Plateforme de tests & honeypot pour l'IOT

Auteurs : Jérémy D'Adamo – Bilal Mersali – Victor Séjourné

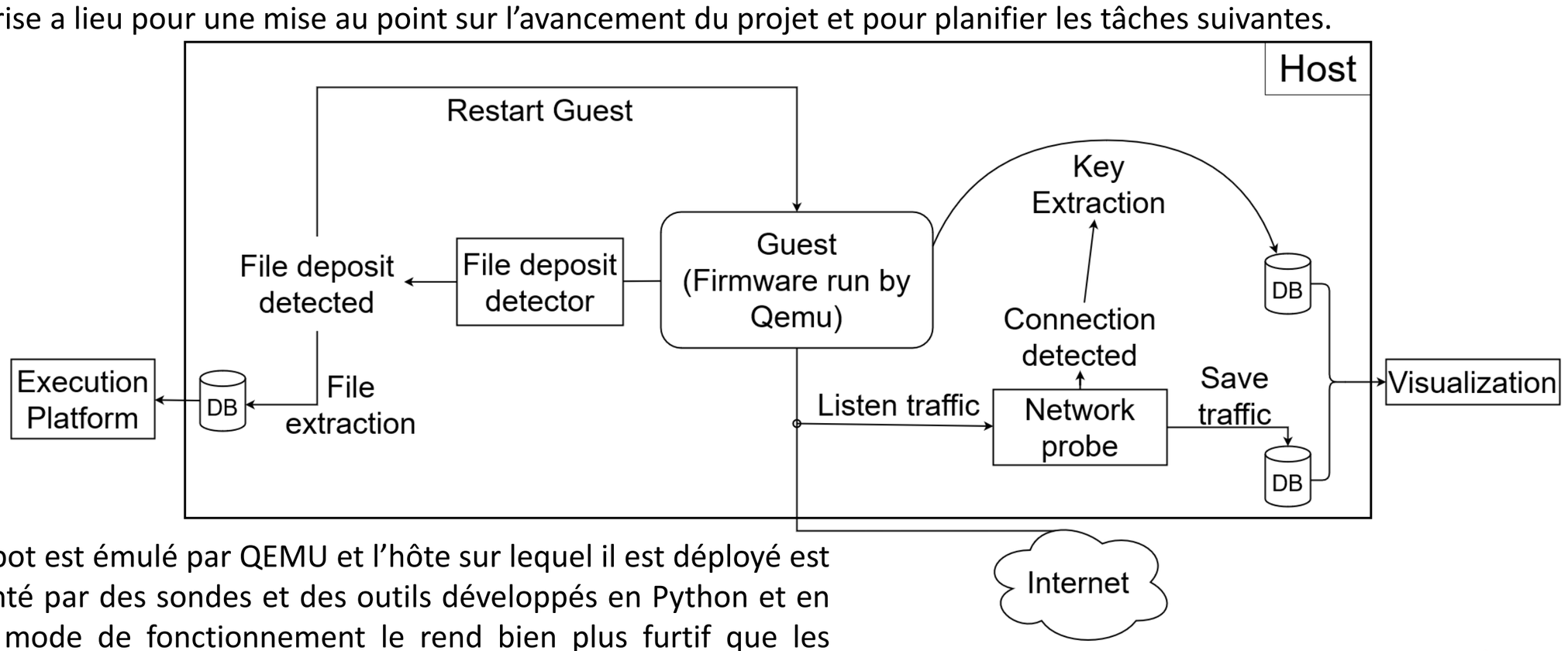
CONTEXTE ET OBJECTIF

Le programme PULSE de l'IRT Nanoelec, qui compte Grenoble-INP, UGA et le CEA parmi ses membres fondateurs, a pour objectif de renforcer la cybersécurité, en particulier dans le domaine de l'IoT. Face à la montée en puissance de la cybercriminalité, il devient nécessaire pour les industriels d'inclure la sécurité dans leurs processus de développement.

L'objectif du projet est la mise en place d'une machine de leurrage numérique (honeypot) basée sur une architecture ARM, comportant un serveur web et un serveur SSH puis de l'exposer sur Internet. Celle-ci va faire l'objet de tentatives d'attaque et de dépôt de fichiers par des attaquants humains ou des programmes automatisés. Les malwares déposés sont récupérés pour être analysés ultérieurement et les informations comme les identifiants/mots de passe, l'adresse IP, les URLs accédées ou encore la localisation de l'attaquant sont relevées afin de réaliser des statistiques. Ces informations sont ensuite affichées sur une interface graphique (SIEM) et vont permettre de comprendre l'évolution des attaques dans le monde de l'IoT.

MÉTHODES ET DÉVELOPPEMENTS

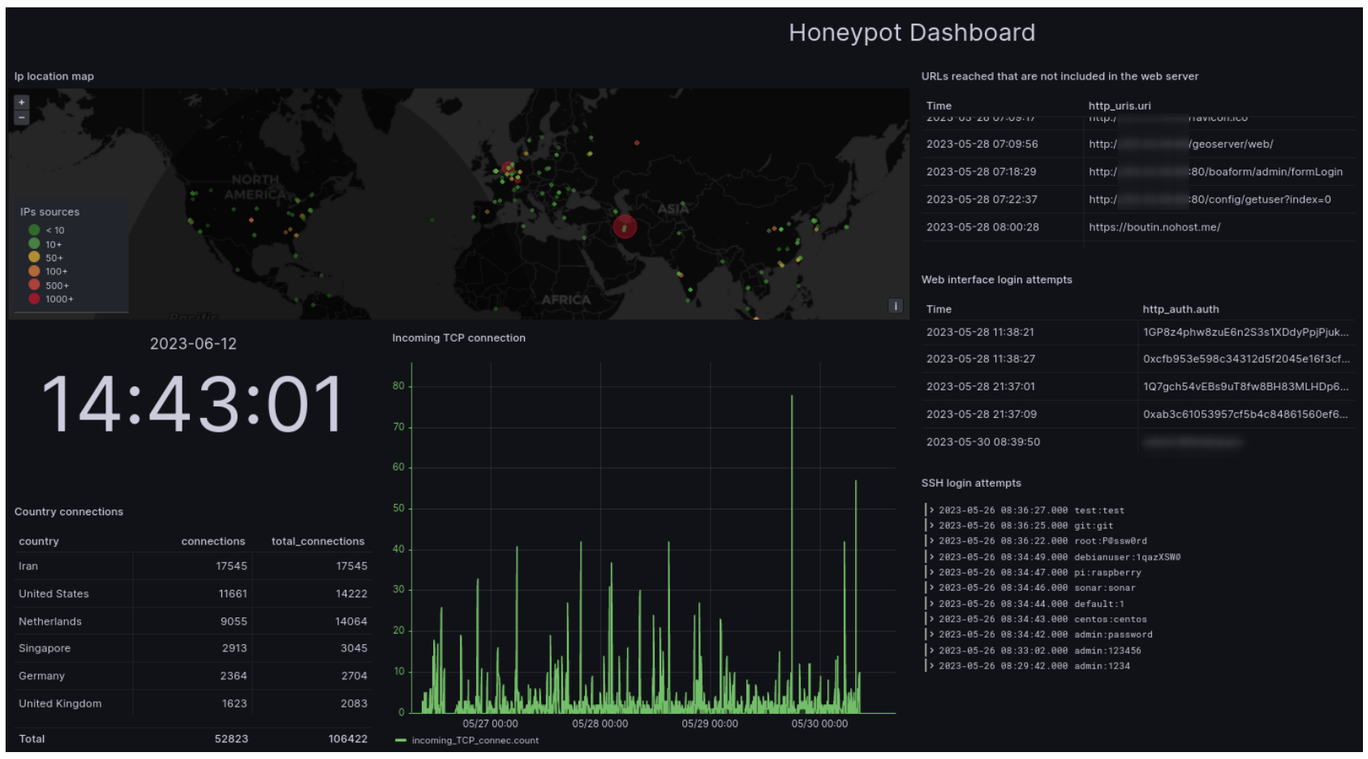
L'organisation du projet est basée sur la méthode Agile Scrum, consistant à découper le projet en plusieurs sprints d'une durée de 2 semaines chacun. Durant un sprint, des tâches sont listées avec un degré d'avancement. A la fin d'un sprint, une réunion avec l'entreprise a lieu pour une mise au point sur l'avancement du projet et pour planifier les tâches suivantes.



Le honeypot est émulé par QEMU et l'hôte sur lequel il est déployé est instrumenté par des sondes et des outils développés en Python et en Bash. Ce mode de fonctionnement le rend bien plus furtif que les honeypots avec agent. Les informations récoltées par les sondes sont affichées sur un dashboard Grafana et les malwares déposés par les attaquants sont analysés sur VirusTotal.

RÉSULTATS ET CONCLUSION

Le projet a démontré la faisabilité de la mise en place d'un honeypot sur une architecture ARM.
Le honeypot est basé sur un firmware commercialisé de l'IoT et est introspecté de manière furtive afin de leurrer plus efficacement les attaquants.
Celui-ci est capable de déchiffrer les connexions HTTPS et SSH en extrayant les clés de chiffrement.
Depuis le dashboard, il est possible avec le trafic en clair de localiser les attaques, connaître les URLs les plus demandées ou encore les identifiants les plus essayés lors de tentatives de connexions.



MOTS-CLÉS : Honeypot – IoT – Malware – Architecture ARM