



heimdall
security research

A DIVISION OF ISH

TLP:CLEAR



Utilização do DNSSEC para proteger contra ataques *DNS Spoofing*

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

<https://twitter.com/heimdallish>



heimdall
security research
A DIVISION OF ISH

heimdall
security research

Edit profile

Heimdall Security Research
@heimdallish

A conta oficial do grupo de Threat Intelligence da ISH. Conheça mais do que fazemos aqui: ish.com.br/vision/

ish.com.br Joined October 2021

Heimdall Security Research @heimdallish · 3h

A CISA adicionou seis novos exploits ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas, com base em evidências de exploração ativa. Esses tipos de vulnerabilidades são um vetor de ataque frequente para agentes cibernéticos mal-intencionados.

CISA:
bit.ly/3dphOEt



Heimdall Security Research @heimdallish · Sep 14

Hoje é o Patch Tuesday de setembro de 2022 da Microsoft, e com ele vem correções para uma vulnerabilidade do Windows explorada ativamente e um total de 63 falhas.

Bleeping Computer:
bit.ly/3BEdEII



Heimdall Security Research @heimdallish · Sep 15

Em nosso Boletim Mensal, acompanhe os endereços IP ofensores, as principais ameaças, entre elas: Malwares, Cryptojacking, SSH Brute Force e TOR Proxy, que afetaram o Brasil no último mês e veja nossas recomendações para proteger sua empresa.

Boletim:
bit.ly/3dfvNww



Heimdall Security Research @heimdallish · Sep 9

Boletim semanal: Uma das principais ameaças da atualidade são os Malwares do tipo Stealer. Neste boletim trazemos informações e IoCs mostrando como você pode proteger sua empresa deste ataque.

Acesso nosso boletim:
bit.ly/3L317ev



Heimdall Security Research @heimdallish · Aug 5

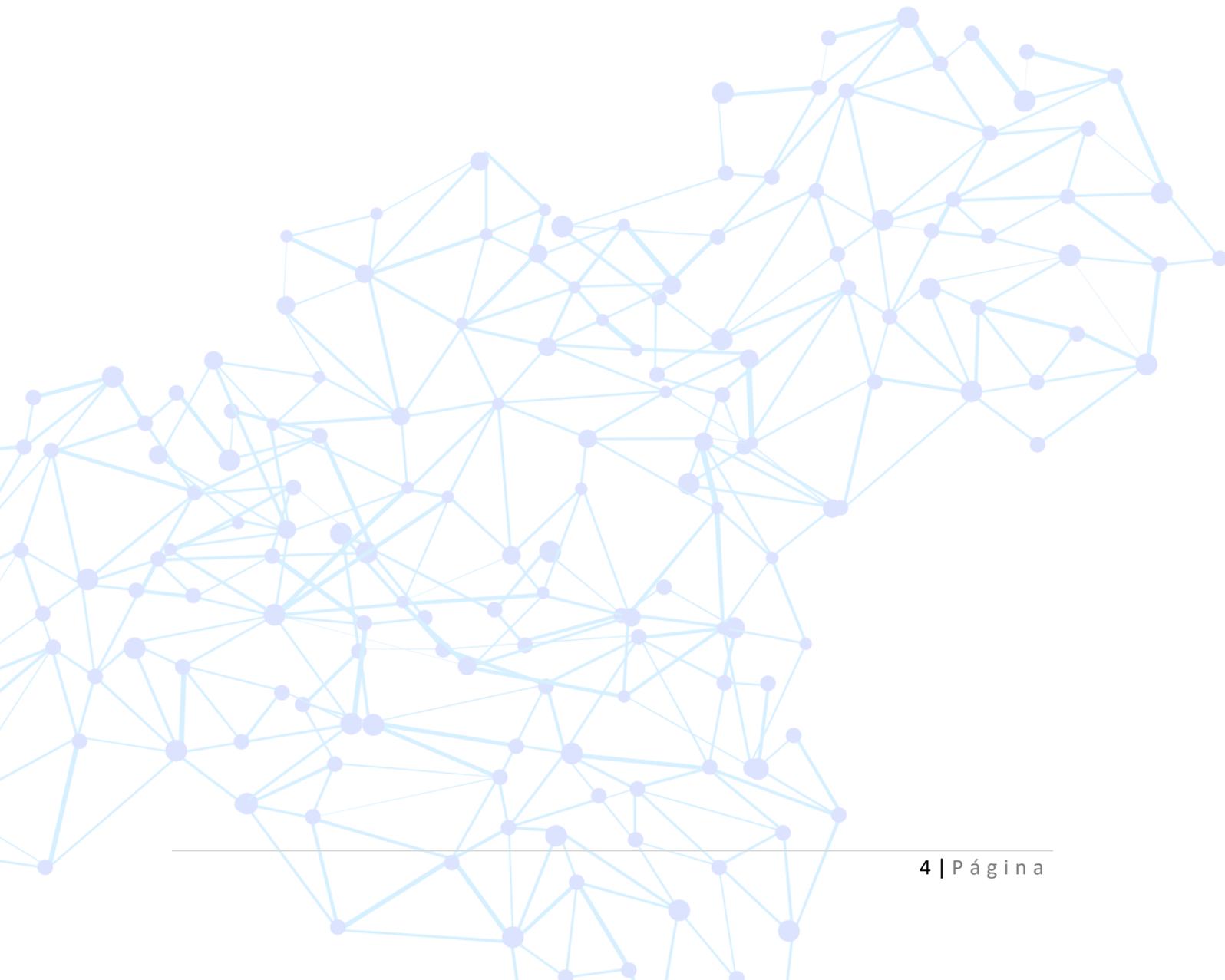
Em nosso Boletim Mensal, apresentamos análises de diversas fontes e, principalmente, da nossa plataforma de inteligência: Heimdall Global Threat Intelligence by ISH.

Acesso nosso material:
d335luupugsy2.cloudfront.net/cms%2Ffiles%2F...



Sumário

1	DNS.....	5
2	DNSSEC.....	6
3	Como configurar o DNSSEC em seu domínio.....	7
4	Recomendações.....	9
5	Referência.....	10



1 DNS

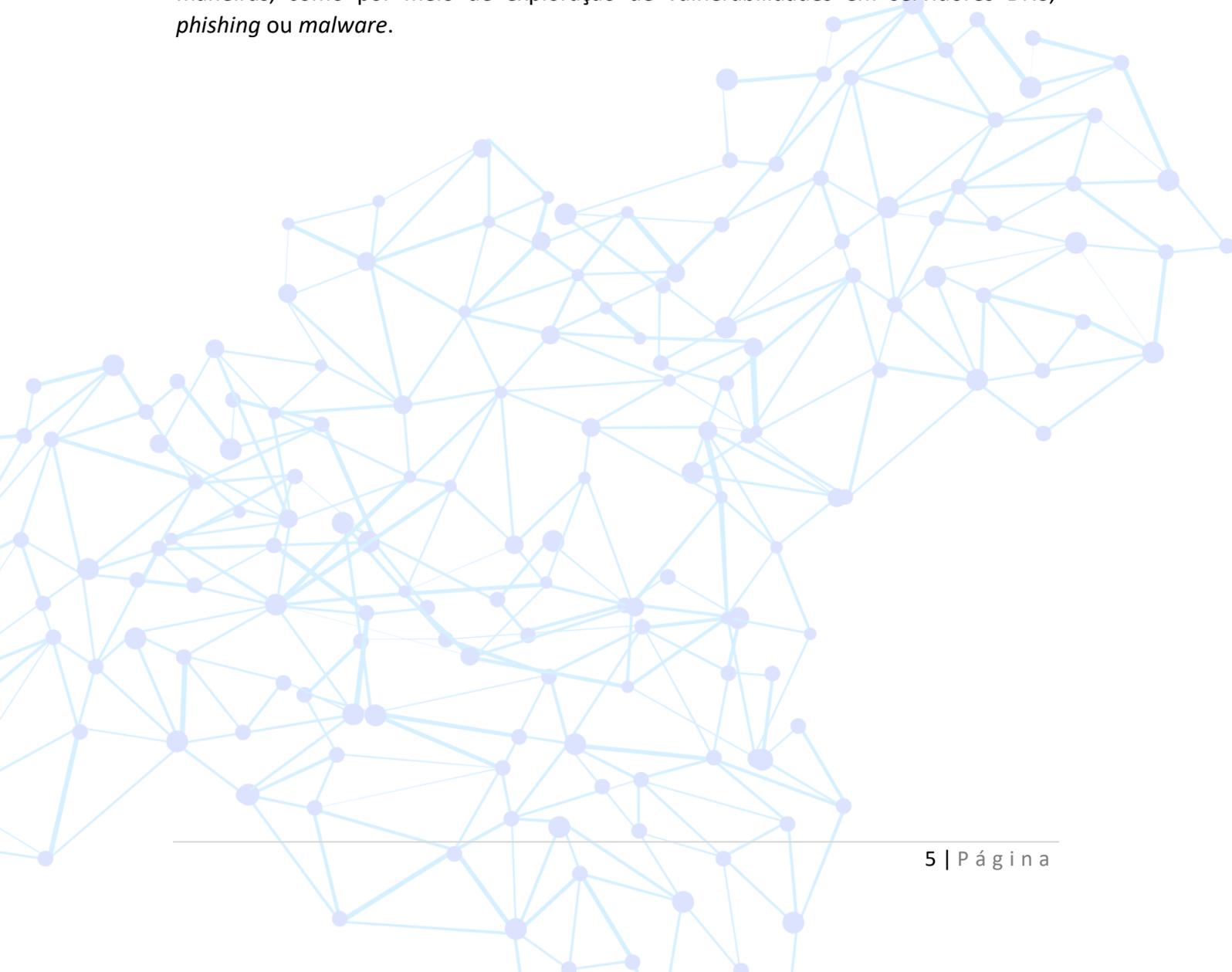
DNS (Sistema de Nomes de Domínio) é um protocolo utilizado na internet para converter nomes de domínios em endereços IP.

Os nomes de domínios são mais fáceis de lembrar, por exemplo, o nome de domínio “ish.com.br”, do que o endereço IP correspondente. No entanto, os dispositivos na Internet usam endereços IP para se comunicarem entre si, e o DNS acaba atuando como um catálogo de nomes de domínios que são vinculados a endereços de IP.

Quando um usuário digita um nome de domínio em seu navegador, o navegador envia a solicitação para um servidor DNS com o objetivo de traduzir o nome de domínio em um endereço IP.

Um exemplo de ataque cibernético envolvendo o DNS é o conhecido “ataque de envenenamento de cache DNS” ou “DNS Spoofing”, no qual um ator malicioso altera ou corrompe os dados do *cache* DNS de um servidor ou cliente DNS, direcionando os usuários para um *site* malicioso em vez do *site* legítimo.

Os ataques de envenenamento de cache DNS podem ser realizados de várias maneiras, como por meio de exploração de vulnerabilidades em servidores DNS, *phishing* ou *malware*.



2 DNSSEC

O DNSSEC é uma extensão de segurança do Sistema de Nomes de Domínio (DNS) que possui o foco em proteger as consultas de DNS contra ataques de falsificação de dados.

Lembrando que o DNS é responsável por traduzir nomes de domínio em endereços IP, permitindo que os usuários acessem *sites* e serviços na Internet. Porém o DNS é vulnerável a ataques que podem redirecionar os usuários para *sites* maliciosos ou interceptar informações confidenciais.

DNSSEC utiliza criptografia de chave pública para assinar digitalmente os registros DNS, garantindo que eles não tenham sido alterados ou falsificados durante a transmissão. Isso acaba permitindo que os usuários verifiquem a autenticidade dos dados do DNS, garantindo que as consultas sejam redirecionadas apenas para os *sites* e serviços corretos e que a segurança e a privacidade dos usuários sejam preservadas.

3 COMO CONFIGURAR O DNSSEC EM SEU DOMÍNIO

Listamos abaixo algumas dicas para que sejam implantadas o DNSSEC no **servidor autoritativo** para determinado domínio, lembrando ainda que todas as operações serão executadas no servidor principal (*Master*):

- Servidor Autoritativo: Ao receber requisições de resolução de nomes, responde um endereço, caso possua; uma referência, caso conheça o caminho da resolução; ou uma negação, caso não conheça o caminho.
- Servidor Recursivo: Ao receber requisições de resolução de nomes, faz requisições para os **servidores autoritativos** e, conforme a resposta recebida dos mesmos, continua a realizar requisições para outros **servidores autoritativos** até obter a resposta satisfatória.

Requisitos:

- Bind 9.7 que poderá ser obtido em <https://www.isc.org/download/>

Criação da Chaves

- `dnssec-keygen -r /dev/urandom -f KSK <domínio>`

O comando acima irá gerar dois arquivos com extensões **.key** e **.private**.

Assinar o domínio (arquivos de zona)

- `dnssec-segnzone -S -z -o <domínio> <db.domínio>`

Aqui, o **<domínio>** deve ser substituído pelo nome de domínio e **<db.domínio>** pelo nome do arquivo de zona.

O comando irá gerar um novo arquivo de zona com a extensão **.signed**. Lembrando que o período de validade padrão da assinatura digital é de 30 dias.

Alteração da referência para o arquivo de zona

```
zone "<domínio>" {  
    type master;  
    file "/etc/namedb/<db.domínio>.signed";  
    ...  
};
```

O **<domínio>** deve ser substituído pelo nome do domínio e **<db.domínio>** deve ser substituído pelo nome do arquivo de zona.

Em sequência, será necessário **reiniciar o Bind**.

Adicionar o DS no *site* do Registro.BR

É necessário copiar os dados de **KeyTag** e **Digest** do arquivo **dsset-<domínio>** para a interface no *site* do Registro.br.

Poderá ser utilizado o comando:

```
• cat dsset-<domínio> | head -1
```

Tendo a saída:

```
<domínio> IN DS 10000 5 1 1AS6DA45AD45ASD56ADA1D2E54T
```

Local para inserir no *site* do Registro.br

DNSSEC

Record	KeyTag	Digest
DS 1	<input type="text"/>	<input type="text"/>
DS 2	<input type="text"/>	<input type="text"/>

Na sequência, é necessário **aguardar a nova publicação** no *site* do Registro.br, na qual as publicações ocorrem a **cada 30 minutos**, podendo, em caso de alteração de dados de um domínio, passar um período de transição que poderá durar até 24 horas.

Por fim, é necessário reassinar a zona antes que as assinaturas expirem, incrementar o seral (*record SOA*) do arquivo de zona original e reassinar a zona utilizando o comando **dnssec-signzone**.

4 RECOMENDAÇÕES

A ISH Tecnologia apresenta, além das recomendações da implantação do DNSSEC, as medidas de segurança abaixo que poderão ser adotadas:

- Utilização de DNS confiáveis, adotando servidores DNS confiáveis e de boa reputação.
- Implementação da DNSSEC, conforme mencionado na seção própria deste documento, mencionando a utilização da medida contra ataques de envenenamento de DNS.
- Atualização de *softwares* e sistemas, sendo necessário sempre a atualização constante visando corrigir vulnerabilidades caso existam.
- Utilização de senhas fortes, troca periódica das mesmas e utilização de 2FA (Múltiplo Fator de Autenticação).
- Utilização de conexões seguras, como o uso do HTTPS, que ajuda a proteger contra ataques de interceptação de dados.

5 REFERÊNCIA

- Heimdall *by* ISH Tecnologia
- Registro.Br – [DNS e DNSSEC](#)
- CloudFlare [about](#) DNS

