WAVESTONE

Retour d'expérience NotPetya

CoRIIN 2018

Vincent NGUYEN - Quentin PERCEVAL - 22/01/2018
@nguvin

#whoamiarewe

CERT W

Quentin Perceval

In charge of CERT-W operations

Rebuilding leader on NotPetya case

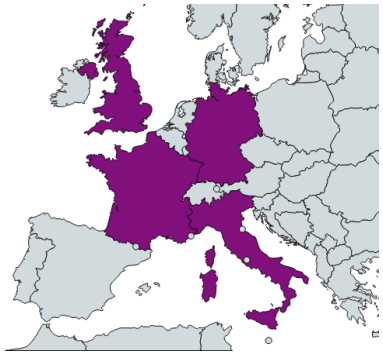
Vincent Nguyen

Head of CERT-W

Team leader on NotPetya case

Feedbacks on 2 emergency operations

Victim 1



Cyber-insurance call on June 27 at 3pm

2 experts on site at 5pm

- / 1 manager
- / 1 forensics analyst

Victim 2

Call from a CERT-W client on June 27 at 4pm

3 experts on site at 5pm

- / 1 senior manager
- / 1 forensics analyst
- / 1 reverse engineer

5pm *We are on site*

TECHNICAL SITUATION

- **Most of Windows assets are down**
  +50K workstations, +50% servers
- **Most traces are destroyed**
  Encrypted or removed logs
- **Restoration systems are unusable**
  Even though some backups exist

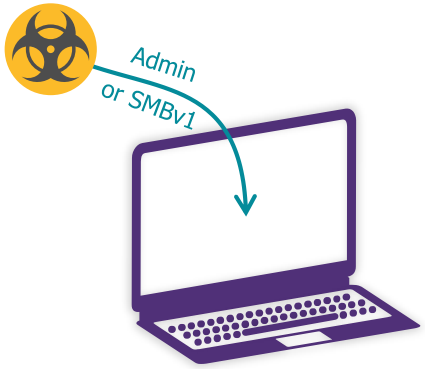
ORGANISATION SITUATION

- **Interrupted business (worldwide)**
  No access to applications, mails…
- **Overwhelmed IT teams**
  Very little understanding of the situation
- **Top management involved in the first hour (CEO)**

In the first hours:

- Understand & explain the situation – coordinate with CERT teams
- Structure the crisis governance (streams, steercos…)
- Save what can be saved – develop a sanity script
- Workforce – internal and partners

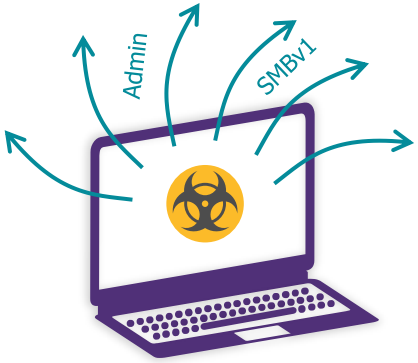
Weeks *of damages* caused in only **one hour** of malware execution



1. Initial infection

Malware **installation on the PC/server** through **Admin protocol** (WMI / PSExec) or **MS17-010 vulnerability** (SMBv1)

Patient zero infection *through an* ***automatic update*** *of an Ukrainian accounting software (M.E.Doc) with 400k users*



2. Spreading

~1 hour

Malware execution and **retrieval of credentials in cache**

Attempt to **spread on other PCs/servers** in private network through **MS17-010 vulnerability** (SMBv1) or **administration protocol** (WMI / PSExec)

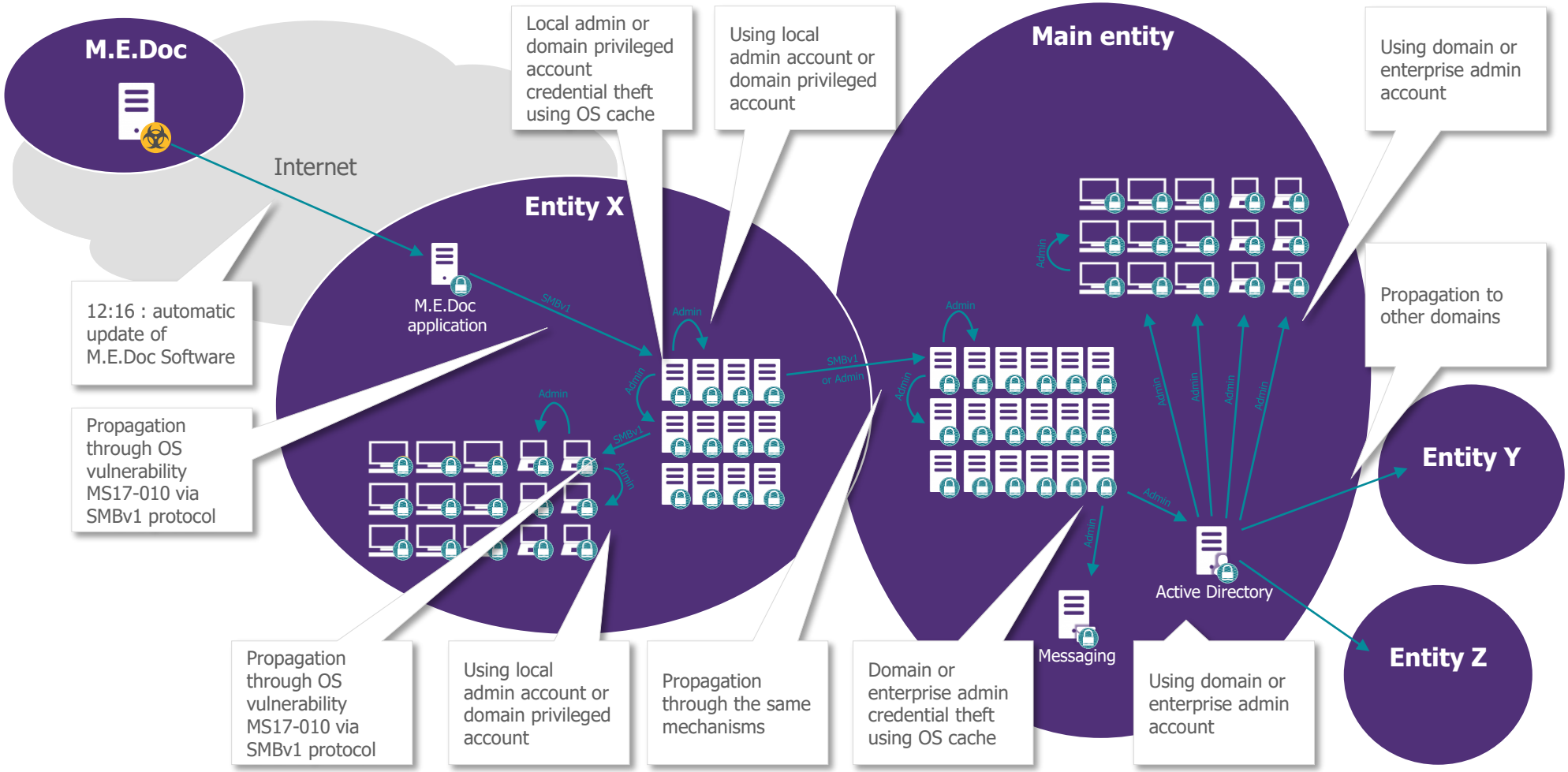
3. Encryption

2 cases:

- Most of the time, **reboot and complete disk encryption**
- If the PC/server disk is encrypted, **encryption of some files** (including Master File Table)

In the end **all infected PCs/servers are unusable,** with no means for remediation

Feedback of **CERT-W** investigation
How did NotPetya enter and spread in a company?



All this, in less than two hours in some companies!

Major difficulties during investigation

1. **Lack of useful logs**

   NotPetya erase logs, very few logging in victims IS, network & security equipment configured with less than 2 days of local logs retention…

2. **Nor detailed view neither overview of the Information System**

   Digital documents destroyed, outdated hard copies, partial knowledge…

3. **Not so many internal expertise in DFIR**

4. **Local teams abroad lost**

5. **Over communication in the media**

   New findings every 20 minutes

6. **No more workstation, no more Internet access, no more crisis management tool, no more knowledge base, no more control on any IT asset…**

7. **Our position between businesses, cyber-insurance and Group**




Zoom on human impacts

IT staff mobilized **24/7 during more than 10 days**

Rest room (people was sleeping on site)

Food available at will

Occupational Health

Employees unable to work during 2 weeks

Specific communication for employees, authorization of alternative ways of working

Timeline of the cyber-crisis

Understand the situation…

"At first I was afraid, I was petrified
Kept thinkin' I could never live without you by my side"

Mobilized workforce
Internals : 40-60
Wavestone : 2-3

Tuesday, June 27th
1PM-3PM

Emergency call from CISO / Cyber-insurance
Mobilization of Wavestone forensics team on site

- From 50% to 90% of servers are down
- No more Internet access
- No more Messaging service
- No more IT administration tools
- No more usable backup servers
- From 25% to 95% of workstations are down
- Backup sites workstations are down
- No access to continuity plans
- Teams are completely lost and overwhelmed by warning messages
- High level of stress

2-3 days

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

Timeline of the cyber-crisis

… & save what can be saved

"Then I spent so many nights Just thinking how you did me wrong
And I grew strong… And I learned how to get along"

Mobilized workforce
Internals : 40-60
Wavestone : 4-5 ↗

Tuesday, June 27th
2PM-12PM

Crisis mode

"What happened? How?"
"What should we do? Shall we pay the ransom?"

Start of the investigations

- Attempt to analyze disks and logs
- Attempt to reinforce the surveillance
- Attempt to identify the malware propagation mode

First emergency actions

- Network cut off on all sites to stop the propagation
- Attempt to identify and isolate sane remaining machines
- Exchange of personal emails and phone numbers to be able to communicate

2-3 days

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

Timeline of the cyber-crisis

Re-assessment of the situation following the 1st actions

"And so you're back from outer space
I just walked in to find you here, with that look upon your face"

Mobilized workforce
Internals : 40-60
Wavestone : 4-5

Wednesday, June 28th
Morning

Crisis mode

Exhaustion of the teams

Discovery that all actions were not synchronized or efficient

First attempt to take a step back

2-3 days

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

Timeline of the cyber-crisis

Organisation of teams around streams

"I should have changed that stupid lock
I should have made you leave your key
If I had known for just one second you'd be back to bother me"

Mobilized workforce
Internals : 40-60
Wavestone : 6-7 ↗

Wednesday, June 28th
Afternoon

Crisis mode

Teams mobilization for investigation and recovery

- Creation of an investigation team to identify the root cause of the incident to rebuild safely
- Structure of the reconstruction in individual threads:
  - Active Directory, Network, Workstations, Servers and Datacenters, Security
- Specific team for international synchronization with local sites
- Establishment of rotations of the workforce: hundreds of people were mobilized 24/7 internationally

2-3 days

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

Timeline of the cyber-crisis

No DRP? Let's build our own: Defend, Rebuild, Prioritize

"Go on now, go walk out the door
Just turn around now… 'Cause you're not welcome anymore"

Mobilized workforce
Internals : 60-120 ↗
Wavestone : 15-20 ↗

Thursday, June 29th

Crisis mode

Defense plan

- Definition of measures to be applied on workstations / servers / network
- Writing and deployment of a script to be applied on sane remaining workstations and servers
  - *Vaccine file* in place, local admin password change, block 139/445 ports…

Recovery plan

- Parallel rebuilding of Active Directory, DNS, DHCP, Antivirus
- Particular focus on backup servers to have access to existing backups

2-3 days

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

3 days later…

Timeline of the cyber-crisis

At last, some success and good news

"Weren't you the one who tried to break me with goodbye?
Did you think I'd crumble? Did you think I'd lay down and die?"

Mobilized workforce
Internals : 60-120
Wavestone : 15-20

Sunday, July 2nd

Crisis mode

First machines recovered and secured

- Core infrastructure is recovered (AD, DNS, DHCP, Antivirus…)
- Critical business applications are recovered (ERP systems…)

New secured PC masters are created

Some investigations still on going

2-3 days | **1-2 weeks**

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

3 days later…

Timeline of the cyber-crisis

Time to think about end-users

"Oh no not I, I will survive
For as long as I know how to love, I know I'll stay alive"

Mobilized workforce
Internals : 60-120
Wavestone : 15-20

Wednesday, July 5th

Crisis mode

Between 20% and 50% of servers recovered

Definition of a "Do It Yourself" PC recovery plan:
USB keys to be sent to users, to re-install their PC by themselves

Differences in investigations success leading to different strategies for rebuilding

2-3 days | **1-2 weeks**

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

5 days later…

Timeline of the cyber-crisis

I'll survive! I will survive!

"I've got all my life to live
And I've got all my love to give"

Mobilized workforce
Internals : 60-120
Wavestone : 15-20
End-users : all ↗

Monday, July 10th

Crisis mode

Starting the execution of the PC recovery plan

Between 50% and 100% of servers recovered

Depending on context, all servers recovered and network reconnected or, due to investigations still ongoing and extra precaution, pursuit of servers recovery

2-3 days | **1-2 weeks**

Mobilisation & 1st actions | **Central recovery** | **Local recovery**

21 days later…

Timeline of the cyber-crisis

"I used to cry, but now I hold my head up high
And you see me, somebody new"

Mobilized workforce
Internals : 40-60 ↘
Wavestone : 4-5 ↘

Monday, July 31st and onwards…

~~Crisis mode~~

Almost all servers and PCs recovered

Progressive return to normal conditions of work

Launch of projects to reinforce the global security level

2-3 days — **Mobilisation & 1st actions**

1-2 weeks — **Central recovery**

1 month + — **Local recovery**


Focus on the rebuilding

Zoom on crisis management organization

A tightened governance

- A daily **business** oriented Steering Committee, chaired by the Executive Director
- A daily **IT** crisis management Steering Committee, chaired by the Executive Director (and occasionally by the CEO)

A structuration in individual streams to rebuild

- Active Directory, Network, Workstations, Servers and Datacenters, Security
- Everyone working in the same open space
- 1 PMO in each stream, and a global governance in crisis cell
- Establishment of 24/7 rotations :
  - 2x12 at the beginning, then 3x8

Lessons learned

- A clear **crisis management process** to be defined and regularly tested
- A particular attention to the reporting and communication, to **convey positive messages**

How to build a healthy IS in two weeks (1/3)

Recover the network

- Get control back on FW and network equipment
  - Use of contractors laptop was necessary
- Create **isolated DMZs** on which rebuild will be performed
- Erase and dedicate physical servers and hypervisors to host these new DMZs

Rebuild core infra

- Define a new up-to-date Windows Server master
- Restore and sanitize **Active Directory** backup
  - Microsoft took 1 week to quarry the backup
  - Deletion of all privilege accounts
  - Hardening (ANSSI, editors…)
- Install a new **AV** infrastructure
  - With manual update installation
- Install a new **SCCM** infrastructure
  - With workstation deployment capabilities

How to build a healthy IS in two weeks (2/3)

Build of a new secured master for workstations

- *Vaccine* in place (C:\Windows\perfc), in readonly, size 0
- Local admin password different for each machine
- Up-to-date Antivirus
- Windows Firewall: block inbound flows (139 and 445)
- Disabling SMBv1, NetBIOS and PS Exec
- Disabling MSOffice macros
- Encrypt passwords stored in OS cache
- **Test the efficiency**

Industrialize workstations rebuilding

- **Thousands of USB keys** ordered with the new master embedded
- **New hardware bought** when existing workstations were not compatible
- USB keys **distributed to all users**, with a procedure to re-install
- **Norton Ghost** farm setup by IBM
  - Capacity: 200 workstations in 4 hours
- **PXE from SCCM** on a dedicated VLAN
  - Time reduced to 1 hour

- Local IT teams provide support if necessary
- Sane and secured PCs are marked with a colored sticker

Focus: Hardening with a "testing lab"

Honeypot

Isolated Lab

Efficiency Assessment	
Deactivation of MSOffice macros	☆☆☆☆☆
Up-to-date Antivirus	★☆☆☆☆
Encrypt passwords stored in OS cache	★★☆☆☆
Windows Firewall: block inbound flows (139 and 445)	★★★☆☆
Deactivation of SMBv1, NetBIOS and PS Exec	★★★★☆
Local admin password different for each machine	★★★★☆
Vaccine in place (C:\Windows\perfc), in readonly & size 0	★★★★☆

How to build a healthy IS in two weeks (3/3)

Rebuild collaborative tools

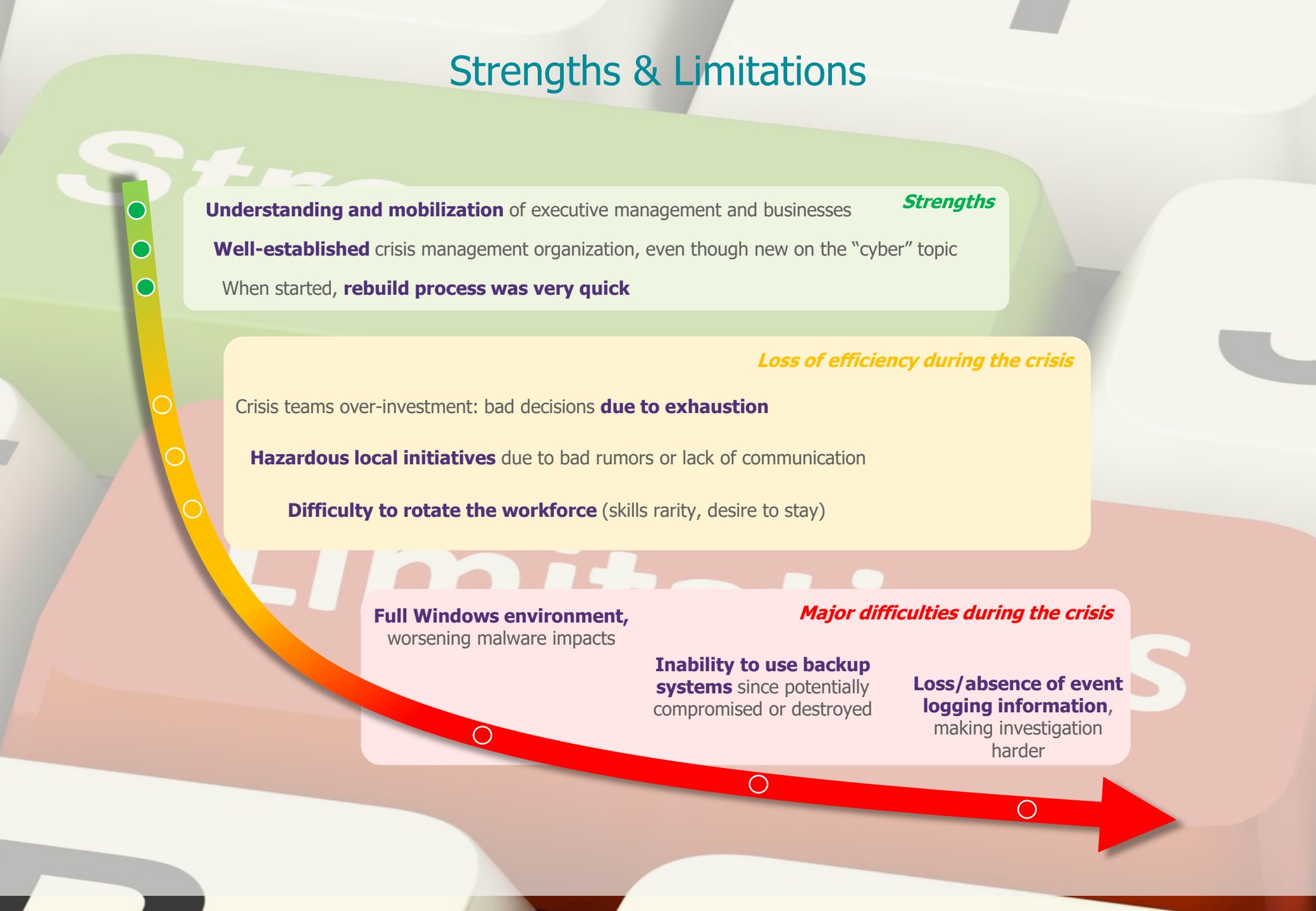
- Migration to **Office 365**
  - Prevent users from using their personal email
  - Doesn't require the rebuild of Active Directory
  - Microsoft created 4k accounts in 3 days
- Use of MI6 solution and MFT
  - Share documents between investigators and different teams involved

Recover the servers

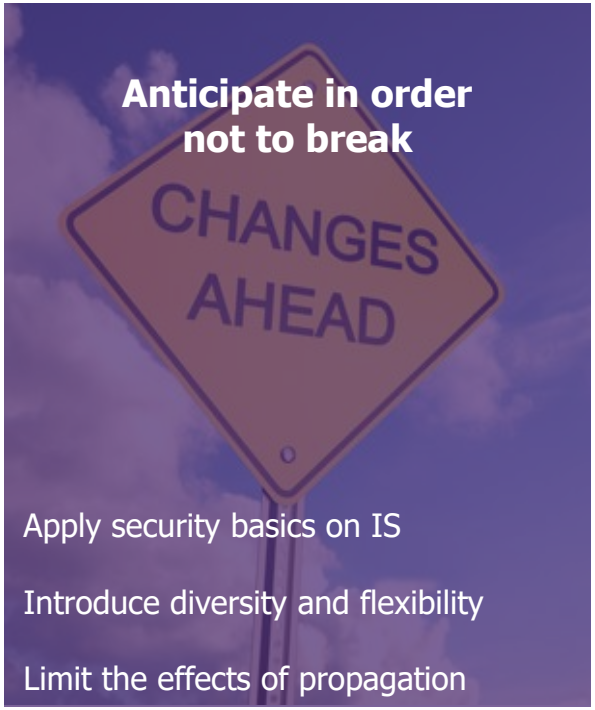
- **Editor's intervention** was needed to recover backups
  - **10 days** were necessary to recover the first server
- Once sanitized, servers were moved into new production DMZs
- Servers were sanitize in an **isolated DMZ**
  - AV installation
  - Hardening script application kill-switch, SMBv1 deactivation, AV update…)
  - Update Windows
  - Local accounts deletion

Key Takeaways

Strengths & Limitations



Lessons Learned

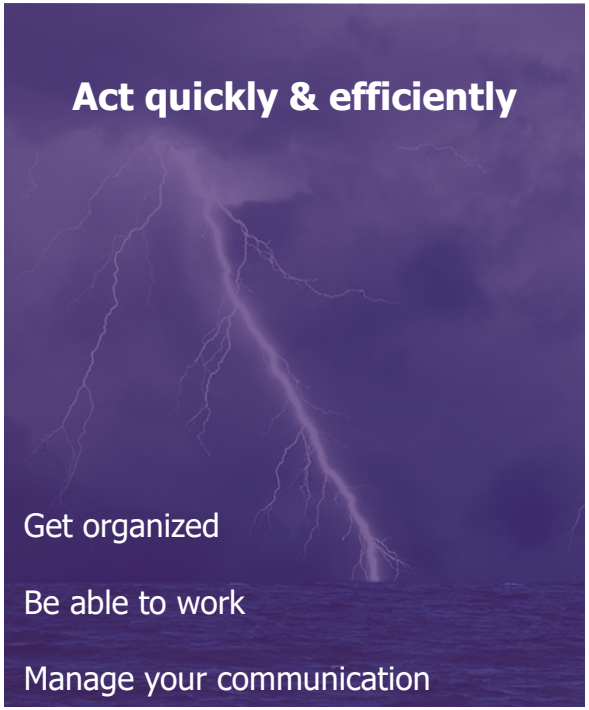


Anticipate in order not to break

Apply security basics on IS

Introduce diversity and flexibility

Limit the effects of propagation



Act quickly & efficiently

Get organized

Be able to work

Manage your communication

Rebuild fast & sane

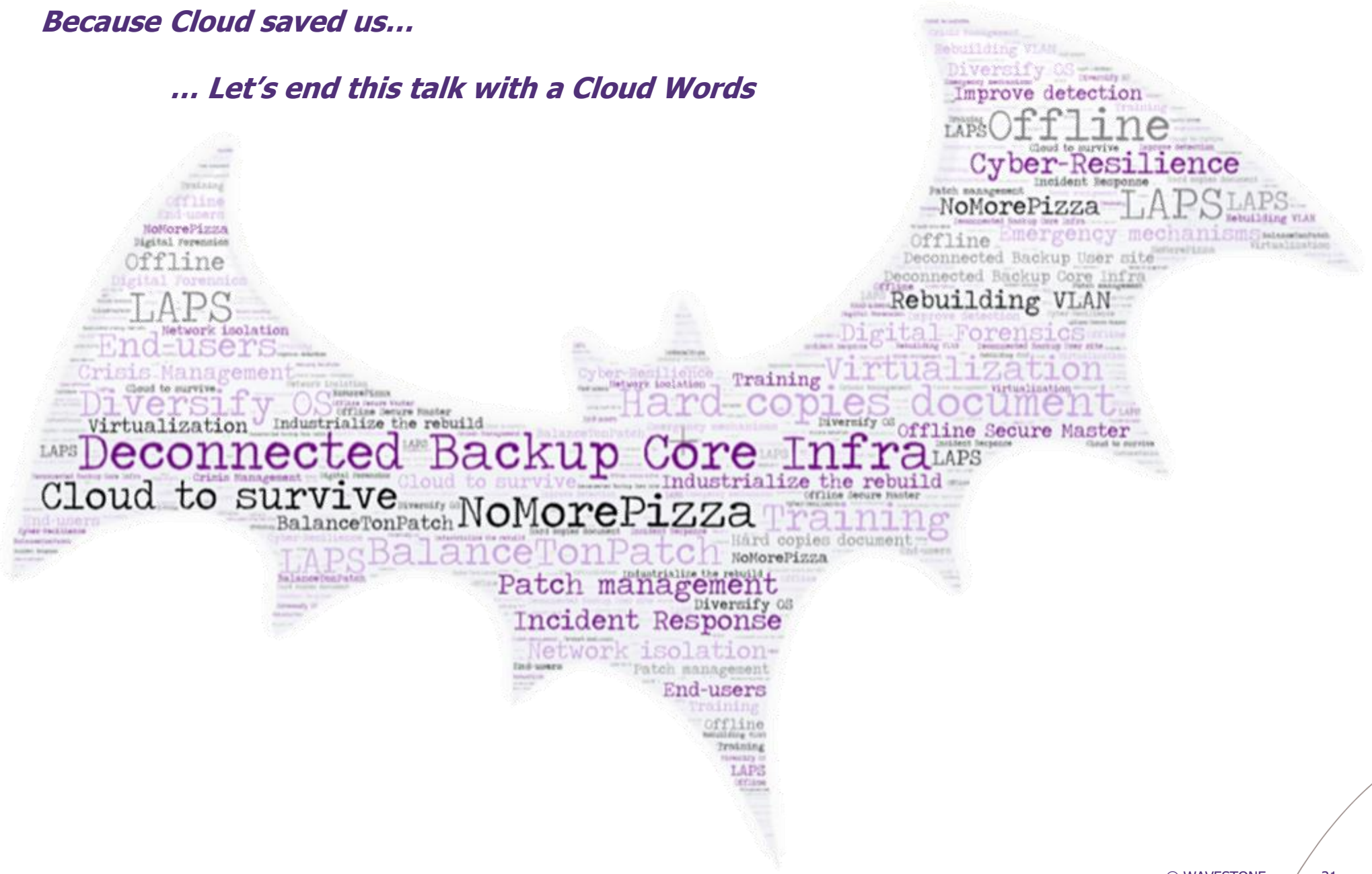
Ensure the rebuild is sane

Industrialize the rebuild

Specific attention on rebuilt systems

Because Cloud saved us…

… Let's end this talk with a Cloud Words



WAVESTONE

Vincent NGUYEN
CERT-W - Manager

M +33 (0)7 62 83 13 61
vincent.nguyen@wavestone.com

Quentin PERCEVAL
CERT-W - Responsable des opérations

M +33 (0)6 68 87 16 60
quentin.perceval@wavestone.com

http://www.securityinsider-wavestone.com

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE