The Investigation

"Investigating is hard"[citation needed]

Facing the logs

- A complex killchain
- Attacks, noisy, or not
- Logs captured from various sources, not uniform...
- Not always human-readable values

Use what's given to you

~~À l'aide de l'énoncé,~~

Good news – We have some info

There's a ransomware involved. There's an IDS: Suricata. We have the topology at our disposal.

Bad news – We have no idea where to start

Do not fret !

Using our expert knowledge

~~À l'aide de vos connaissances...~~

Suricata records event severity

- Severity 1 is the highest degree
- There are only 14 alerts classified as such
- There's a CVE number in them !

The initial compromission

This CVE is a **log4j** exploitation. So that's how our webserver got infected. Better update our Tomcat huh.

Ok, from there, what do I do ?

Finding out the rest

~~Show your work~~

Fiddling around with anything the webserver interacts with

This is where it gets tricky. I don't instantly find anything that weird. That's fine I just look for things sent to the webserver instead of what it does. I find a **payload.ps1 meaning powershell use.** And here I don't find anything more for now

Start back from the attacker's machine

It discusses with the AD, client2, the webserver and the NTP server. Maybe that's my next step.

What happened on those machines ?

Finding out the rest

~~Show your work~~

Looking at timestamps

As we know the webserver was the first to be compromised. Client2 seems to be the second one. Somehow he used some **powershell** and downloaded some files using **wget**

Some noise, finally

A series of discovery actions ensue to find out open ports, applications installed, users...

→ This was in the shape of encoded powershell commands

And then ?

The filenames previously downloaded clearly inform us of the attackers intentions.

Goals of our attacker

Discovering the capacities and ressources of the machine

See who it can communicate with

Persistency

Compromising the AD

Profit ?

Finishing the job

~~Get a good grade~~

Compromising the AD

Here our attacker used an exploitation of the vulnerability **Zerologon** to be able to impersonate the AD administrator

A new power

Instantly abusing his new powers our attacker instantly dumps all the credentials in the AD and now has access to everything

Impact

The final attack is **ransomware.exe** and you know where this is going...

Figures from the exercise

100% had fun. We hope.

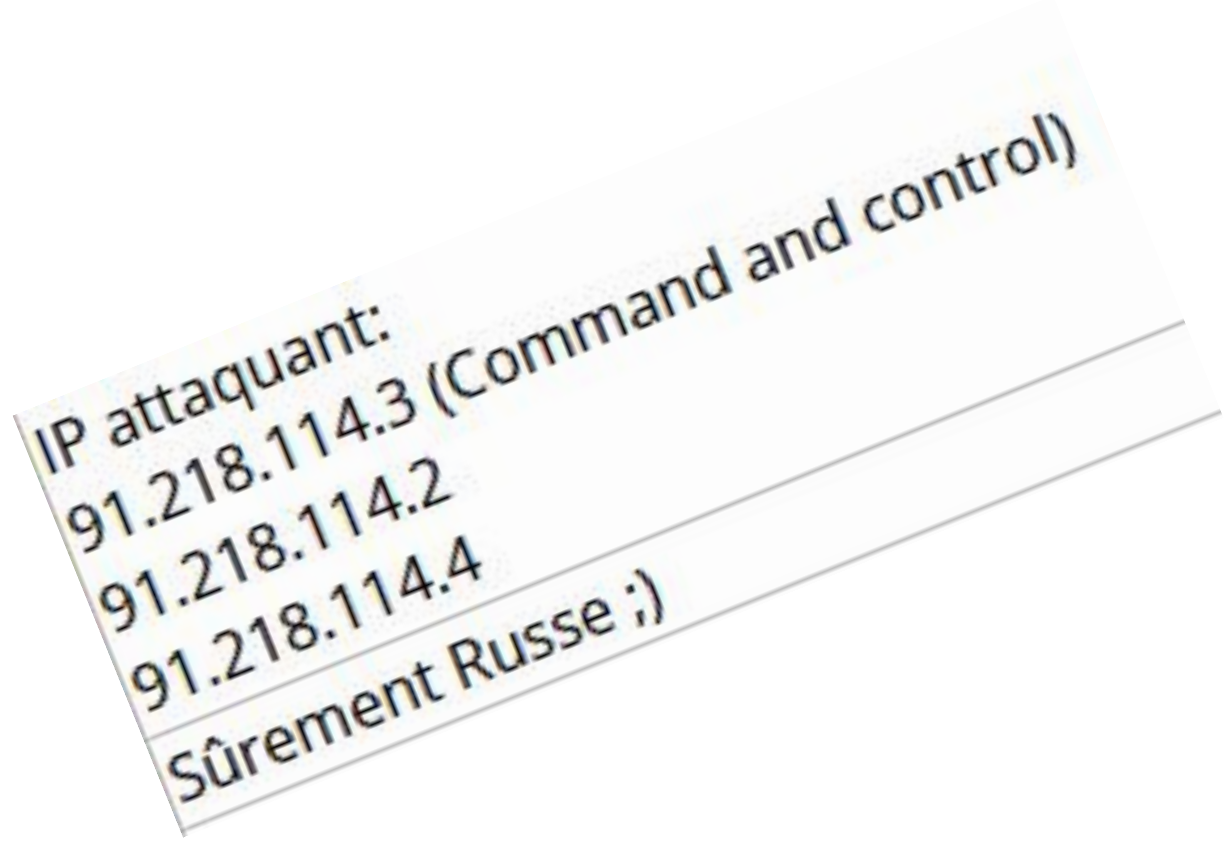
2 Sessions

32 participants

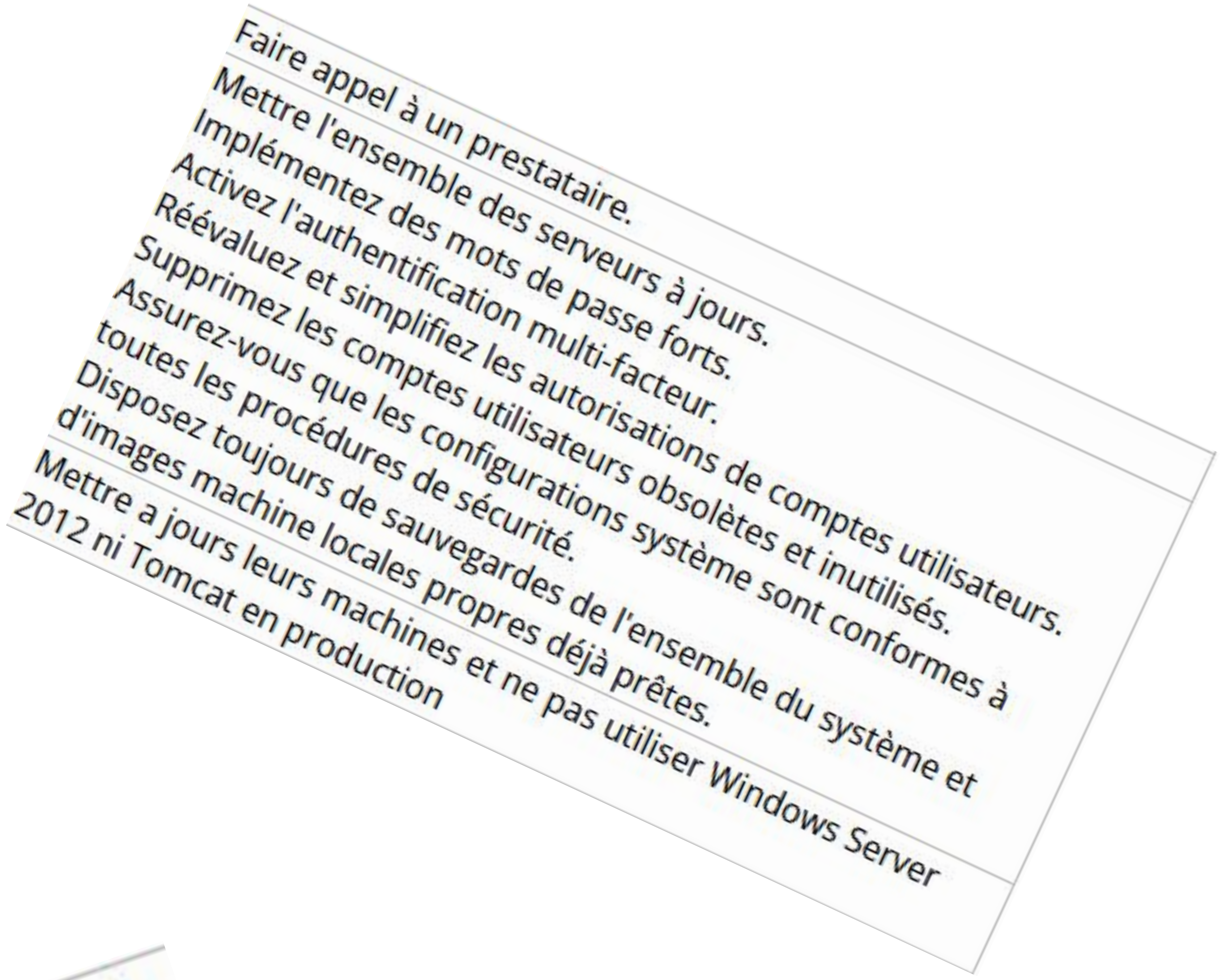
17 attacks to uncover

6 Winners

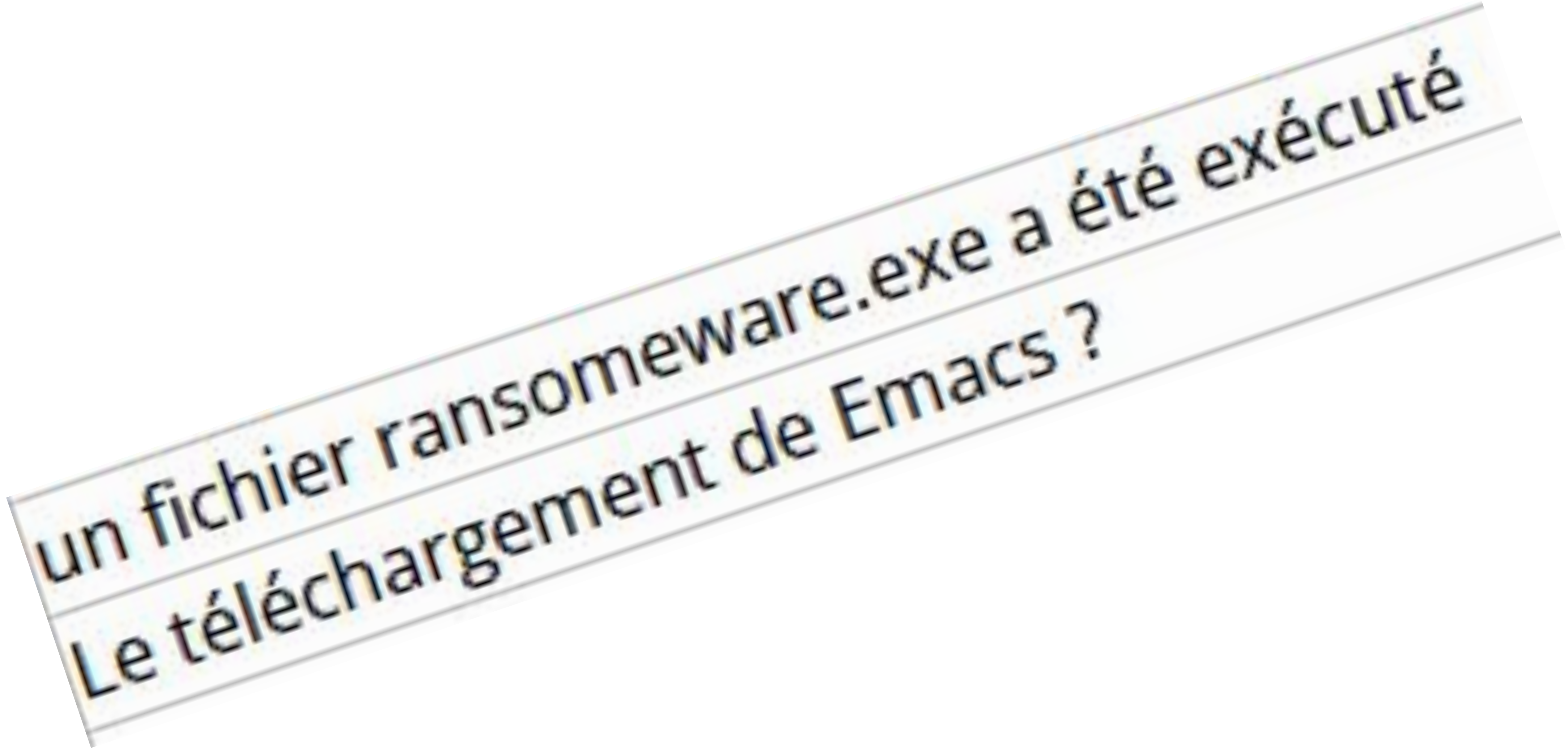
Thanks !



IP attaquant:
91.218.114.3 (Command and control)
91.218.114.2
91.218.114.4
Sûrement Russe ;)



Faire appel à un prestataire.
Mettre l'ensemble des serveurs à jours.
Implémentez des mots de passe forts.
Activez l'authentification multi-facteur.
Réévaluez et simplifiez les autorisations de comptes utilisateurs.
Supprimez les comptes utilisateurs obsolètes et inutilisés.
Assurez-vous que les configurations système sont conformes à toutes les procédures de sécurité.
Disposez toujours de sauvegardes de l'ensemble du système et d'images machine locales propres déjà prêtes.
Mettre a jours leurs machines et ne pas utiliser Windows Server 2012 ni Tomcat en production



un fichier ransomeware.exe a été exécuté
Le téléchargement de Emacs ?

Malizen

Data Science to accelerate cybersecurity.

romain@malizen.com