

## Veille Technologique Passive

Les cyber-attaques font partie des menaces les plus graves à l'heure actuelle qui planent sur l'État, les institutions publiques et les entreprises privées. Le Ransomware fait partie des menaces majoritaires et il n'épargne donc aucun organisme. Nous verrons donc l'impact qu'il a au sein des entreprises.

L'entreprise, c'est une cible privilégiée par les pirates informatiques car elle dépend énormément de la technologie, encore plus avec le nouvel air de "l'industrie 4.0". Le ransomware est un des fléaux qui touche ce milieu et on l'a vu récemment avec l'attaque Akira envers Technology Group :



The terminal window has a green title bar with the text '[ AKIRA ]'. The main area of the terminal is black with white text. At the top, it says 'AKIRA'. Below that is a message: 'Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.' Another message follows: 'Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.' A third message: 'Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.' A fourth message: 'Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.' Below these messages is a command-line interface. It starts with 'guest@akira:~\$ help', followed by a list of commands: 'List of all commands:'. The commands and their descriptions are: 'leaks - hacked companies', 'news - news about upcoming data releases', 'contact - send us a message and we will contact you', 'help - available commands', and 'clear - clear screen'. The session ends with 'guest@akira:~\$'.

Ces attaques consistent à demander une rançon aux victimes comme son nom l'indique, pour que le PC ou les fichiers soient de nouveaux accessibles. En effet, elles pourraient être évitées : en renforçant le système de sécurité informatique comme par exemple, mettre à jour ses outils régulièrement ou encore éviter les

tâches automatisées au sein des applications, qui facilitent la propagation des rançongiciels.

Pour conclure, les ransomwares dans le monde de l'entreprise sont un réel problème d'une part parce que cela paralyse la production et d'autre part parce que la prévention n'est pas encore au point. Les campagnes de sensibilisation à la cyber sécurité permettrait de minimiser voire éviter certaines de ces attaques et on peut se demander si elles sont réalisées de manière réellement efficace au sein des entreprises ?

## **SOURCES :**

### **Grâce à l'outil Feedly**

- <https://www.economie.gouv.fr/entreprises/rancongiciels-ransomware-protection#:~:text=Veillez%C2%A0%C2%80%C2%80mettre%C2%A0%C2%80%C2%80jour,via%C2%A0les%C2%A9v%C2%A9n%C2%A9ments%C2%A9s%C2%A9s%C2%A9des%C2%A9applications>.
- <https://www.redpacketsecurity.com/akira-ransomware-victim-pgf-technology-group/>