

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgib.br

Comitê Gestor da
Internet no Brasil



registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

nic.br cgi.br

ceptro.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is symmetrical and fills the entire frame.

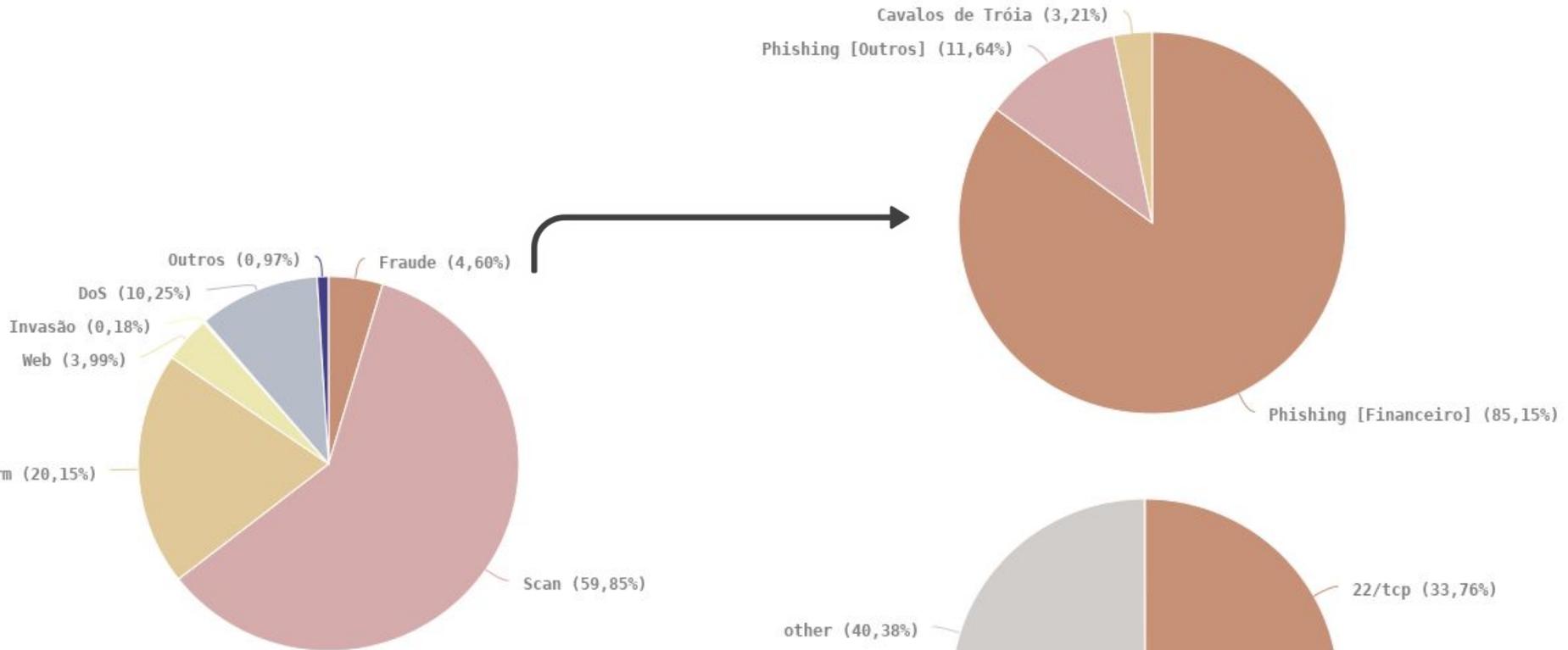
Hardening de equipamentos

ceptro.br nic.br egi.br

Atividades nos Honeypots Distribuídos

- **Força bruta de senhas (usado por malwares de IoT e para invasão de servidores e roteadores):**
 - Telnet (23/TCP)
 - SSH (22/TCP)
 - Outras TCP (2323, 23231, 2222)
- **Protocolos explorados pela *botnet* Mirai, na variante para CPEs (roteadores de banda larga)**
 - TCP: 7547, 5555, 37777, 6789, 81, 37215, 52869
- **Busca por protocolos que permitam amplificação**
 - UDP: DNS, NTP, SSDP, SNMP, Chargen, Netbios, Quotd, mDNS, LDAP

Ataques dentro da Internet



Scan

Portas 22 e 23: força bruta de senhas de servidores, CPEs e IoT

Alteração de DNS para fraudes

Comprometidos

via força bruta de senhas (geralmente via telnet)

explorando vulnerabilidades

via ataques CSRF, através de *iFrames* com *JavaScripts* maliciosos

- Colocados em *sites* legítimos comprometidos pelos fraudadores

Objetivos dos ataques

alterar a configuração de DNS para que consultem servidores sob controle dos atacantes

servidores DNS maliciosos hospedados em serviços de *hosting/cloud*

- casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

O que é Hardening?

- **É um procedimento para:**
 - **Analisar vulnerabilidades.**
 - **Mapear as ameaças.**
 - **Minimizar/Mitigar riscos.**
 - **Aplicar medidas corretivas.**
- **Proteger**
 - **Ataques vindos de terceiros**
 - **Seus equipamentos façam ataques em outros.**

Recomendações para Autenticação

● Básico

- **Criar um usuário para cada funcionário.**
 - Desative contas antigas e inutilizadas.
- **Não deixe os funcionários utilizarem a mesma conta padrão de administração do sistema!!!**
 - Guarde o acesso padrão somente para backup e emergências.
- **Não permita senhas fracas de acesso!**
 - O CERT.br possui fascículo sobre recomendações de senhas!
 - <https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf>
- **Não armazena sua senhas em texto puro!**
 - Use uma função hash (PBKDF2, Bcrypt, Scrypt e Argon2)

Recomendações para Autenticação

● Avançado

- Aplique técnicas de **autenticação em 2 fatores**.
 - Coisas que eu **sei!**
 - Ex: Senhas.
 - Coisas que eu **sou!**
 - Ex: Biometria.
 - Coisas que eu **posso!**
 - Ex: Chave.
- Usar **2 coisas do mesmo tipo não caracteriza autenticação em 2 fatores**.
 - Não vale colocar 2 senhas!
- O CERT.br possui fascículo
 - <https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf>

Recomendações para Autorização

● Básico

- Cada usuário deve ter permissão para acessar o roteador de acordo com o seu trabalho.
 - Não forneça acesso administrador para todos o seus usuários
 - Pense no que seu estagiário/agente malicioso poderia fazer no seu sistema.
- Em alguns sistemas pode se criar grupos de privilégios.
- Em alguns sistemas é possível escalar privilégios.

Recomendações para Auditoria

● Básico

- Manter um **registro de cada usuário com suas respectivas permissões**.
- **Registrar as ações** de cada usuário no sistema.
- Operar com **nível de criticidade** nos registros.
 - Informativo
 - Aviso
 - Crítico
- **Tipos de registros**
 - Documentos.
 - Logs.
 - Backups de configuração.
- **É importante** guardar a informação com a **data e hora certa!**

Recomendações para Acesso

● Básico

- **Não utilize protocolos inseguros** para acesso.
- **Desative-os** se eles estiverem operando.
- **Se for o único meio** de acesso a máquina, **restrinja** o alcance para somente ser utilizada pela **interface de gerencia** (uma rede apartada e protegida)
- Exemplos:
 - Telnet
 - FTP
 - HTTP
 - MAC-telnet
 - Winbox

Recomendações para Acesso

- **Básico**

- Utilize preferencialmente protocolos com mensagens **criptografadas!**
 - SSH
 - HTTPS
 - SFTP
 - Winbox (secure mode)
- Lembre-se de utilizar a última versão estável disponível
 - SSH v2 com strong crypto

Recomendações para Acesso

- **Básico**

- Adicione uma **mensagem de login**.
- **Existem governos que exigem** essas mensagens para o **âmbito legal**.
- Exemplo:
 - “Roteador pertencente a empresa X, acessos não autorizados serão monitorados, investigados e entregues às autoridades responsáveis”

Recomendações para Acesso

- **Básico**

- Mudar a porta padrão do serviço de acesso.
- Bloquear acesso a porta padrão.
- Não é bem uma proteção mas pode ajudar contra um ataque simples que procura portas padrão.

Recomendações para Acesso

● Básico

- Armazene informações para auditoria.
- Log de ações.
 - Identifica comandos indevidos
- Log de tentativas de acesso.
 - Identifica ataque de força bruta
 - Identifica ataque de negação de serviço
 - Identifica tentativa de roubo de informações
- É possível criar políticas de mitigação de ataque.
 - Filtros
 - Blackhole
- Utilize a hora legal brasileira com NTP.br

Recomendações para Acesso

- **Básico**

- Não permita acesso por todas as interfaces.
- Escolha uma interface de loopback para os seus serviços
 - São mais estáveis.
 - Não sofrem com variações no link.
 - Caso uma interface física fique indisponível os protocolos de roteamento procuram um novo caminho.
- Faça essa interface parte da sua rede de gerência

Recomendações para Acesso

● Básico

- Forçar o logout depois de um tempo de inatividade.
 - Isso evita que alguém use sua máquina em seu período ausente.
 - Isso evita que um atacante monitore o seu tempo de inatividade para tomar controle da máquina.
- Forçar o logout depois de se desconectar o cabo.
 - Isso evita que alguém reconecte o cabo e use o seu login.

Recomendações para Acesso

- **Avançado**

- Port Knocking

- Nenhuma porta aparece aberta no scan
- Diminui a superfície de ataques
- Para acessar um serviço
 - Testar uma sequência de portas fechadas.
 - Configurar a mudança de regras de Firewall dinamicamente.
 - Conectar na porta desejada.

Recomendações para Logs

- **Básico**

- Configure logs com diferentes níveis de criticidade.
- Evite gerenciar logs dentro dos roteadores.
 - Quanto mais funções o roteador tiver que fazer, menos processamento será utilizado para rotear pacotes.
- Envie de maneira segura os logs para uma outra máquina.
 - Algum agente malicioso pode interceptar
- Guarde de maneira segura seus logs.
 - Eles podem te ajudar num processo judicial.
- Mantenha a hora correta com NTP.

Recomendações para o Sistema

● Básico

- Desative todas as interfaces não utilizadas.
 - interfaces que não possuem cabos conectados.
- Desative todas os serviços não utilizadas, inseguros e que podem ser utilizados para ataques de amplificação.
 - Testador de banda.
 - DNS recursivo.
 - Servidor NTP.
- Remova ou desative os pacotes de funções extras não utilizados.
 - Pacote wireless.

Recomendações para o Sistema

● Básico

- Desabilite protocolos de descoberta de vizinhança
 - CDP
 - MNDP
 - LLDP
- Facilita para o atacante descobrir o tipo do seu roteador.
- Inunda a rede com mensagens desnecessárias.
- Tome cuidado com o IPV6
 - Descoberta de vizinhança é essencial.
 - Sem ela, nada funciona.

Recomendações para o Sistema

- **Básico**

- Mantenha o sistema sempre atualizado na versão estável.
 - Incluindo seus pacotes.
- Aplique todos os patches de segurança.
- Procure testar as atualizações, antes de aplicar em produção, num ambiente controlado.
 - Emulador.
 - Simulador.

Recomendações para Configurações

● Básico

- Mantenha sempre um backup atualizado das configurações atuais.
- Envie de maneira segura esse backup para uma outra máquina.
 - Email criptografado
 - SCP
 - SFTP
- Guarde esse backup numa máquina segura.
- Lembre, o operacional da sua empresa está guardado lá!
 - hashes de senhas podem ser quebrados!

Recomendações para Configurações

- **Básico**

- Mantenha um script de hardening de roteadores.
- Assim ao comprar um novo roteador, você saberá as políticas mínimas de segurança que precisam ser aplicadas.
- Mantenha esse script atualizado. Cada nova política precisa ser agregada ao script.

Dúvidas?



Patrocínio Super Like



Apoio de Mídia



Obrigado !!!

nic.br egi.br

www.nic.br | www.cgi.br