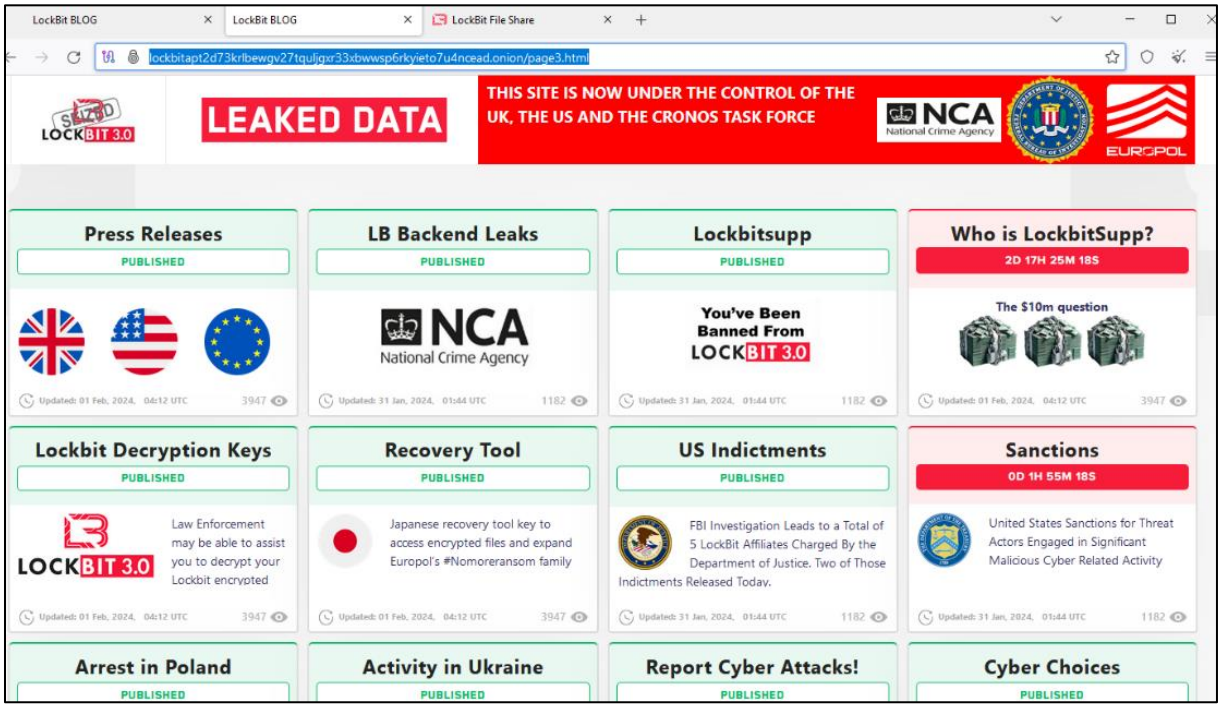
Cyber Hackademy

Red Team – zadanie 3 (Purple Teaming)

W lutym 2024, dzięki skoordynowanej akcji służb wielu państw, udało się zatrzymać operacje cybergangu LockBit. Zatrzymań dokonano na terenie Ukrainy oraz Polski. Po udanej akcji, służby przeprowadziły *defacement* serwisu, na którym gang publikował dane ofiar:



Więcej informacji o *Operacji Cronos* możesz przeczytać na:

[Feds Seize LockBit Ransomware Websites, Offer Decryption Tools, Troll Affiliates – Krebs on Security]

Zadanie

Na podstawie danych znalezionych w Internecie, zaplanuj ćwiczenie *Purple Team*, w trakcie którego będziesz symulował operacje grupy LockBit. Ćwiczenie będzie miało na celu zweryfikowanie czy zespół SOC klienta jest w stanie wykryć poszczególne etapy cyberataku. Na użytek ćwiczenia, wykorzystamy standardowy model cyber killchain:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objective

Do każdego z powyższych etapów, znajdź informacje na temat technik, taktyk i procedur grupy LockBit, które zostały zaobserwowane w historycznych atakach. Pamiętaj o dokładnym wskazaniu źródeł, z których korzystasz.

Dla każdego kroku podaj nazwy narzędzi z których będziesz korzystał oraz wskaż umiejscowienie symulacji w sieci: własna infrastruktura, infrastruktura zewnętrzna klienta (poziom sieci Internet) lub sieć wewnętrzna klienta (LAN).