Bacula Contra o Ransomware!
Campus Party - 2021

www.bacula.lat | heitor@bacula.com.br

Bacula LatAm

- Sede no Brasil, subsidiária nos Estados Unidos (FL)
- Distribuidor exclusivo da Bacula Systems LatAm e Brasil
- Nacionaliza licenças e serviços
- Equipe certificada pelo desenvolvedor
- Missão: *Fornecer o melhor e mais acessível Software de Backup e Restauração de Dados*

TERESINA
SHOPPING

MINISTÉRIO PÚBLICO
ESTADO DE RORAIMA

MINISTÉRIO PÚBLICO
DO ESTADO DA PARAÍBA

CÂMARA MUNICIPAL DE
CAMPINAS

PREFEITURA DE
APARECIDA
Fazendo cada vez mais

- Udemy.com <http://www.bacula.lat/community/treinamento-bacula-ed/>
- YouTube <https://www.youtube.com/user/heitorfaria>
- Livro Bacula 4a Edição Brasport
- Telegram: @baculabr
- Meu contato: <heitor@bacula.com.br>
- Nosso site <http://www.bacula.lat/>

- Ransomware
- Backups
- Bacula
- Linux
- Regra 3-2-1
- Hardening
- Perguntas e Respostas

Ransomware

De acordo com a Kaspersky [1], os Trojans Ransomware são um tipo de malware projetado para extorquir dinheiro de uma vítima. Em geral, ele vai exigir um pagamento em troca, prometendo reverter as alterações que o vírus trojan fez para o computador da vítima. Essas alterações podem incluir:

1. Criptografia de dados armazenados nas máquinas, para que as informações não possam mais ser acessadas.
2. Bloquear o acesso normal aos sistemas operacionais.

Ransomware

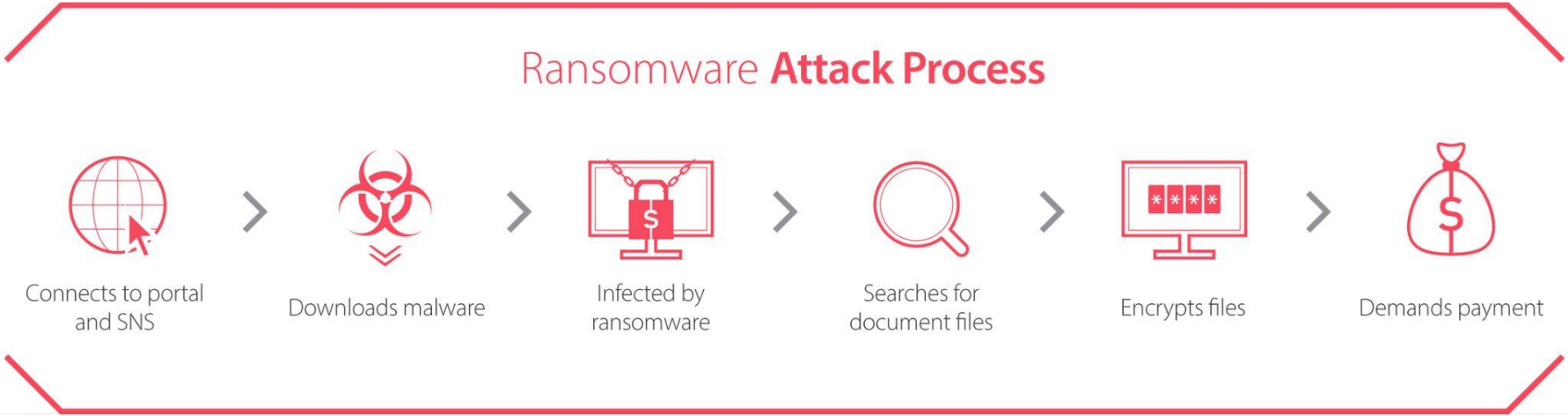


Figura 1. Processo de Ataque Ransomware

Ransomware

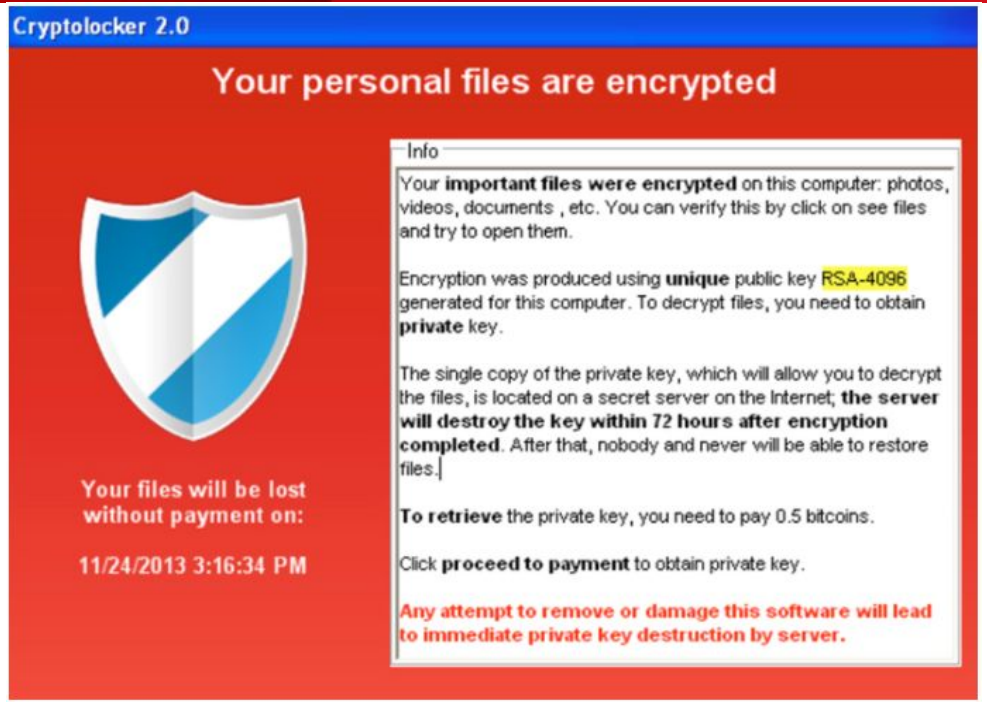
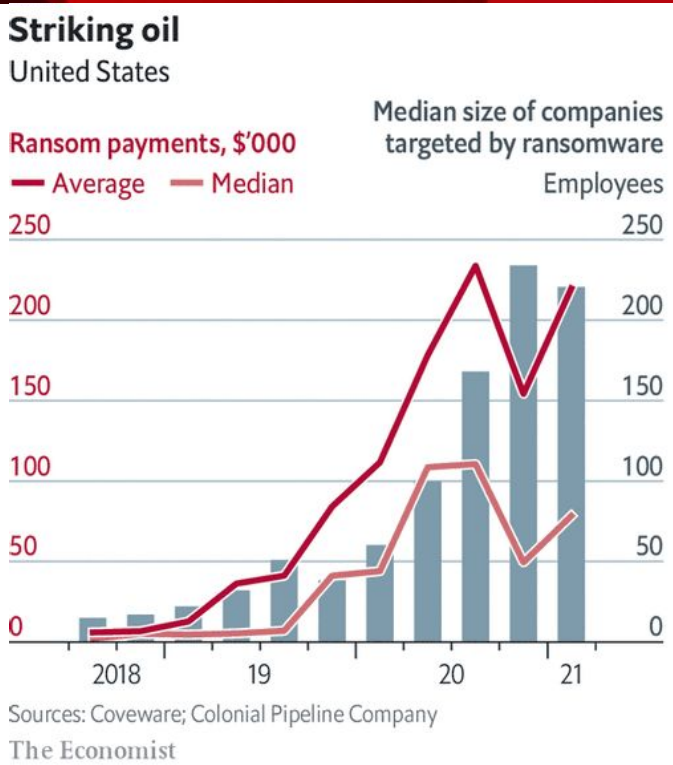


Figura 2. Exemplo Tela Sistema Contaminado

Ransomware



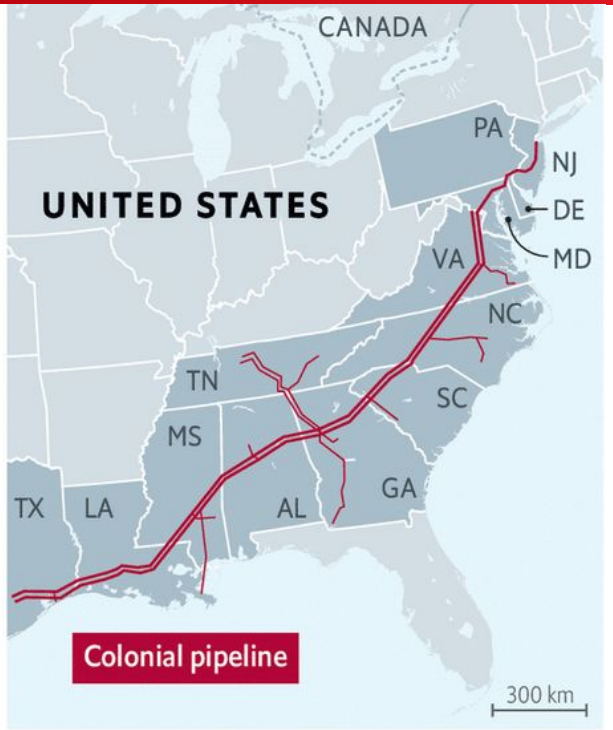


Figura 3. Evolução preço do resgate extensão do oleoduto da Colonial

Ransomware

Mesmo com seguro contra cyber ataques, pagar o resgate nem sempre é uma boa opção:

1. Sem garantia de cooperação do atacante
2. Sem garantia de funcionamento da descriptografia
3. Não mitiga novos ataques posteriores
4. Restrições de compliance e de governo (ex.: embargos governamentais contra países)
5. Moralmente questionável pois incentiva a atividade criminosa

Ransomware

Em linha com a AhnLab [2], patches de segurança e backups podem ser as únicas soluções eficazes para ataques de ransomware.

Os últimos ataques de ransomware tendem a usar novos malwares e suas variantes para burlar programas antivírus. Uma vez que é basicamente impossível preventivamente prevenir e bloquear ransomware, só podemos estabelecer uma estratégia de resposta passiva para minimizar os danos.

[2] Ransomware Response: Ideal versus Reality.<http://www.gartner.com/imagesrv/media-products/pdf/ahnlab/ahnlab-1-2VS6RBW.pdf>

Ransomware

Infelizmente, alguns fornecedores de segurança induziram os clientes a pensar que suas soluções de segurança, como programas AV, podem impedir os ransomware. No entanto, todos os fornecedores de segurança enfatizam duas medidas de segurança básicas para evitar ataques de ransomware: ***fazer backup de arquivos importantes*** *e aplicar os patches de segurança de sistemas mais recentes.*

Em outras palavras, a aplicação dos últimos patches do sistema pode prevenir a infecção (pré-resposta) e, mesmo se ela estiver infectada, os danos podem ser minimizados ao restaurar o último backup.

Ransomware

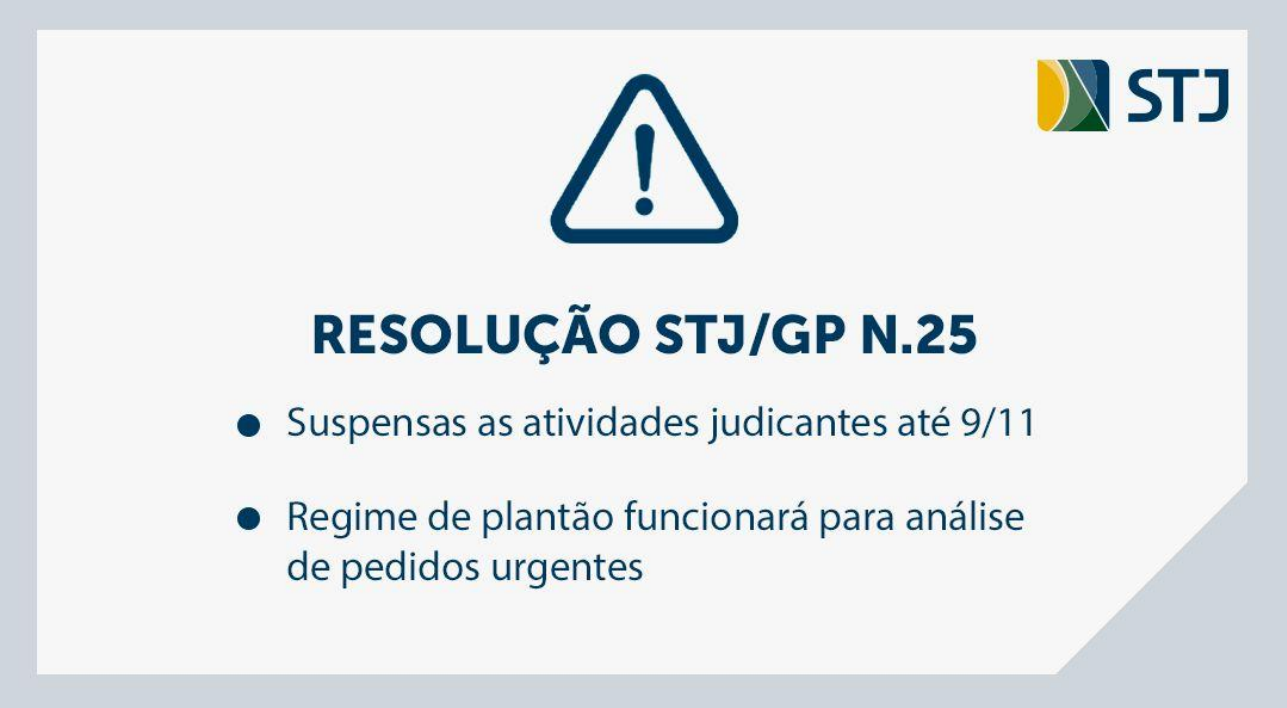
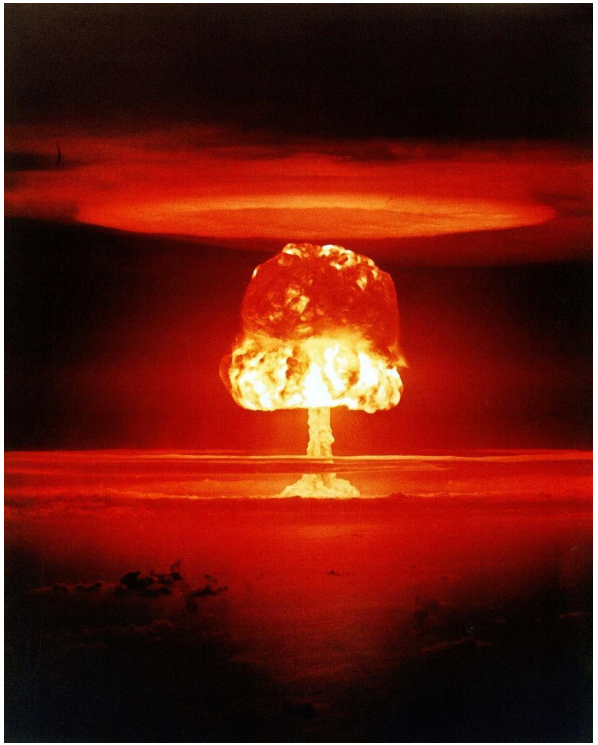


Figura 4. Mensagem sistemas STJ inativados por Ransomware

Backups



- Redundância de dados com o propósito específico de restauração no caso de perda dos originais
- Falha de hardware; catástrofes físicas; atividade maliciosa; updates falhos de software; "eu não mexi em nada!"; update sem where; rm -rf errado; etc.
- Também precisa resistir ao Ransomware!

Backups

- Desde meados de 2000. **Cringe!**
- Requer Política de backup. Exemplo do Governo Federal:

  Apesar de se tratar de um controle básico, ***metade das organizações respondentes (208 de 410: 50,7%) ainda não possuem tal documento.*** *Das 202 que o elaboraram, quase metade (98 de 202: 48,5%) ainda não formalizaram essa política.*

  Ref.:

  <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-politica-de-backup-em-422-organizacoes-federais.htm>

Backups

- 44 Zettabytes de dados a backupear em 2020 [IDC]
- Armazenamento Conjuntos de Discos, Fitas Magnéticas Nuvem

Backups

Os Três Níveis de DR

- **Nível de Dados.** Proteção dos dados de usuários e aplicações (dumps, cópia de arquivos)
- **Nível de Aplicação.** Continuidade da aplicação (PITR, CDP, plugins para aplicações)
- **Nível de SO.** Reduzir o tempo de recuperação do sistema para o menor possível (export de VM, CDP, snapshot de FS, Bare Metal)

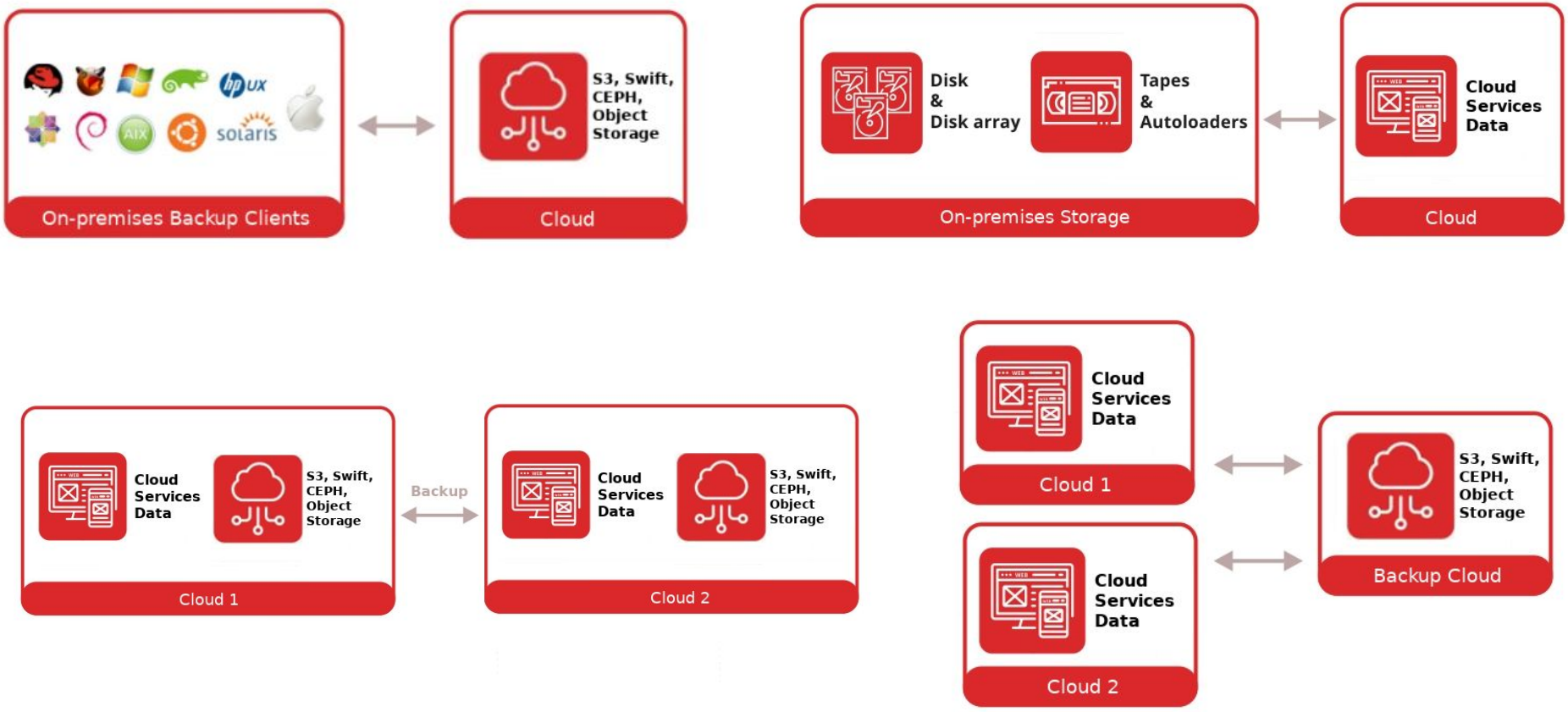


Figura 5. Principais Arquiteturas de Backup

Bacula

Figura 6. Backup + Drácula = Bacula

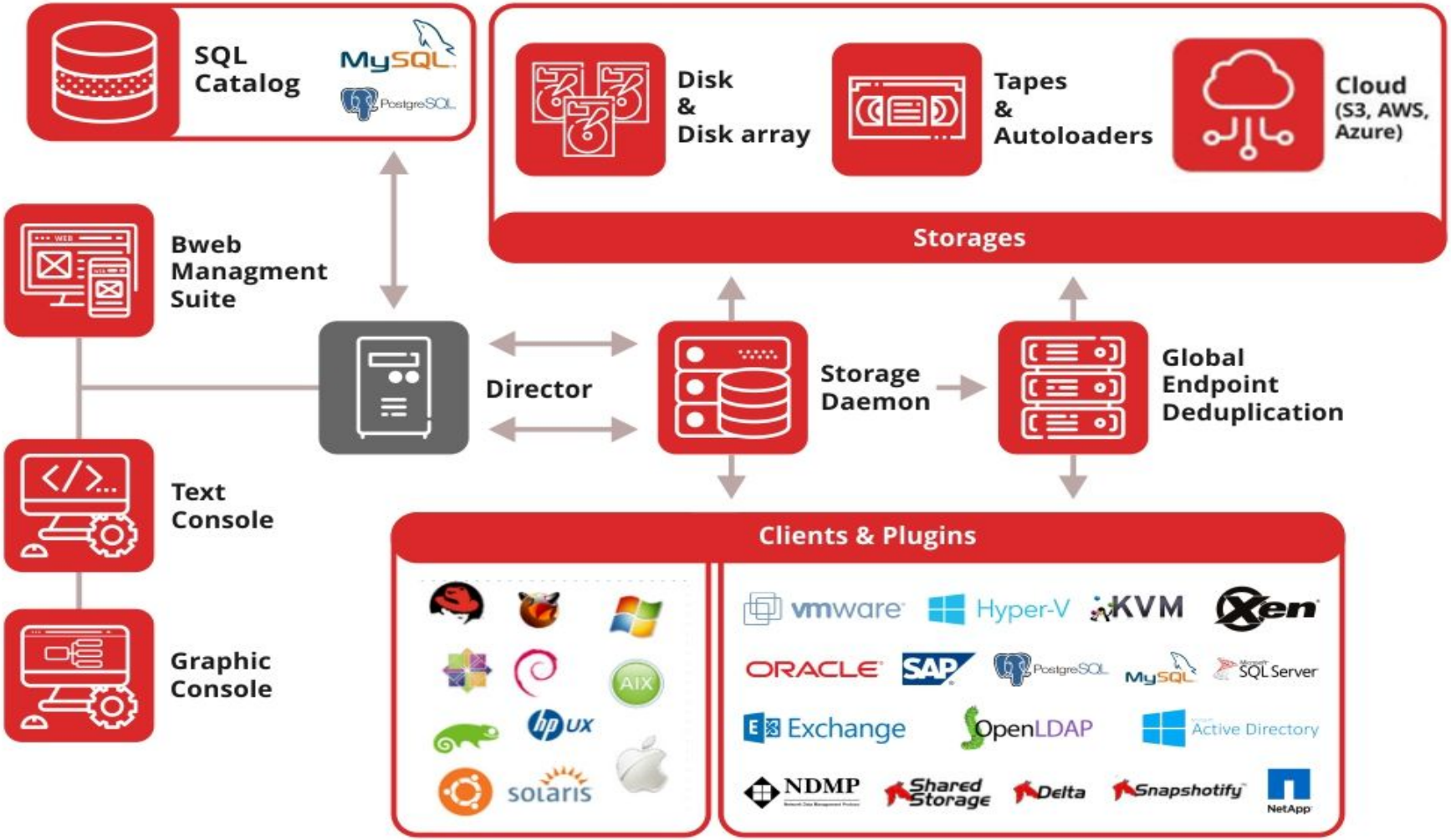


Figura 7. Arquitetura do Bacula. Também precisa ser resistente ao ransomware.

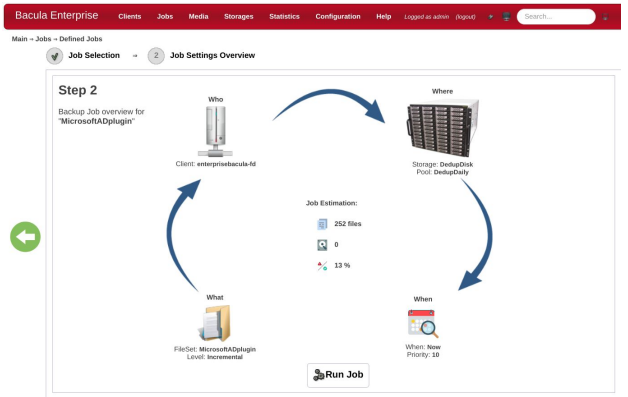
Bacula

- Deduplicação Global (**na origem ou somente storage**: Windows, Unix, Linux etc.).

  Até 99% de redução no tráfego e armazenamento.
- CBT para outras Virtualizações (RHV, XEN etc.)
- Primeiros Plugins para **Docker, Kubernetes, Proxmox, Hadoop, PostgreSQL e MySQL**;
- Altíssima Escalabilidade (**poucas conseguem fazer backup de 10.000 hosts ou mais**).

Bacula

- Mais avançadas Interfaces Web do Mercado, sem requerer **Java/Flash**. Deploy/update remoto de agentes, etc.
- Equipe de Desenvolvimento própria
- Não é uma suíte!
- Formato de Catálogo e de Backup Abertos (sem aprisionamento);
- Versão Livre/Enterprise



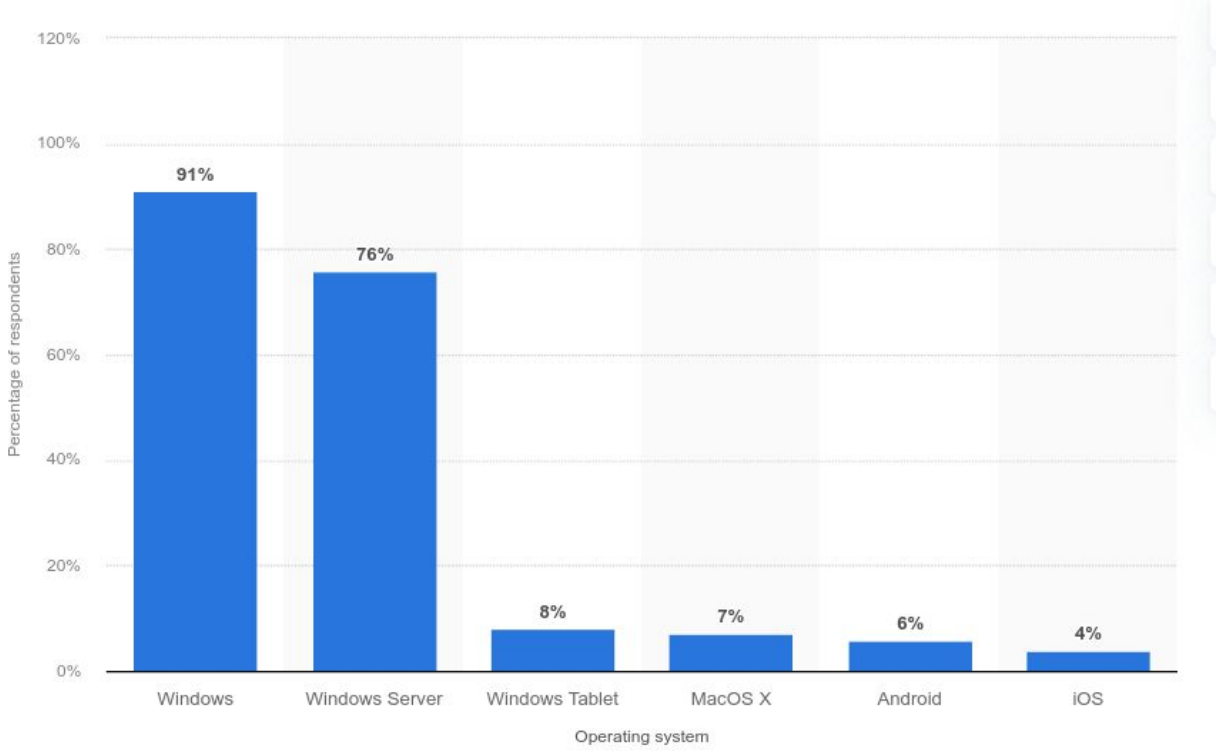


Figura 8. SOs que Usuários Reportaram Contaminação de Ransomware

Linux

1. In 2021, 100% of the world's top 500 supercomputers run on Linux.
2. Out of the top 25 websites in the world, only 2 aren't using Linux.
3. 96.3% of the world's top 1 million servers run on Linux.
4. 90% of all cloud infrastructure operates on Linux and practically all the best cloud hosts use it.

Ref.: <https://hostingtribunal.com/blog/linux-statistics/>

Linux

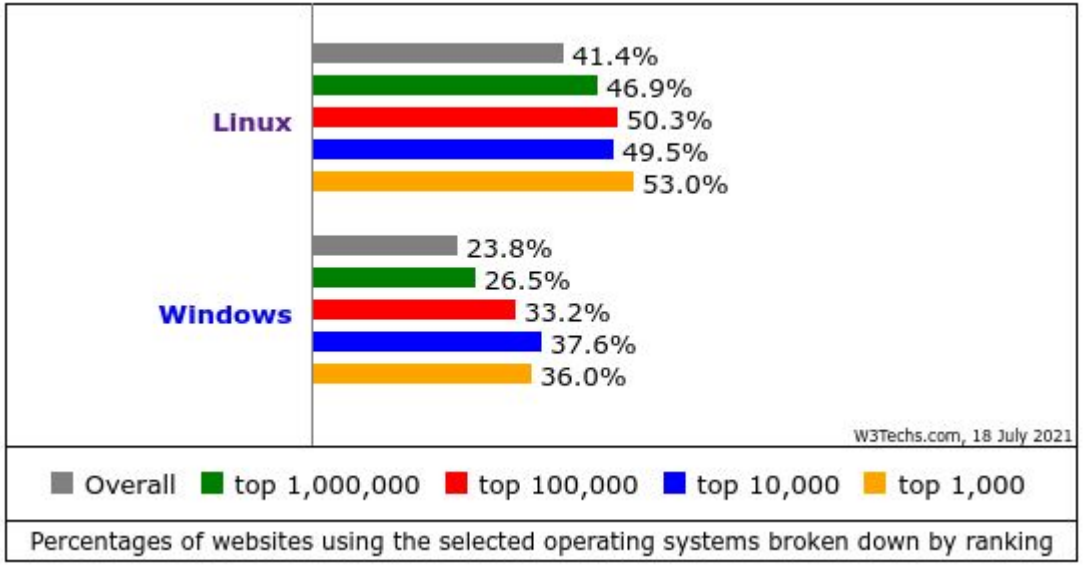


Figura 9. SO de Servidores WEB. Ref.:
<https://w3techs.com/technologies/comparison/os-linux,os-windows>

Linux

- ★ Bacula é pioneiro no Servidor primariamente em Linux, dentre os Líderes
- ★ Maior quantidade de plataformas Clientes, incluindo Windows, Mac OS, Linux, Unix, Android etc.

Figura 10. Clientes de Backup suportados pelo Bacula

Regra 3-2-1

Using tape backup as part of an overall data management strategy allows use to follow best practices in data backup and compliance, specifically the widely known 3-2-1 rule, which is:

1. Maintain three separate copies of your data.
2. Store your data on at least two different types of storage media.
3. Keep one copy of your data in an off-site location.

Ref.:
<https://searchstorage.techtarget.com/IronMountainCloud/A-New-Old-Weapon-Against-Ransomware-Tape-Backup>

Regra 3-2-1

- Suporte nativo desde a concepção de gravação direta em todas as **fitas, cartuchos, VTL etc.**
- Primeira a suportar driver de armazenamento em múltiplos provedores de Object Storage **(S3, Glacier, Oracle, Google, Azure, Swift etc.).**

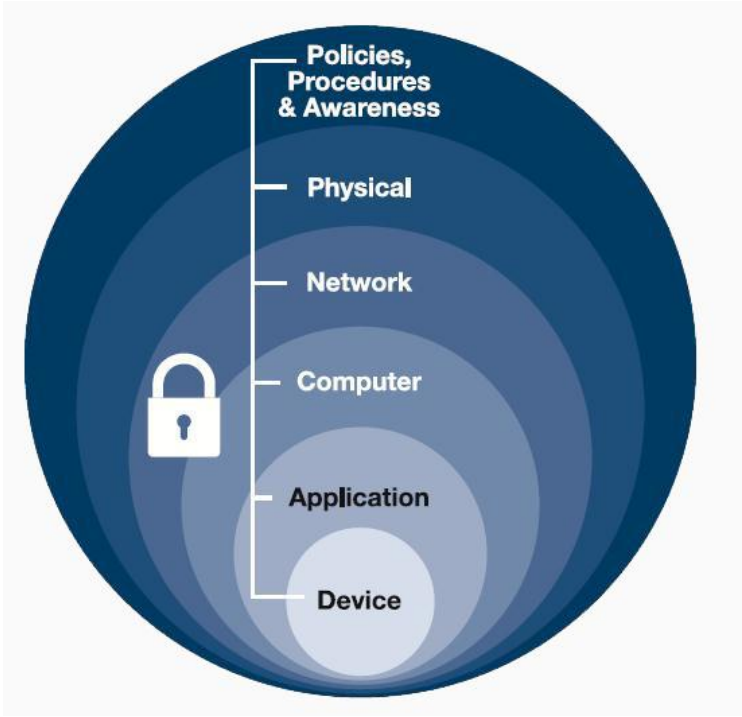
Figura 11. Plugins de Nuvem do Bacula

Hardening

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem.

Ref.: <https://www.beyondtrust.com/resources/glossary/systems-hardening>

Hardening



- ★ Apenas o usuário bacula do sistema de arquivos precisa ter acesso de escrita nos volumes de backup em disco, fita, nuvem e catálogo de backup.
- ★ Protocolos de conexão socket exclusivo e nunca violado. Todas comunicações criptografadas automaticamente com certificado FIPS.

Figura 12. Processo Geral de Hardening. Ref.: <https://paralok.com/?page_id=36>

Hardening

★ Possibilidade de imutabilizar os volumes de backups em disco ou em nuvem encerrados para gravação. Ex. disco:

```
# Seta o atributo imutável no volume de disco:
chattr +i <volume_bacula>

# Remove o atributo imutável no volume de disco:
chattr -i <volume_bacula>
```

Hardening

- ★ Esquema GFS com Pool Off-site. Ou uso de fitas WORM (Ref.: <https://techmonitor.ai/techonology/data/could-worm-help-build-local-govt-resilience-to-ransomware>).

Figura 13. Foto de Fita WORM LTO-6

Perguntas e Respostas

www.bacula.com.br

heitor@bacula.com.br

Diretoria Comercial

Melissa Faria – melissa@bacula.com.br