Отчёт

Методика:

Анализ DNS-запросов в Wireshark

Поиск доменов с цифровыми последовательностями

Проверка на VirusTotal

|  |
| --- |
| Результат: |
| Обнаружен вредоносный домен: 6449584247ac64f2e2d2498a2d38c5a2e2d2498a2d38c5a2.1yf2g3p4y5t6q7r8e9w0r[.]com |

2. РАСШИФРОВКА ПОХИЩЕННЫХ ДАННЫХ

Методика:

Обнаружение Base64 в DNS-трафике

Декодирование ключа RC4

Brute-force пробела в ключевой фразе

Дешифровка RC4-трафика

Найденные данные:

Base64: lNIyF8hH0U0pW5P5h7vWm8Y6K2i8n6p6m6u6r6c6d6b6a69686766

Ключ RC4: P@ssw0rd SecretKey (после brute-force)

Расшифрованное значение: classified\_data\_2024

ВЫВОД:  
Успешно идентифицирован C&C сервер и расшифрованы похищенные данные. Рекомендуется блокировка домена и усиление мониторинга DNS-трафика.