VEEAM ON 2023

You're Hit by a Ransomware Attack, What's Next?

Eric Machabert
CTO/CISO
Maincare Solutions

Julien Mousqueton
CTO Cybersecurity
Computacenter

Christopher Glemot
CTO & Head of Alliances
Monaco Cyber

VEEAMON2023

Day 1 – Time to react

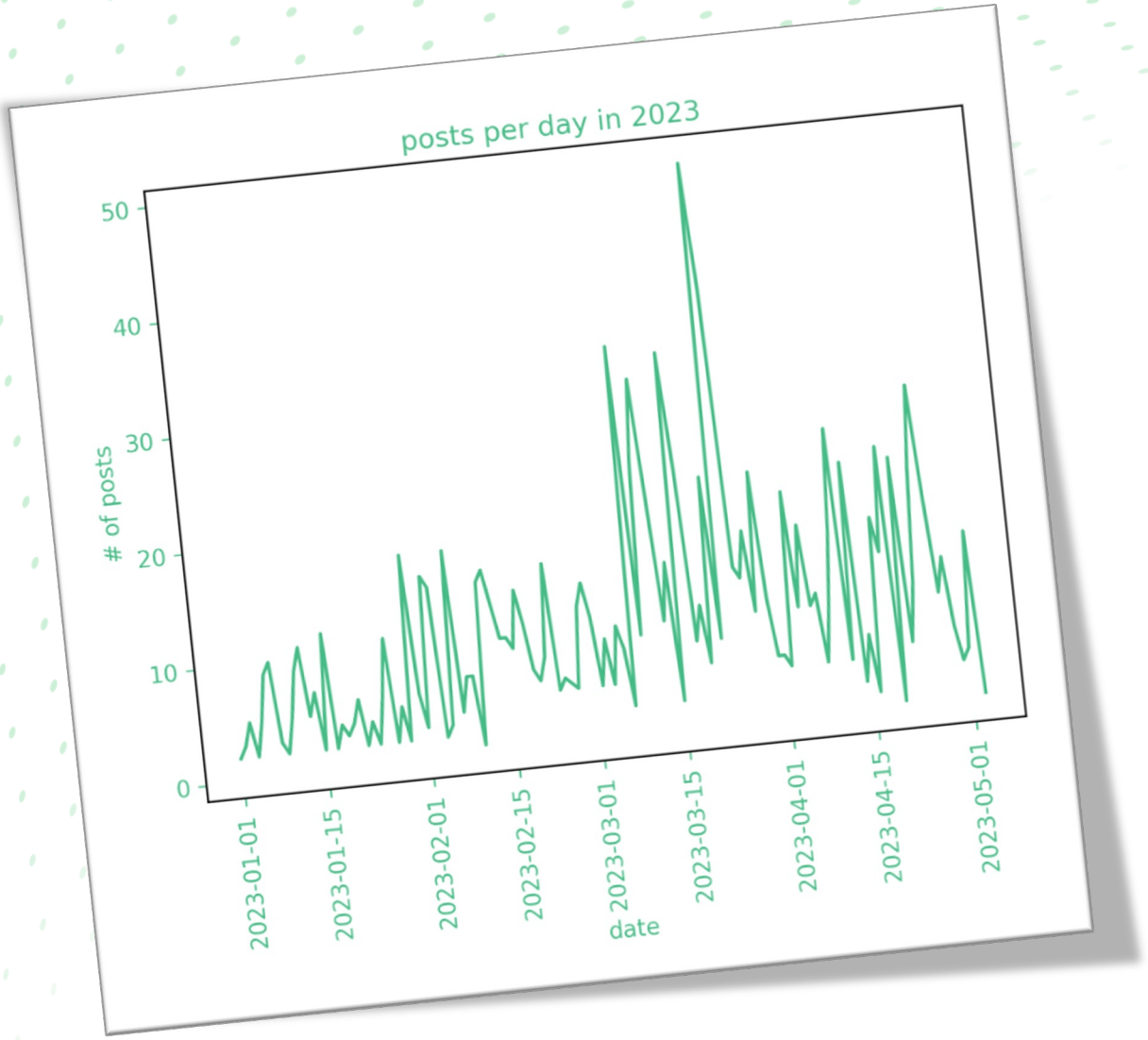
Julien Mousqueton
CTO Cybersecurity @ Computacenter
Cyber SOC & CSIRT Manager
Owner of **ransomware.live**

VEEAMON2023

It’s not too late

Don’t panic

VEEAMON2023



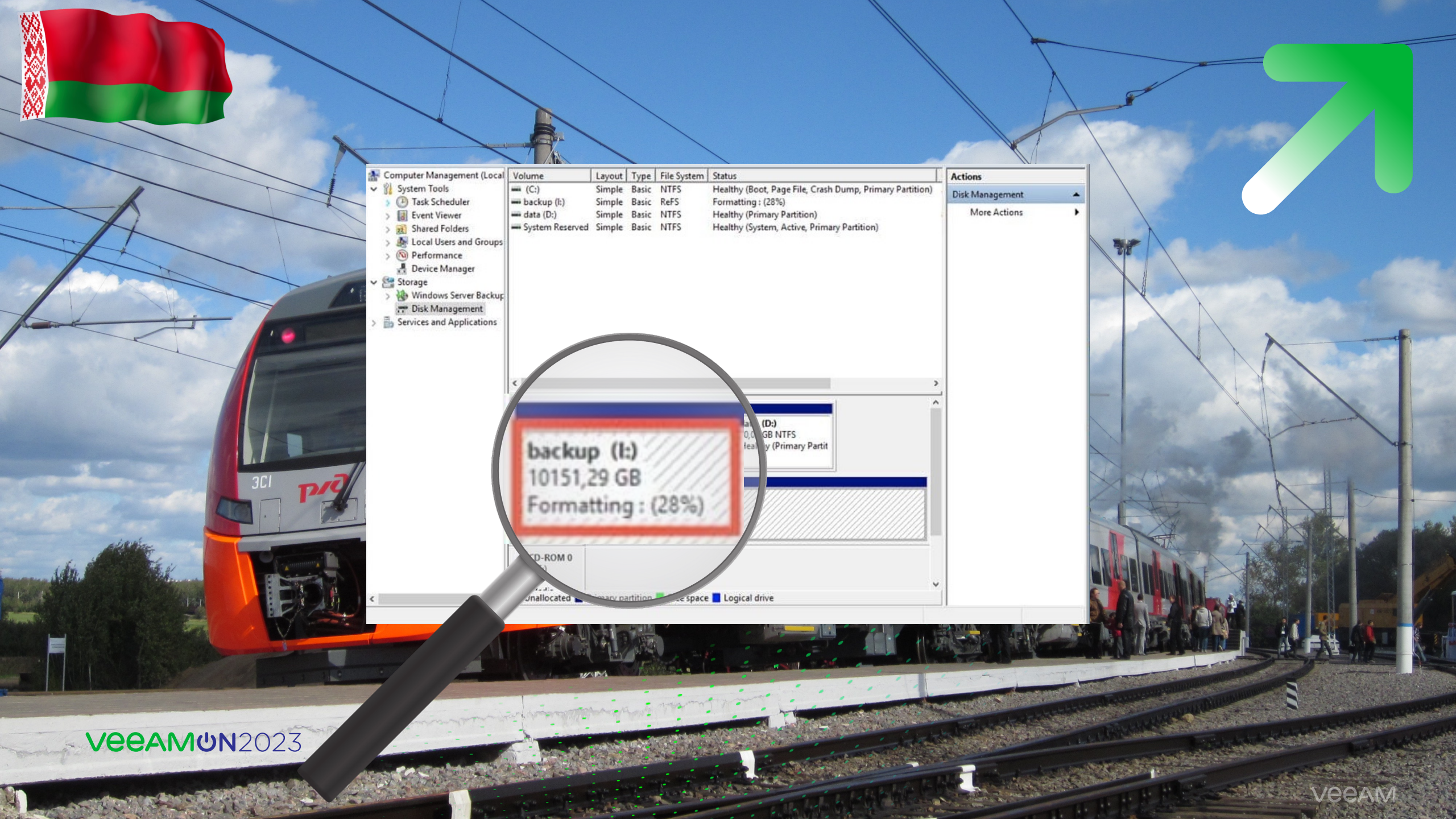
You're not the only one

Source: Ransomware.live

Proof for investigation

VEEAMON2023

VEEAMON2023


Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Windows Server Backup
Disk Management
Services and Applications
Volume
Layout
Type
File System
Status
(C:) Simple Basic NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)
backup (I:) Simple Basic ReFS Formatting : (28%)
data (D:) Simple Basic NTFS Healthy (Primary Partition)
System Reserved Simple Basic NTFS Healthy (System, Active, Primary Partition)
Actions
Disk Management
More Actions
backup (I:)
10151,29 GB
Formatting : (28%)
(D:)
GB NTFS
(Primary Partit
CD-ROM 0
Unallocated
Logical drive
VEEAMON2023
VEEAM


BACKUP

My tips

- ✓ Perform "realistic" e
  - Taking into cons vestigation
- ✓ Build an internal and
  - Use external too
- ✓ Audit the security of
- ✓ Perform regular recc

Avoid Schrödinger’s cat on backup

VeeAMON2023

Don’t gamble with your data

VeeAMON2023

VEEAMON2023

Day 2 – Time to rebuild!

Christopher Glemot

CTO & Head of Alliances @ Monaco Cyber
Owner of Original-Network.com - @c_glemot

How to build a resilient architecture against Ransomware? (circumstance and beyond)

VEEAMON2023

First 48 hours crucial for the rebuild step

1) Safe Assets analysis (data)
- Production
- Backup

2) Forensic
- Playbook
- Anatomy (understanding)
- Logs (exporting and analysis)

2) Rebuild & Monitor
- Secure by design
- Backup of circumstance

My Tips

Be accompanied by a dedicated specialist of Data Protection to manage this stream!

Forensic: Use Veeam® Explorer *for Active Directory*.

Active Directory (the weak point)

- Tiering model + Least Privilege
- Network segmentation + Hardening policy
- No critical infrastructure asset relying on AD for management

My Tips

Monitor your AD in real time (lateral movement, escalation of privileges..).

Secure by design infrastructure

- Segmentation of network **and** authentication
- Password vault not based on AD authentication for admins
- Bastion host with 2FA for admins
- Dedicated admin workstations in an admin enclave
- Observability: collect events, analyze and trigger alerts
- Backup with off-site copy and immutability

VEEAMON2023

My Tips

Secure Backup is your last line of defense.

Don't neglect this point and respect the **3-2-1-1** rule!

What we saw in 2022

Sophisticated attacks on backup environment

- Domain and **Off domain**,
- Groups target **Password Management tools** (KeyPass, etc.),
- Lateral Movement and Exfiltration though RDP session stealing

Backup data

- **Removing Backup** data from Management/Administration interface (server, appliance etc.),
- Skills to **empty the headers** of backup appliances (knowledge for each vendor),
- **Enabling other protocol** on Backup appliances (CIFS/NFS) in order to bypass proprietary and secure protocols.

Backup software used as an “attack tool”

- **Erasing data on tapes** (in the library) by installing another Backup software to take ownership of the library

Recommendations

- **Segment your passwords** into different Password Management tools according to your management organization
- **Never leave your Password Management tool open** on your workstation, and never store it on the Filer Server,
- **Network Segmentation** (dedicated network for management, for backup etc)
- Build an Admin enclave

Recommendations

- Enabling **2FA** on the management interface (storage hardware, appliances, etc.), bastion,
- **Anonymizing** the name of backup servers and repositories – and the name of service accounts,
- Integrating **Trusted Repository Storage** with secure features (immutability, proprietary protocol, MFA, Security Officer mode, etc.).

Recommendations

- Store the tape in a secure place (Fire-Resistant Box).

VEEAMON2023

More info: https://original-network.com/play-ransomware-infection-routine/

VEEAMON2023

Why I’m not fun at parties

Eric Machabert

CTO & CISO @ Maincare Solutions

What not to do.

VEEAMON2023

Act without any risk assessment

- Don’t do any risk identification and evaluation
- Don’t do any Business Impact Analysis
- Set up technical risk treatment measures out of habit

My Tips

Be kind to yourself : Take time for this stuff

Business Continuity Plan drives the efforts

Review ISO 27005,27001 & 22301 for guidance

Avoid the “techy” approach, act wisely

Build for space efficiency only

- Set up a space efficient only, single tier architecture
- Don’t consider the “restore all” scenario
- Think a week or two available on tier 1 is enough
- Don’t test and measure real restore performance on large dataset, **over time**

My Tips

Build for speed at backup AND restore for Tier 1

At least 2 tiers, first one holding at least a month

Avoid deduplicating storage appliances at Tier 1

Tier 2 must be offsite

Use encryption only because it is cool

- Don’t do risk assessment regarding the use of encryption
- Don’t plan for “unavailable keys” scenario
- Don’t test recoverability and data integrity frequently

My Tips

Remember encryption only protects privacy

Evaluate the risks coming with encryption

Offsite copy → encrypt, protect the keys

Local Tier 1: encrypt based on the risk assessment

Do not have an offline copy

- Think everything will go as planed
- Assume risks never overlap
- Don’t like offline backup because it is slow legacy stuff ☺

My Tips

Have an offline, encrypted, copy

Tape is still alive and affordable for large dataset

Trust me: old data is better than no data

Do not broaden the scope

- Prepare only for “IT based” issues
- Avoid crisis management training
- Don’t plan for alternative communication stream
- Don’t plan for the worse with no Plan B

My Tips

Law enforcement process can slow down recovery

Supply chain/hardware availability is important

Being prepared removes quite of the stress

VEEAMON2023

MIA06 - You're Hit by a Ransomware Attack, What's Next?

Eric Machabert
CTO/CISO
Maincare Solutions

Julien Mousqueton
CTO Cybersecurity
Computacenter

Christopher Glemot
CTO & Head of Alliances
Monaco Cyber