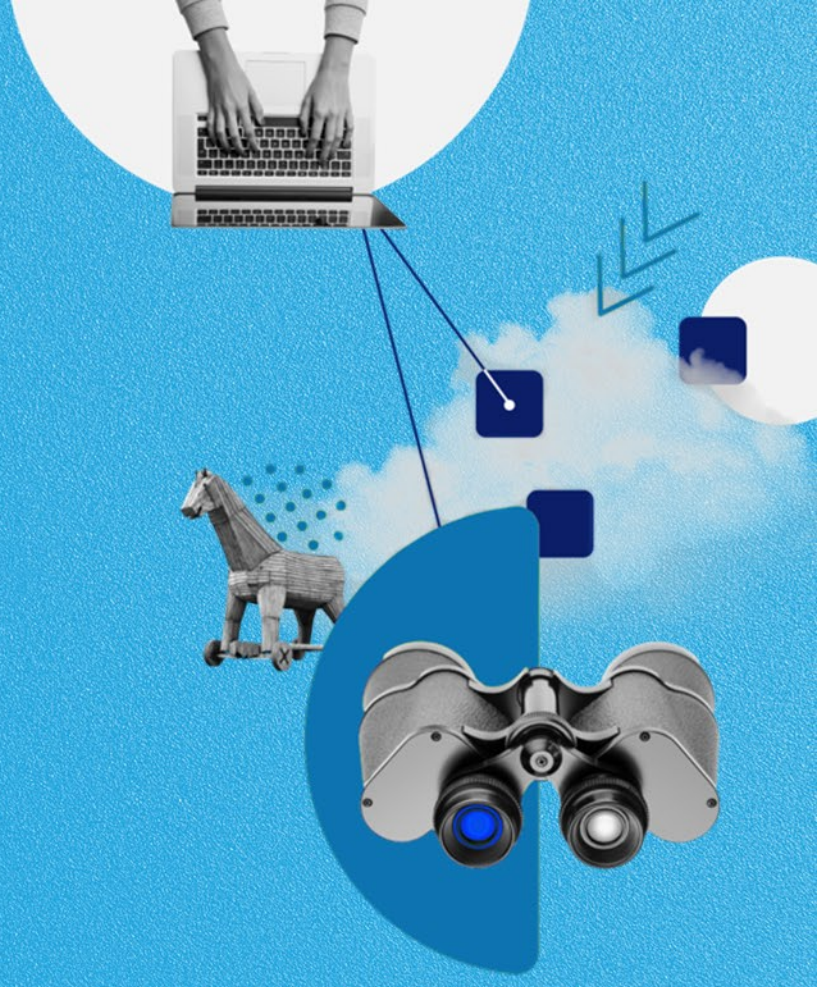
Mais que tecnologia

# DNS: o salvador desconhecido de ameaças.

O guardião que nos leva para onde queremos ir na rede, e desempenha um papel crucial na segurança, velocidade e confiabilidade da nossa jornada virtual.

SAIBA MAIS



# A nova realidade de hoje

A mudança que leva a gaps na visibilidade e proteção

À medida que aplicações, dados e uma série de recursos migram para a nuvem, as redes se reconfiguram rapidamente para atender a essa demanda crescente. Simultaneamente, o acesso direto à internet se estabelece como uma prática cada vez mais comum e fundamental.

Acentuada pela recente necessidade, a adoção do trabalho remoto se consolida, redefinindo os padrões tradicionais de trabalho. No entanto, essa transformação não vem sem desafios, especialmente no âmbito da segurança, que se torna notavelmente mais complexa de gerenciar, exigindo abordagens inovadoras para proteger dados e sistemas em meio a essa evolução tecnológica.

## As empresas estão sob ataques!

Empresas de diversos portes lidam com os mesmos desafios.

**66%**

de pequenas empresas já sofreram um **ataque cibernético**

**63%**

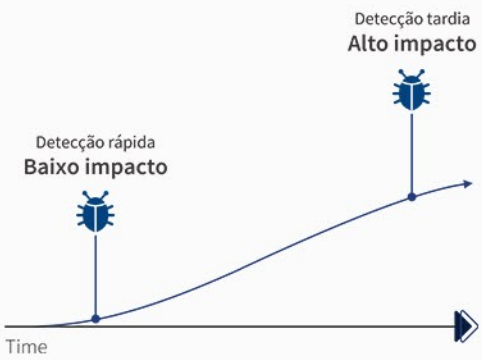
de pequenos negócios já sofreram uma **violação de dados**

Em média, na indústria, são necessários

**280 dias**

**para identificar uma violação**

**207** dias **para detecção** + **73** dias **para conter**



# A segurança do DNS desempenha um papel vital em todo programa de segurança completo.

Sua importância é inegável devido a alguns fatores-chave:

**Útil**
A proteção do DNS é essencial, pois evita ameaças no nível mais fundamental da conectividade online.

**Bom custo-benefício**
Investir em segurança DNS oferece vantagens substanciais em relação aos custos associados a possíveis violações de segurança.

**Simples de implantar**
A implementação de medidas de segurança DNS é relativamente direta, contribuindo para uma postura mais segura sem complexidade excessiva.

**Melhora os tempos de detecção e resposta**
A segurança DNS agiliza a detecção de ameaças e a reação a elas, reforçando a postura de defesa cibernética de uma organização.

# Como o DNS potencializa sua segurança online?

**Ele é o primeiro passo para acessar a internet,** convertendo nomes de domínio em endereços IP. Isso acontece antes da execução de arquivos e conexões, permitindo a filtragem e encaminhamento seguro do tráfego. Como quase todos os dispositivos usam e dereços IP, controlar o DNS é essencial para implementar medidas de segurança, **prevenindo ataques como phishing e malware** desde o início.

# Navegação é o segundo **vetor de ataque**

**90%** dos malwares usam protocolo DNS para promover ataques

| | NAME | Initial Access Vector | Encryption | C2 (IP/DNS) | Exfiltration | Payment | Focus OS |
|---|---|---|---|---|---|---|---|
| | WannaCry (2017) | Exploit (SMBv1) | AES-128/RSA-2048 | DNS | N/A | BTC - TOR | Windows Only |
| | Sodinokibi (2019) REvil RaaS | Exploit (Oracle WebLogic) 0-day, phishing | AES/Salsa20 | DNS/IP | March, 2020 > SSH over 443, Cloud Storage | BTC - DNS (TOR) | Unix, ESXi, NAS, Windows |
| | Hades (2020) Former WastedLocker | Stolen VPN/RDP credentials, SocGholish via Chrome updt | AES-256/RSA-2048 | DNS/IP | 7zip > mega.nz | BTC - TOX (TOR) | Windows |
| "Ransomware Cartel" | Maze RaaS (2019) Sekhmet > Egregor | Exploit Kits, spear-phishing, Valid Accounts, RDP brute-force | ChaCha20/RSA-2048 | IP | WinsSCP - FTP | BTC – DNS & TOR | Windows |
| "Ransomware Cartel" | Babuk RaaS (2021) | Exploit (MS Exchange) | ChaCha8/AES-256 | DNS/IP | Mega, GDrive | XMR - Email | Cross-platform, Win, ESXi, Unix |
| "Ransomware Cartel" | Conti RaaS (2019) old Ryuk (2018) | Spear-phishing, valid accounts, malicious links | AES-256/RSA-4096 | DNS/IP | Rclone > Mega | BTC - TOR & Email | Windows |
| "Ransomware Cartel" | RagnarLocker (2020) Viking Spider APT | Valid accounts, brute-force, insiders | Salsa20/RSA-2048 | DNS/IP | SSH over 443 | BTC - TOR | Windows |
| | Lockbit 2.0 RaaS (2021) | Insiders, Fortigate Vuln, phishing | AES-128/RSA-2048 | DNS/IP | StealBIT 2.0, Rclone > Mega | BTC - DNS | Windows, Linux, ESXi |
| | DarkSide RaaS (2020) REvil former affiliates | Exploit (ESXi), valid accounts | Salsa20/RSA-1024 | DNS/IP | MEGASync, GoToAssist | BTC - TOR | Windows, Linux |

Most active in 2022

*Most variants, (apart from Wannacry), uses multiple vectors to deploy the initial payload, mostly phishing or malicious links.

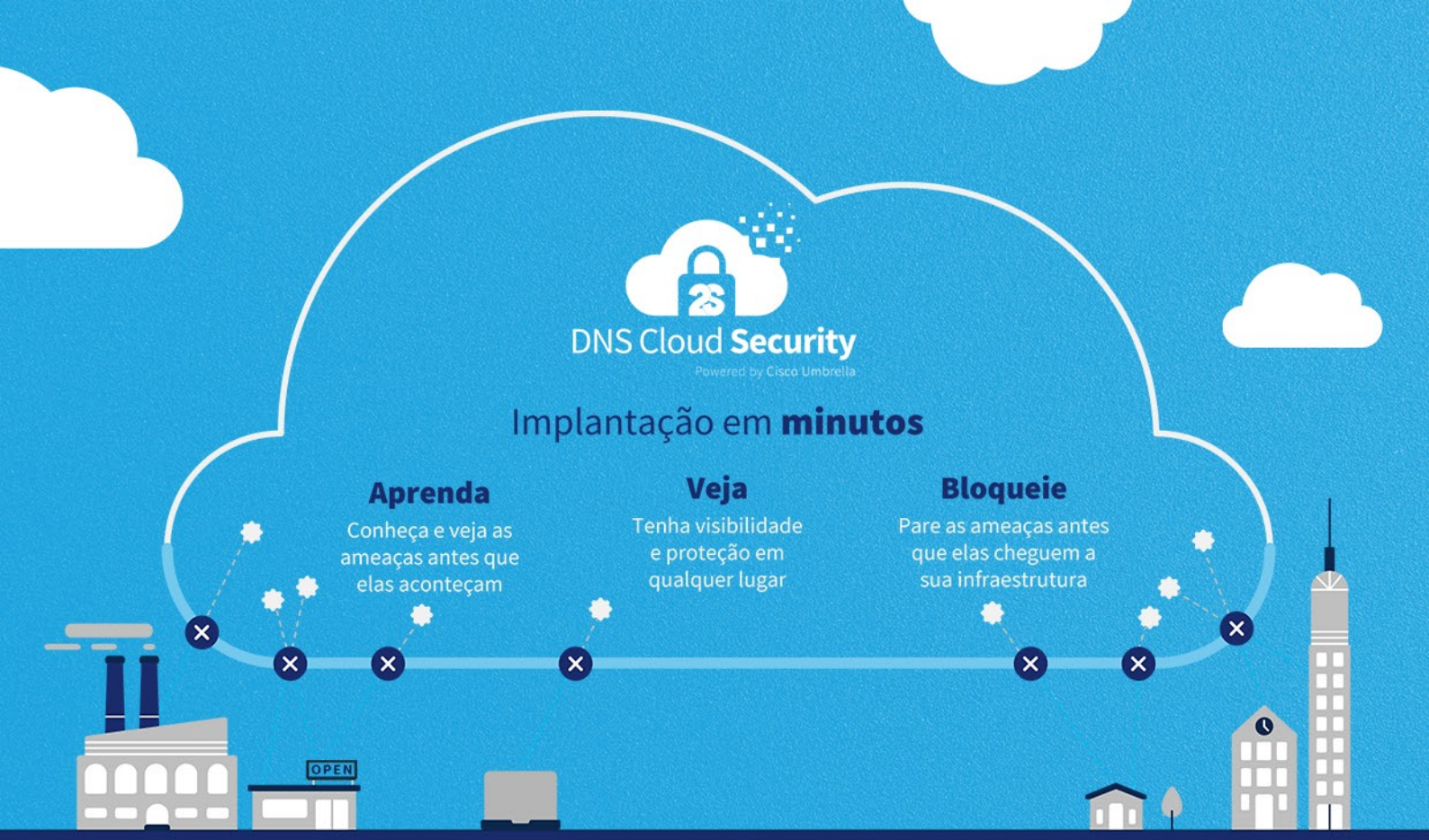
Red color = "officially closed"

{ = relations

Talos direct contribution

Decryption key available

*"The average mitigation cost of a ransomware attack was **$1.85 million**,"*
*"…**21 days of downtime** on average, followed a ransomware attack."*




## Com o **2S DNS Cloud Security** você terá:

- Ampla proteção na camada de navegação e aplicação em nuvem, garantindo segurança e visibilidade para usuários em diversos contextos;
- Defesa abrangente com bloqueio de domínios ligados a phishing, malwares, botnets e criptomineração, onde quer que os usuários estejam;
- Expertise na gestão, com um time de especialistas gerenciando todo o ambiente, te garantindo maior segurança e eficiência.

## E mais...

- Licenciamento e serviços de acordo com as necessidades do seu ambiente.
- Flexibilidade de licenciamento (upsell e downsell).
- Vigência de contrato de acordo com a sua necessidade.
- Visão ampla do ambiente com relatórios consultivos.

# Quais são os desafios da segurança?

**Prioridades**
75% sentem que mais que precisam de mais segurança dentro de sua organização

**Riscos**
41% se preocupam com violações de dados

**Usuários Remotos**
48% comprometidos por ataques direcionados

## Transforme o seu negócio com a **nossa ajuda!**

Entre em contato com a nossa equipe de profissionais certificados e descubra como a tecnologia pode impulsionar o seu negócio.

DNS Cloud Security
Powered by Cisco Umbrella