TV5MONDE

TV5MONDE cyber-attack
crisis management and feedback analysis

Alexis RENARD

2016/09/09 15:00

TV5MONDE

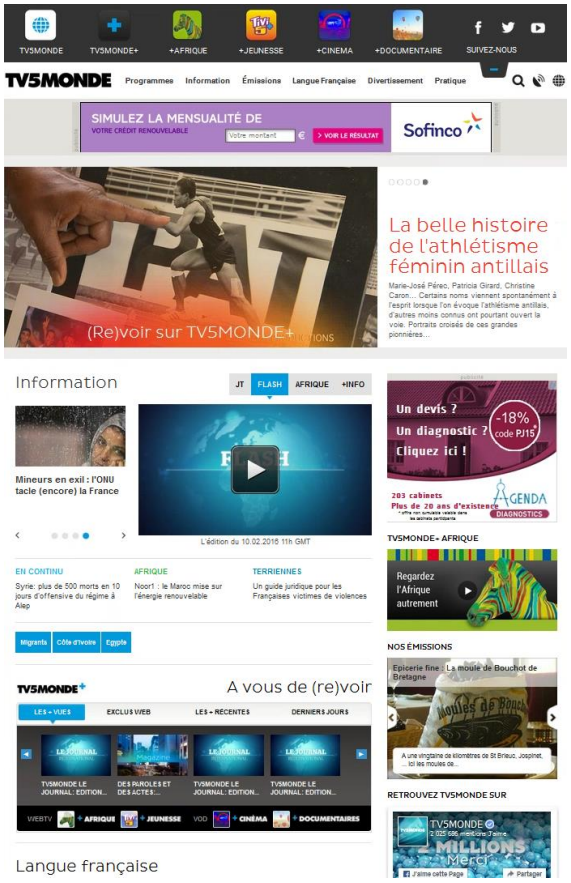
Overview

- Company presentation
- Recall of facts
- Incident response actions
- Lessons learned from the event
- Operational impacts and challenges
- Information system security management
- Conclusion

TV5MONDE

TV5MONDE

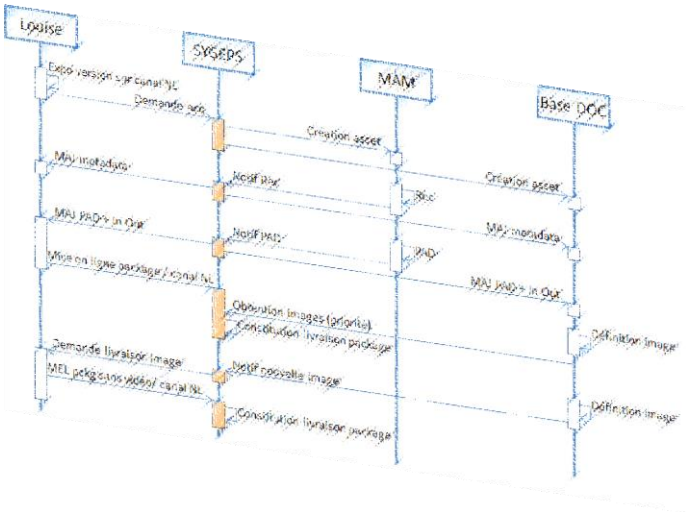
- Present in more than 200 countries and territories
- Broadcast in 250 million connected households
- 9 general interest channels specific to each continent
- 4 thematic channels
- Broadcasted in french only with multi-lingual subtitling



TV5MONDE

IS features

- Technical facilities
  - Dozens of thousands hours of video content
  - 5 functional zones
  - 1200 servers and 400 workstations
  - 30 business processes and 20000 daily workflows
- High availability
  - Operations 365/24/7
  - No SPOF
- Hyper-connectivity



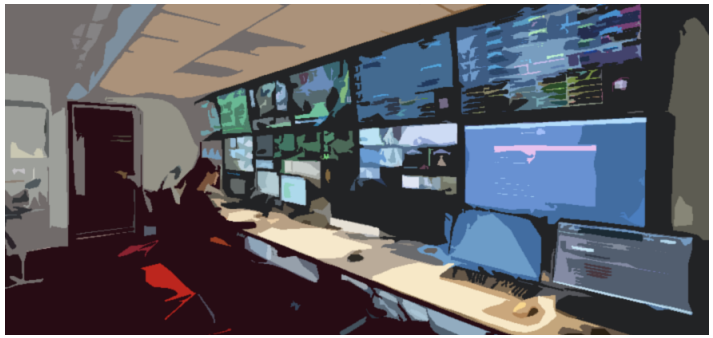
BORDERLESS CYBER

Europe 2016

TV5MONDE

Recall of facts

- April 8th 8:30 pm : beginning of the attack
- Red alerts and black screens
- Destroyed components
- Coordinated attack
- Controlled from outside



Approaching phase

- Spear phishing campaign
- Malicious software reaches email server
- Fake web site for trapping service provider users and stealing administrator account
- Using VPN and installing 0-day malware and keylogger

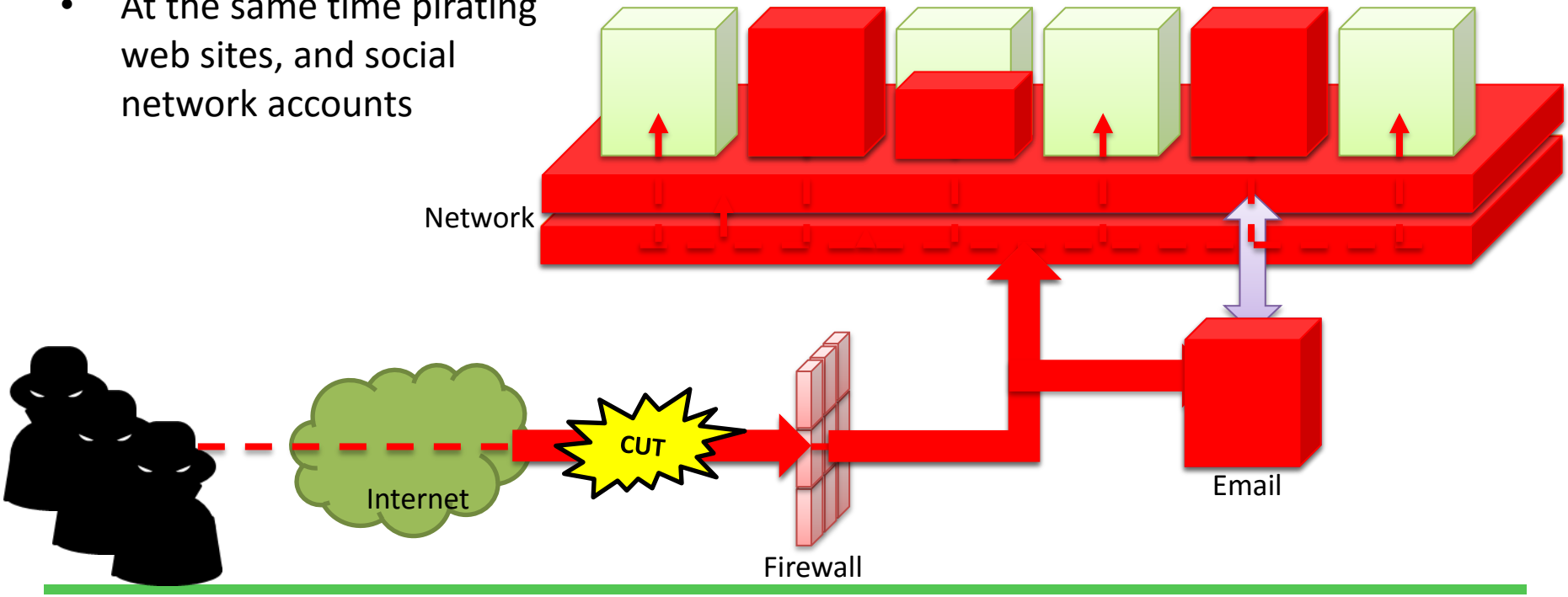
Observation phase

- Using backdoors and remote access tools through VPN channels
- Several months of network observation
  - Information system comprehension and cartography

TV5MONDE

Attack phase

- On April 8th, several attackers act simultaneously according to a structured plan of methodical destruction
- Sabotage of several core components in the information system
- At the same time pirating web sites, and social network accounts



TV5MONDE

First hours

- Network switch off and major services shutdown
- 11:00 pm : General Director crisis meeting
- Reestablishing basic signal in the middle of the night
- Progressive restart of major services the following morning and afternoon
- ANSSI joined us early in the morning

First days and short term actions

- Incident response
  - Attack analysis and information system check
  - Recovery and hardening
- Isolating compromised components
- Reduced functionality operational mode
- AD switch over
  - Several weeks preparation
  - Successfully realised in 24 hours
  - Without interruption of broadcasting services

Internal communication

- Regular and frequent internal communication of security rules
  - April 9th : massive display campaign on premise (+ emails + sms)
  - April 17th : browsing internet, using intranet and IT tools
  - April 22th : using USB drives and exchanging files
  - May 3rd : general IT rules
  - August 4th : using smartphones
  - August 21st : reinforcing rules on password policies, using computers and smartphones
  - September 8th : reinforcing rules on securing email accesses, computer and smartphones passwords policies
- Communication never stopped

TV5MONDE

Middle term actions

- Working on enhancing global IS security without decreasing productivity
  - Preparing content, news, programs
  - Broadcasting multiple TV channels
  - Publishing online digital content (web, catch up, mobile platform)
- Progressively reestablishing 100% of businesses and activities
- Implementing and relying on IDS/IPS services

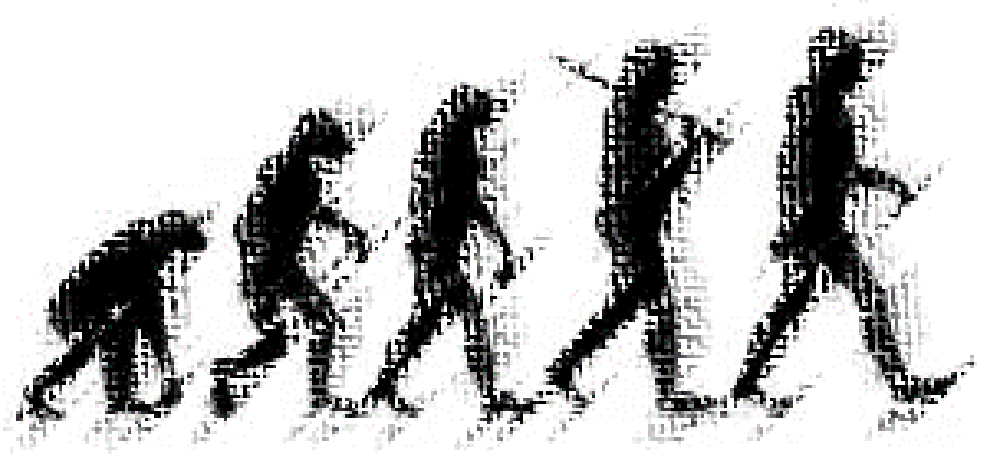
Reaction

- In the whole company
- What happened and what to improve and work on
- Massively communicating with internal users, business partners and service providers
- Increasing global IS security level
  - Strong commitment from General Direction
  - Remarkable involvment from users
- Sharing experience and best practices with other broadcasters and CTOs

TV5MONDE

Lessons learned

- Anybody can be hacked !
- BUILD : consider IS security at the earliest stage of your project
- RUN : maintain IS security management as a continuous process
- Align IS security level and i challenges and budget



User's side

- Strenghtened authentication (passwords policy, personnal sessions, faster standby, …)
- Strict boundaries between main business tools and Internet
- Hardening video media flows and exchanges (inputs and outputs)
- Managing remote working and users mobility
- Trainings
  - Following company IS security rules
  - Getting good IT and security practices
  - Including at home

TV5MONDE

Technologies and vendors

- Strenghtening authentication
- Installing security patches
- Managing obsolescence
- Keeping documentations and cartographies up to date
- Adopting best IS security practices
- We are working on getting commitments from hardware and software vendors

TV5MONDE

IS security management

- IS security governance
- Documentation
- Providers
- Events and incidents
- Risks
- Credentials
- Trainings
- Security KPIs
- Compliance
- Internal audits
- Company global IS security policy

TV5MONDE

Conclusion

- A dramatic speed up
- Adapt to IS security
- Focus
  - Getting out of crisis mode
  - Communication
  - Vendors and solution providers