DEEP TECH CYBER

FRANCE RECHERCHE CENTRE

FRANCE RESEARCH CENTRE

DÉTAILS DES COMPÉTENCES

A. Technologue en cybermalwares

1. Rechercher et comprendre les algorithmes d'infection de pointe utilisés dans la nature.
2. Responsable de l'identification et de la recherche de nouveaux points d'infection détenus par la plateforme cible.
3. Effectuer des recherches sur les parasites (stratégies ret-to-OEP également).
4. Recherche sur les composants internes du système d'exploitation.
5. Recherche sur les théories mathématiques autoréplicatives.
6. Rechercher et effectuer une analyse post-mortem et déterminer l'exploitabilité de la vulnérabilité trouvée.
7. Recherche et rédaction d'exploits pour diverses classes de bogues (y compris les corruptions de segments de pile/tas/données, etc.).
8. Recherche sur la réalisation de contournements et recherche sur les atténuations appliquées par l'application cible.
9. Recherche pour réaliser l'exécution de l'implant de 1ère étape (exécution de code arbitraire).

10. Rechercher et comprendre les techniques d'exploitation de pointe utilisées dans la nature.
11. Familier avec les environnements Malware Sandbox
12. Recherche Linux
13. Recherche et expérimentation de loaders et droppers écrits dans de nouveaux langages
14. Rechercher, expérimenter et exécuter le codage de logiciels malveillants
15. Préparer la documentation de recherche sur les logiciels malveillants
16. Recherche sur le contournement des signatures et l'analyse basée sur l'heuristique.
17. Recherche sur le développement et le contournement de la détection basée sur le bac à sable.
18. Recherche sur l'anti-analyse (compilation) et l'anti-débogage (détection à l'exécution des outils d'analyse dynamique)
19. Recherche sur la kleptographie et les canaux subliminaux
20. Recherche sur le développement et l'intégration de techniques furtives aux logiciels malveillants