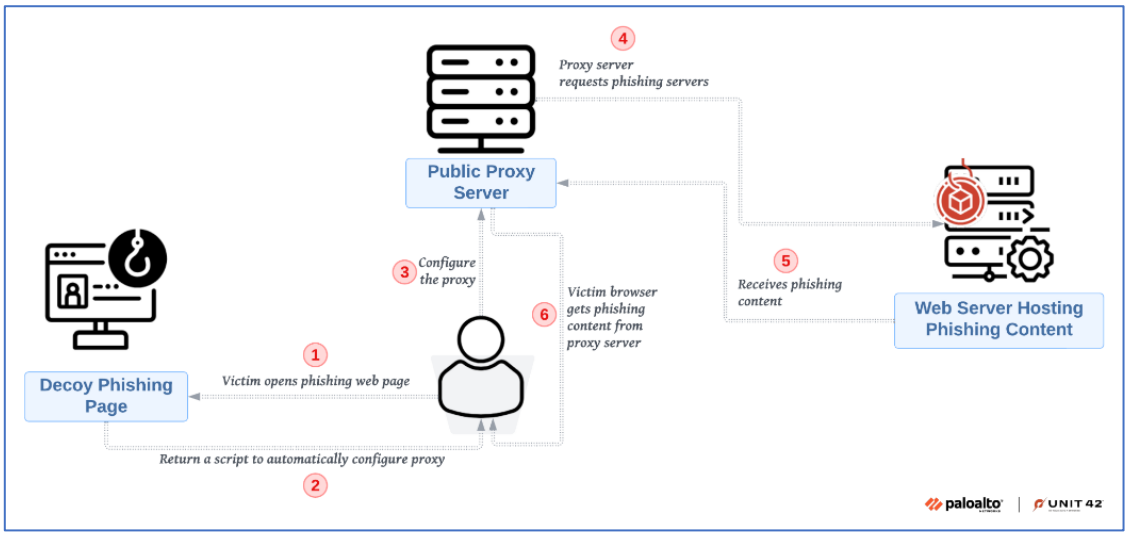


Figura 3 – Fluxo de trabalho para ocultar conteúdo de phishing atrás de um servidor proxy público.

Essas páginas de phishing enviam credenciais para uma infraestrutura centralizada controlada pelo Sniper Dz. Na figura abaixo apresenta uma captura de tela do console do depurador do Google Chrome, mostrando a URL de exfiltração **raviral[.]com/k_fac.php**, onde os parâmetros email e pass são usados para exfiltrar e-mail e senha.

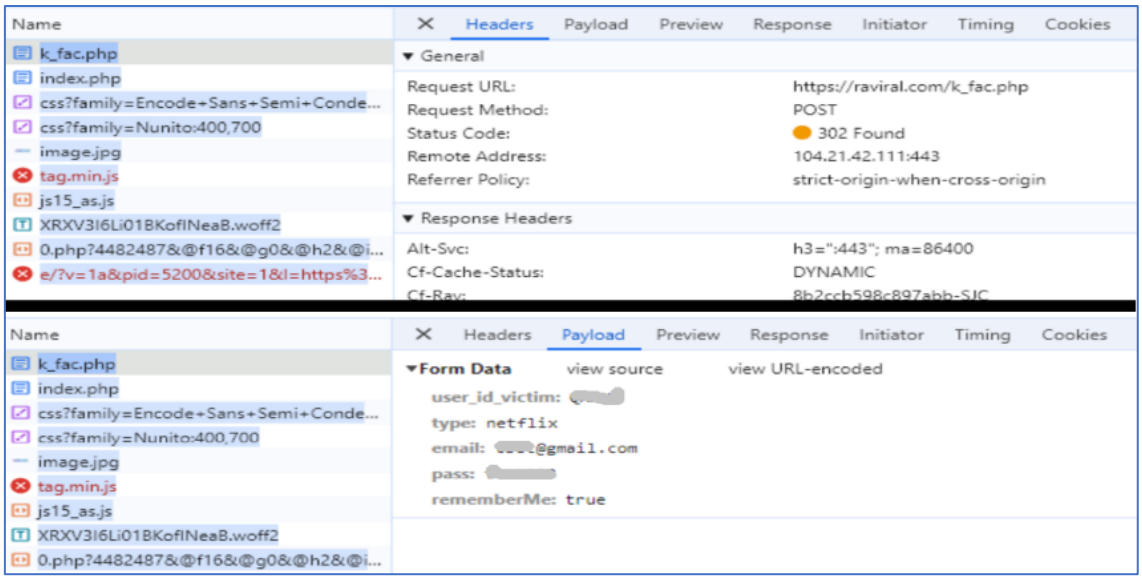


Figura 4 – Credenciais exfiltradas para o endpoint raviral[.]com/k_fac.php controladas pelo Sniper Dz.

Ao enviar credenciais para uma infraestrutura centralizada que controla, o Sniper Dz consegue reunir dados de todas as vítimas de seus clientes, mesmo aquelas que caíram em modelos de phishing hospedados em servidores diferentes. Para os phishers, as credenciais roubadas são apresentadas em um painel de administração. Esse painel exibe detalhes como nome de usuário, senha, nome do modelo de phishing, data e hora da exfiltração, endereço IP e país da vítima.

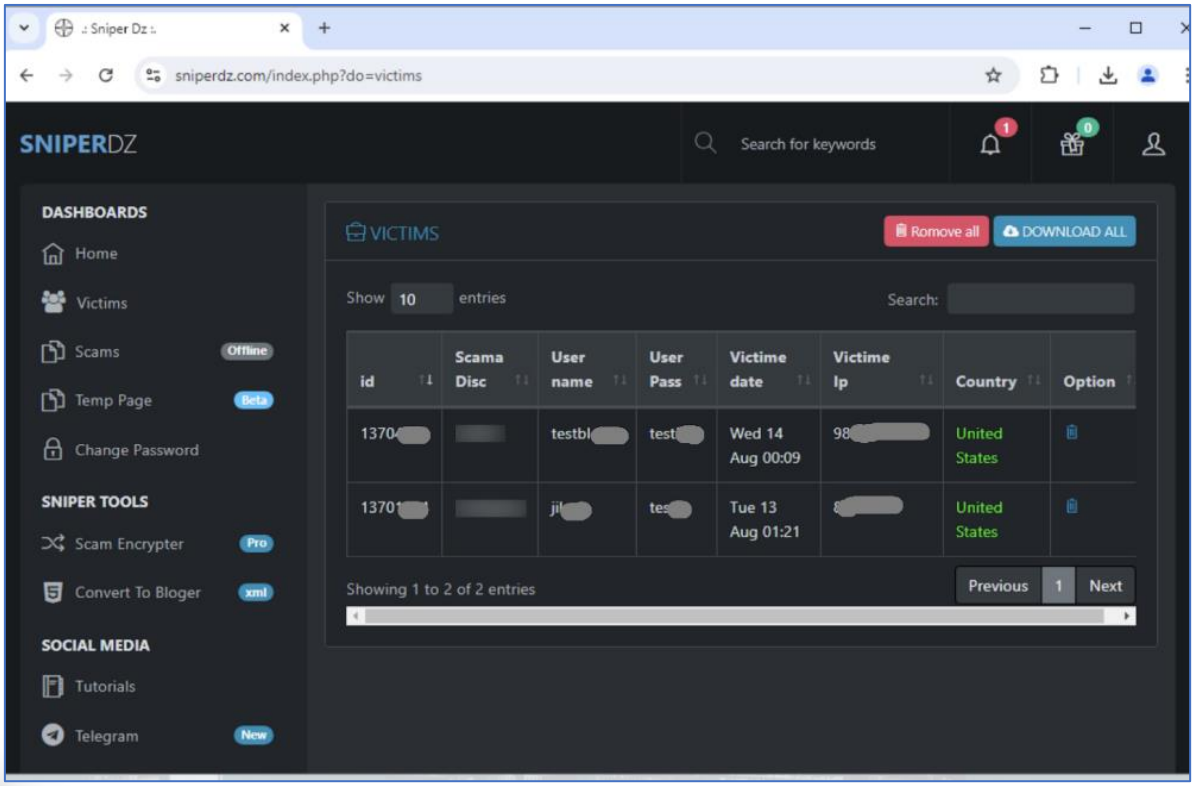


Figura 5 – Painel de administração mostrando credenciais roubadas da vítima.

O Sniper Dz manteve-se ativo ao longo de todo esse período. Apesar de seu pico de atividade ter ocorrido no final de 2023, notamos um aumento significativo a partir de julho de 2024. Geograficamente, esses sites de phishing visam principalmente usuários da web nos EUA. Esse grupo pode ter milhares de phishers como clientes, utilizando sua plataforma PhaaS para realizar ataques de phishing. Por exemplo, o Sniper Dz gerencia um canal no Telegram (**t[.]me/JokerDzV2**) para suporte ao cliente, que contava com 7.156 assinantes em agosto de 2024.

Figura 6 – Canal do Telegram t[.]me/JokerDzV2 para Sniper Dz.

As páginas de phishing do Sniper Dz podem direcionar os usuários para outros sites sob seu controle, como **raviral[.]com**, após a vítima fornecer suas credenciais de login. Os invasores enchem o site raviral[.]com com anúncios maliciosos e distribuem bloqueadores de anúncios suspeitos, rotulados como PUA/PUP, além de outras extensões de navegador. Em alguns testes, o site iniciou o download de um instalador para um navegador malicioso chamado **Artificus**. O Artificus é conhecido por seu comportamento invasivo e também foi relatado que ele é distribuído por anunciantes maliciosos.

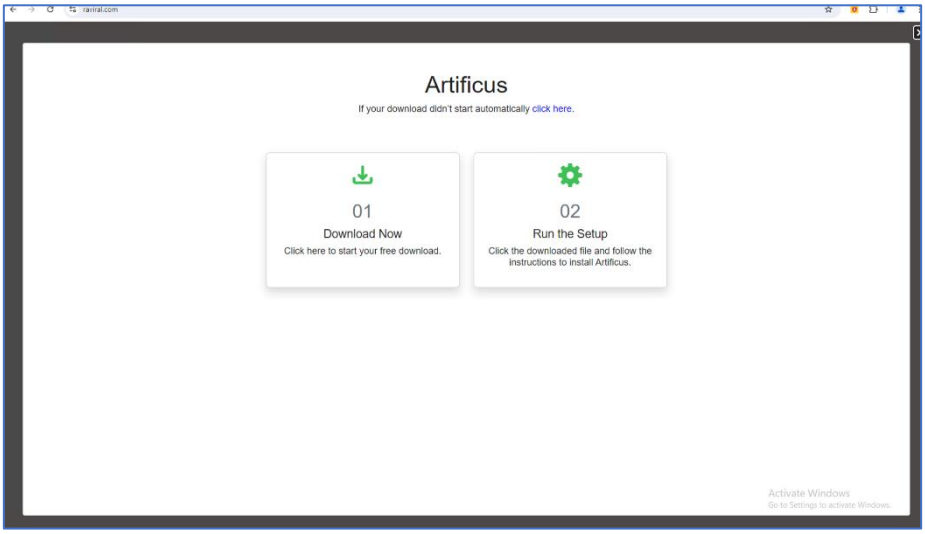


Figura 7 – Página da Web distribuindo um navegador desonesto chamado Artificus.

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:

Verifique os e-mails com atenção

- Sempre examine os e-mails cuidadosamente antes de clicar em links ou baixar anexos. Verifique o remetente e procure por erros gramaticais ou de ortografia.

Não forneça informações pessoais

- Nunca compartilhe informações pessoais ou financeiras em resposta a e-mails não solicitados. Bancos e instituições legítimas não pedem essas informações por e-mail.

Use autenticação de dois fatores (2FA)

- Ative a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança, exigindo um segundo fator além da senha.

Mantenha seu software atualizado

- Certifique-se de que seu sistema operacional, navegador e outros softwares estejam sempre atualizados para proteger contra vulnerabilidades conhecidas.

Utilize senhas fortes e únicas

- Crie senhas complexas e diferentes para cada conta. Considere usar um gerenciador de senhas para ajudar a gerenciar suas credenciais.

Eduque-se sobre phishing

- Mantenha-se informado sobre as táticas de phishing mais recentes e como identificá-las. Quanto mais você souber, melhor poderá se proteger.

Denuncie tentativas de phishing

- Se você receber um e-mail suspeito, denuncie-o ao seu provedor de e-mail ou à instituição que o e-mail finge representar. Isso ajuda a combater os criminosos e a proteger outras pessoas.

4 INDICADORES DE COMPROMETIMENTO (IOC)

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	sniperdz.com raviral[.]com automaticgiveaway[.]000webhostapp[.]com Climbing-green-botany[.]glitch[.]me facebookbusiness0078[.]blogspot.be free-fire-reward-garena-bd-nepazl[.]epizy[.]com proxymesh[.]com

Tabela 1 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Unit42**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH