

Sistemas de arquivos indelévelis: defesa "infalível" contra ransomware?

***Danton Nunes, Internexo Ltda.
danton.nunes@inexo.com.br***

GTER/GTS – Belém, PA, maio de 2019

SUPORTE_

O SEU COMPUTADOR FOI INFECTADO POR UM RANSOMWARE QUE BLOQUEOU O ACESSO A TODOS OS SEUS ARQUIVOS.

MAS PAGANDO O RESGANTE TALVEZ POSSAMOS RECUPERAR OS DADOS.

VOCE TEM QUE AVISAR IMEDIATAMENTE O MEU CHEFE SOBRE ESSE RESGATE.

NESSE PC ESTÃO VARIOS RELATORIOS QUE PRECISO CONFERIR PARA A DIRETORIA, DEZENAS DE PLANILHAS QUE TENHO QUE PENCHER PARA O DEPARTAMENTO FINANCEIRO, ALEM DE INUMEROS CADASTROS QUE DEVO DIGITAR PARA A CONTABILIDADE.

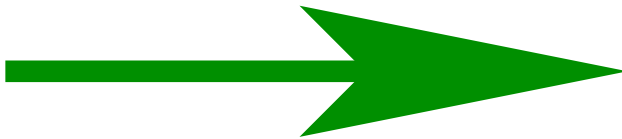
TOMA AQUI CINQUENTINHA PRA FICAR DE BICO FECHADO.

Capítulo I

O pesadelo não acabou!

Há três anos eu falei sobre isto em Uberlândia, no GTS-27. De lá para cá as coisas não mudaram tanto quanto eu gostaria. Ataques de sequestro de dados ainda acontecem.

***disponível no
arquivo do
GTS***



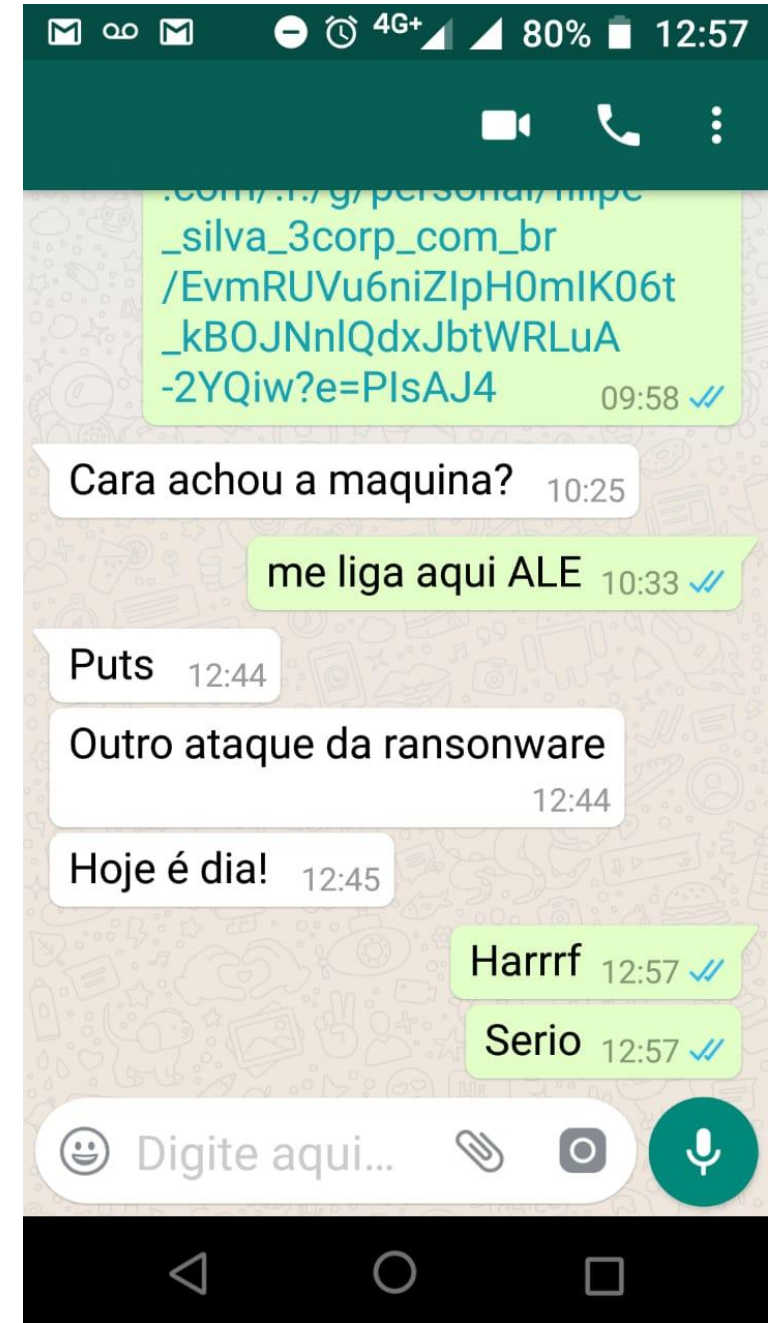
Ransomware

backup e outras medidas preventivas

GTS-27 Uberlândia, Maio de 2016

*Danton Nunes <danton.nunes@inexo.com.br>
Internexo Ltda. São José dos Campos, SP*

Trecho de uma conversa por whatsapp entre dois técnicos de TI, há apenas algumas semanas.



Sistemas de arquivos indelévels: defesa "infalível" contra ransomware?

depois que o estrago foi feito...

The screenshot shows a Windows File Explorer window titled "BackupBD" displaying a directory of backup files. The files are organized in a table with columns for Name, Date de modificaç..., Tipo, and Tamanho. The files are named with a pattern: SINAPSE-YY-MM-DD-YY-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos. A tooltip is visible over one of the files, showing its details: Tipo: Arquivo PHOBOS, Tamanho: 1,93 GB, and Data de modificação: 17/04/2019 01:48. The taskbar at the bottom shows the system tray with the time 10:58 and date 17/04/2019.

Nome	Data de modificaç...	Tipo	Tamanho
SINAPSE-31-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-31-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-29-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-30-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-30-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-30-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-31-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-27-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-28-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-28-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-28-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-28-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-29-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-29-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-26-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-26-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-26-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-26-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-27-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-27-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-27-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-25-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-25-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-24-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-24-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-24-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-24-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-25-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-25-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-22-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-22-03-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB
SINAPSE-22-12-2018-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-23-01-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	1.793.873 KB
SINAPSE-23-02-2019-22-00.FDB.id[2AC1A109-0001].[carmichael.lion@aol.com].phobos	17/04/2019 01:48	Arquivo PHOBOS	2.025.617 KB

Resumo da história:

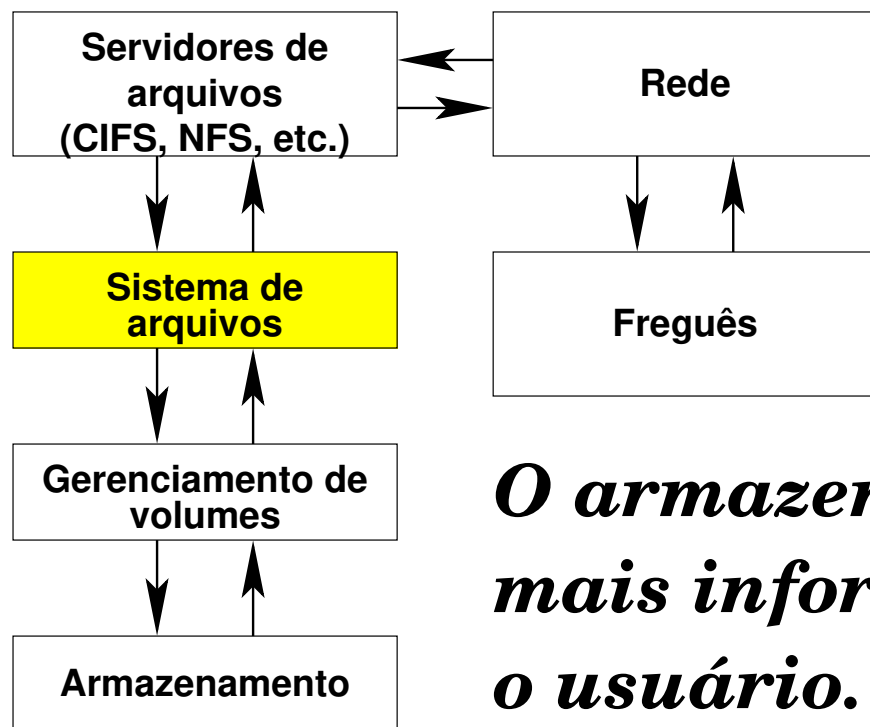
- Ransomware ainda está à solta pelo mundo!***
- Depois de feito o estrago, a recuperação é quase impossível.***
- Em alguns casos nem é mais possível pagar o resgate porque os criminosos já estão presos, mas os transmissores da encrenca ainda estão à solta!***
- A melhor saída é a PREVENÇÃO!***

Capítulo II

Onde entra o sistema de arquivos?

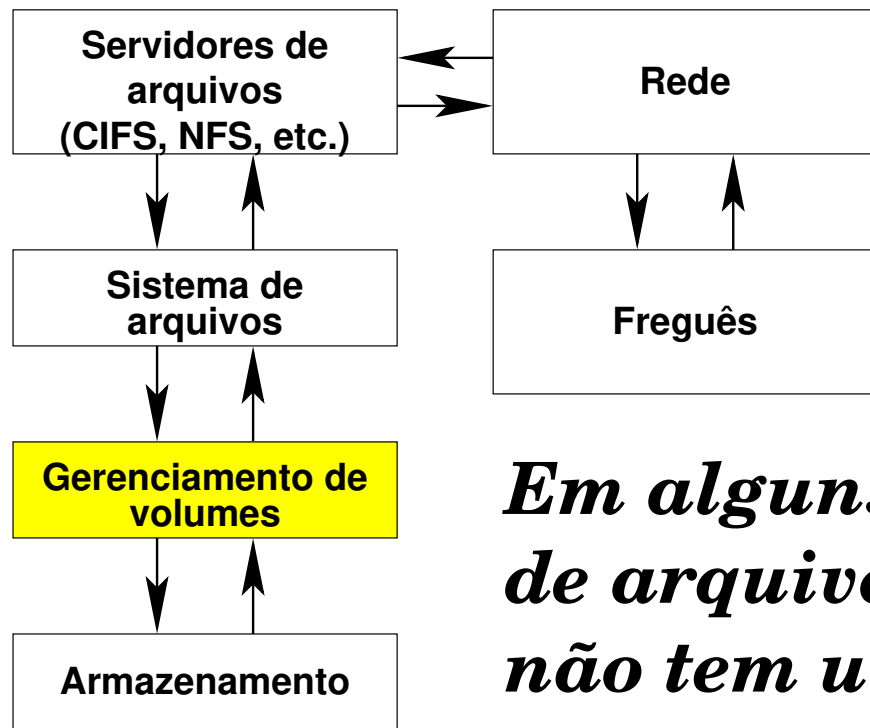
Tipicamente, em ambientes corporativos, os arquivos "moram" em servidores e são acessíveis pela rede.

Um programa em uma estação de trabalho invadida pode cifrar os arquivos no servidor, como se fossem arquivos locais.



O sistema de arquivos cria uma camada de abstração sobre o armazenamento com arquivos e pastas.

O armazenamento pode conter muito mais informação do que aparece para o usuário. E isso pode ser útil!



O sistema de gerenciamento de volumes também tem um papel importante na prevenção de desastres.

Em alguns casos (ex. btrfs, zfs) o sistema de arquivos e gerenciamento de volumes não tem uma fronteira bem definida.

Há estratégias de defesa contra ransomware que se baseiam em propriedades do gerenciamento de volumes, ou na combinação deste com o sistema de arquivos, p.ex. nilfs2 + lvm2.

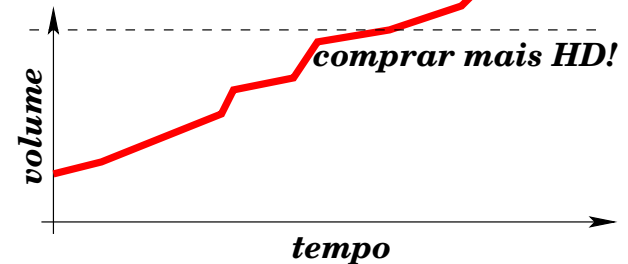
Capítulo III

Arquivos indelévels e a arte de viajar no tempo

Sistemas de arquivos "indelévels"

**** Todos os dados são guardados em um silo circular e só são removidos se for necessário reaproveitar espaço.***

**** Consequencia imediata: a ocupação do disco cresce com o tempo.***



**** Consequencia interessante: pode ser possível recuperar informações no passado.***

Exemplos:







MVS-SP2, IBM, 1980 (havia vida inteligente no sec.XX)

Plan 9's fossil, Bell Labs, 2002

NILFS, NTT/Verio, 2005

NOVA, UCSD, 2017

NILFS(2)

-  ***log circular, com "garbage collector"***
-  ***pontos de controle a cada poucos blocos modificados gerados automaticamente.***
-  ***pontos de controle podem ser convertidos em snapshots => granularidade temporal fina.***
-  ***os snapshots somente podem ser montados para leitura, o que dificulta a recuperação.***
-  ***é um notório devorador de disco, apesar de ter alguma deduplicação e coletor de lixo.***
-  ***não suporta ACLs POSIX.***

NILFS(2)

Lista de pontos de controle (caso real!)

```
# lscp -a
```

CNO	DATE	TIME	MODE	FLG	NBLKINC	ICNT
1	2015-09-18	13:00:46	ss	-	11	2
2	2015-09-18	13:10:05	cp	-	23	9
3	2015-09-18	13:11:58	cp	-	1669	53
4	2015-09-18	13:12:00	cp	-	1247	53
5	2015-09-18	13:12:09	cp	-	830	53
6	2015-09-18	13:12:14	cp	-	2018	53
7	2015-09-18	13:12:23	cp	-	3215	53
8	2015-09-18	13:12:28	cp	-	1605	53
9	2015-09-18	13:12:37	cp	-	1935	53
10	2015-09-18	13:12:44	cp	-	388	65
.....						
136506	2019-05-08	14:39:34	cp	-	24	299521
136505	2019-05-08	14:39:28	cp	-	28	299522
136504	2019-05-08	14:39:13	cp	-	23	299520
136503	2019-05-08	14:38:59	cp	-	23	299520
136502	2019-05-08	14:38:49	cp	-	23	299520
136501	2019-05-08	14:38:37	cp	-	24	299520
136500	2019-05-08	14:38:32	cp	-	38	299521
136499	2019-05-08	14:35:53	cp	-	25	299521
136498	2019-05-08	14:35:48	cp	-	33	299522
136497	2019-05-08	14:29:58	cp	-	24	299521

NILFS(2)

Convertendo um ponto de controle em snapshot.

```
# chcp ss 123456 /dev/disk  
# mount -o ro,cp=123456 -t nilfs2 /dev/disk /mnt
```

1. converte o ponto de controle 123456 em snapshot

2. monta o snapshot em /mnt

Todos os arquivos e pastas aparecem sob /mnt exatamente como se encontravam no momento da criação do ponto de controle 123456.

btrfs (Butter Fuss?)

Sistema de arquivos baseado em b-trees, remanescente do ReiserFS.

Permite criar snapshots de subvolumes mais ou menos à vontade. Cada snapshot é também um subvolume e pode ser montado a parte ou visto como um diretório.

Outras características interessantes:

- conversão "rápida" de ext3, ext4, ReiserFS para btrfs.***
- union mounting ou overlays, permite criar um novo fs a partir de um pré-existente (seeding, na linguagem do btrfs)***
- compressão transparente e criptografia (prometido).***

Funções típicas de gerenciamento de volumes.

lvm – Sistema de Gerenciamento de Volumes

O lvm do Linux também pode ajudar na prevenção de ataques de ransomware.

Criar snapshots de volumes lógicos inteiros, independente do conteúdo.

Excelente opção para backup.

Mas há alguns problemas:

- Os snapshots aumentam a carga do sistema pois a cada bloco modificado no volume original, o bloco anterior é reescrito no snapshot. => Limite no número de snapshots.***
- Não permite snapshot de um snapshot.***

Procedimentos de prevenção comparados

nilfs2

não fazer NADA! pontos de controle criados automaticamente.

btrfs

criar snapshots periodicamente (crontab?)

lvm

criar snapshots periodicamente (crontab?)

remover snapshots mais antigos para evitar degradação de desempenho.

A periodicidade de criação de snapshots deve garantir que pelo menos um tenha sido criado ANTES do ataque ter se iniciado!

Procedimentos de recuperação após o ataque

nilfs2, sem overlays

- 1. Remover todos os arquivos cifrados da imagem corrente,*
- 2. Copiar os arquivos removidos do último ponto de controle anterior ao ataque. => Isto pode demorar!*

nilfs2, com overlays

- 1. Remover TUDO da imagem corrente,*
- 2. Criar um sistema de arquivos estratificado (overlays):*

```
# mount -t overlay none \  
-o lowerdir=/lower, upperdir=/upper, workdir=/work \  
/merged
```

ponto de montagem do snapshot (ro)

ponto de montagem da imagem corrente vazia (rw)

pasta de trabalho do sistema de overlays

pasta com os arquivos "recuperados".

Procedimentos de recuperação após o ataque

btrfs

É a opção mais simples do ponto de vista de recuperação.

Basta remover o subvolume corrente e "promover" o snapshot mais recente não corrompido à posição corrente.

Identificar o snapshot mais recente não corrompido pode não ser muito fácil (o mesmo vale para nilfs2).

É necessário criar snapshots a intervalos regulares, p.ex. uma hora, e remover os mais antigos ou não haverá disco que agüente apesar do btrfs tem um bom esquema de deduplicação.

Procedimentos de recuperação após o ataque

lvm2

Infelizmente o lvm não tem um mecanismo de promoção de um snapshot para o volume principal.

Ou se copia todo o snapshot mais recente não corrompido para o volume principal ou se usa o artifício da montagem em camadas mostrada anteriormente no caso do nilfs.

Um problema com o lvm é o fato de que os snapshots guardam as modificações, portanto não se pode criá-los às centenas, o que pode dificultar ter um snapshot não corrompido, especialmente se a detecção do ataque não for imediata.

Observações importantes

A escolha do método de prevenção depende muito das circunstâncias. Por exemplo, se for necessário migrar rapidamente de ext4, btrfs certamente será uma boa escolha.

Além do uso de sistemas de arquivos/volumes com alguma inteligência, nunca se esqueça de ter cópias de backup. Backup e canja de galinha só fazem mal a esta última.

Quanto mais rapidamente o ataque for detectado e o servidor isolado da rede, melhor.

Tráfego de rede anormalmente alto de e para o servidor é um bom indicador de ataque em andamento.

Conclusões

Melhor prevenir do que tentar remediar. Há sistemas de arquivos e volumes que ajudam bastante na prevenção.

Truques como a montagem estratificada (union mount) tornam a recuperação razoavelmente rápida.

Em caso de falha destes procedimentos, apele para o backup! É para isso que ele deve ser feito regularmente.

Agradecimentos

GTER/GTS, registro.br, nic.br, Internexo Ltda.

