Національна поліція України

By Kitsoft

Archived: 2026-04-10 03:06:04 UTC

За допомогою шкідливої програми-вимагача “Clop” фігуранти криптували дані, що знаходилися на інформаційних носіях компаній у Республіці Кореї та США. Надалі за відновлення доступу вимагали гроші.

Хакерське угруповання викрили співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції. Зловмисники були викриті в рамках міжнародної операції за сприяння та координації Інтерполу (IGCI), та спільно з працівниками правоохоронних органів з Республіки Корея та США.

Встановлено, що шестеро фігурантів здійснювали атаки шкідливого програмного забезпечення типу “Ransomware” на сервери американських та корейських компаній. За дешифрування даних вимагали «викуп», а в разі несплати - погрожували оприлюднити конфіденційні дані потерпілих.

Так, у 2019 році вірусом-шифрувальником “Clop” атакували чотири корейські компанії, в результаті – було заблоковано 810 внутрішніх серверів та персональних комп’ютерів працівників. Хакери розсилали електронні листи зі шкідливим файлом на скриньки працівників компаній. Після відкриття зараженого файлу програма послідовно завантажувала додаткові програми із сервера розподілу та здійснювала повне зараження комп’ютерів жертв віддаленою керованою програмою “Flawed Ammyy RAT”.

Використовуючи віддалений доступ, фігуранти активували шкідливе програмне забезпечення “Cobalt Strike”, яке надавало інформацію щодо вразливостей заражених серверів для подальшого їхнього захоплення. За дешифровку інформації зловмисники отримали «викуп» у криптовалюті.

У 2021 році фігуранти здійснили атаку та зашифрували персональні дані співробітників і фінансові звіти Медичної школи університету Стенфорда, Університету Меріленду та Університету Каліфорнії.

На відміну від загальних атак-вимагачів, що шифрують велику кількість невстановлених персональних комп’ютерів та серверів, – це атака APT (Advanced Persistent Threat), вона націлена на комп’ютерну мережу конкретної жертви та заражає всю систему за допомогою програми-вимагача.

Загальна сума збитків сягає 500 мільйонів доларів.

Спільними зусиллями правоохоронців вдалося припинити роботу інфраструктури, з якої здійснюється розповсюдження вірусу, та заблокувати канали легалізації криптовалюти, отриманої злочинним шляхом.

Правоохоронці провели 21 обшук у столиці та на Київщині, в оселях фігурантів та в їхніх автівках. До проведення обшуків було залучено підрозділ Тактико-оперативного реагування патрульної поліції. Вилучено комп’ютерну техніку, автівки та близько 5 мільйонів гривень готівкою. На майно зловмисників накладено арешт.

Відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч. 2 ст. 209 (Легалізація

(відмивання) майна, одержаного злочинним шляхом) Кримінального кодексу України. Фігурантам загрожує до восьми років ув’язнення. Слідчі дії тривають.

Процесуальне керівництво здійснює Офіс Генерального прокурора України.

Ett fel inträffade.

Det går inte att köra JavaScript.

Департамент кіберполіції
Національної поліції України