Deanonimizacja sprawców cyberprzestępstw metodami OSINT

od <nicku> do wyroku

Zdj. Mediarecovery

Norbert Ptak

Ekspert ds. OSINT, Mediarecovery

W artykule omówiono zastosowanie nowoczesnych technik pozyskiwania i analizy informacji z powszechnie dostępnych źródeł internetowych jako narzędzia, które – łączone z tradycyjnymi metodami operacyjnymi i procesowymi – stanowi obecnie jeden z kluczowych elementów w walce z przestępczością, cyberprzestępczością i przestępstwami motywowanymi nienawiścią.

Wprowadzenie: od anonimowości do odpowiedzialności

Wielu sprawcom przestępstw w cyberprzestrzeni wydaje się, że nick, avatar bez twarzy i jednorazowy adres e-mail wystarczą, by zostać nieuchwytnym dla organów ścigania. Tymczasem nowoczesne techniki OSINT (*Open-Source Intelligence*), czyli wywiadu jawnoźródłowego, pozwalają krok po kroku przekuć pseudonim w imię, nazwisko i numer akt w prokuraturze. OSINT rozumiany jako systematyczne pozyskiwanie i analiza informacji z powszechnie dostępnych źródeł, takich jak media tradycyjne, dane administracji publicznej, publikacje profesjonalne i akademickie, dane z otwartych rejestrów handlowych czy finalnie Internetu – pod pojęciem WEBINT (*Web Intelligence*) – stał się dziś jednym z kluczowych narzędzi w śledztwach i nie ogranicza się tylko do cyberprzestępczości.

Nick jako punkt wyjścia – WEBINT

Media społecznościowe, fora, komunikatory, wycieki baz danych czy aktywność w Darknecie – wszystkie te elementy tworzą cyfrowy ślad, który przy odpowiedniej metodyce można skorelować i przypisać konkretnej osobie lub wykorzystać do uzyskania szerszego spojrzenia na śledztwo. W wielu sprawach pierwszym i jedynym punktem zaczepienia jest pseudonim używany na jednym z portali, w grze online, na forum czy w komunikatorze – dokładnie z takim scenariuszem na co dzień pracują policyjni analitycy, śledczy i prokuratorzy. Nick jest wartościowym selektorem, ponieważ użytkownicy mają tendencję do powtarzania raz wymyślonej nazwy na różnych platformach.

Zanim do gry wejdą zaawansowane narzędzia, wykonywana jest zwykle prosta analiza treści samego pseudonimu: czy zawiera imię, rok urodzenia, nazwę miasta albo inne wskazówki, które zawężają grupę potencjalnie podejrzanych osób. Kolejny krok to próba wyszukania kont należących do tej samej osoby w portalach i aplikacjach innych niż nasze pierwotne źródło.

Korelacja kont w mediach społecznościowych

To, co kiedyś wymagało żmudnej ręcznej pracy, dziś w dużej mierze wspiera automatyka i wyspecjalizowane narzędzia SOCMINT (*Social Media Intelligence*), ale kluczowe pozostaje analityczne spojrzenie człowieka.

Z jednego nicku prowadzi się ścieżkę do profilu na przykład na TikToku, Facebooku, forum dyskusyjnym czy niszowym komunikatorze – każde z tych miejsc może ujawniać inne informacje: zdjęcia, lokalizacje, listę znajomych, deklarowane miejsce pracy czy zainteresowania.

Analiza profili obejmuje między innymi treści postów, styl wypowiedzi, częstotliwość publikacji, geolokalizację zdjęć i relacji, a także powiązania społeczne – wspólne fotografie, komentarze, oznaczenia osób czy przynależność do konkretnych grup. Na tej podstawie może zostać zbudowany graf powiązań, który pozwala zidentyfikować osoby z bliskiego otoczenia sprawcy oraz zweryfikować hipotezy co do jego tożsamości i miejsca przebywania.

Fora, Darknet i komunikatory

Dla sprawców poważniejszych przestępstw naturalnym środowiskiem są zamknięte fora, serwisy w Darknecie i komunikatory, takie jak: Telegram, Signal czy Discord, które często oferują niższy poziom moderacji i większą swobodę działania. Także tam OSINT ma zastosowanie – analitycy, monitorując wybrane słowa kluczowe, nazwy kanałów, ogłoszenia sprzedaży czy oferty, mogą powiązać ujawnione nicki, adresy e-mail, numery telefonów z innymi aktywnościami w sieci.

W praktyce prowadzi to na przykład od pseudonimu sprzedawcy z darknetowego forum, przez jego konto na komunikatorze, aż po profil w serwisie programistycznym czy mediach społecznościowych, gdzie pojawia się to samo zdjęcie, charakterystyczny podpis albo e-mail.
Korelacja tych danych z informacjami z rejestrów publicznych czy danych abonenta pozyskiwanych przez służby w trybie procesowym pozwala już przejść z poziomu hipotezy OSINT do twardego dowodu łączącego konkretnego człowieka z określoną aktywnością w sieci.

Mowa nienawiści i nawoływanie do przemocy – dlaczego OSINT jest kluczowy

Razem ze stałym wzrostem liczby aktywnych użytkowników rośnie liczba przypadków szerzenia mowy nienawiści w sieci, a skrajne treści publikowane online mogą przekładać się na realne incydenty przemocy – od przestępstw z nienawiści po ataki motywowane ideologicznie.
Monitoring treści w mediach społecznościowych pokazuje, że największy udział w rozpowszechnianiu mowy nienawiści mają duże platformy – takie jak X (dawny Twitter) czy Facebook – ale nie można lekceważyć mniejszych serwisów, grup na komunikatorach ani lokalnych forów.
Deanonimizacja sprawców gróźb karalnych, uporczywego nękania, stalkingu czy nawoływania do przemocy wymaga nie tylko zabezpieczenia materiału dowodowego (screenshoty, logi, metadane), lecz także odtworzenia chronologii zdarzeń, eskalacji treści oraz struktury sieci, która sprzyjała rozprzestrzenianiu się nienawistnych komunikatów. Tak odtworzona historia aktywności w sieci bywa kluczowa przy kwalifikacji prawnej czynu i ocenie, czy mamy do czynienia z jednorazowym incydentem, czy z długotrwałą, zorganizowaną kampanią ataków na ofiarę lub określoną grupę społeczną.

Etapy współpracy służb z zespołem OSINT Mediarecovery

W pracy polskich organów ścigania coraz częściej pojawia się moment, w którym prowadzący sprawę prokurator lub policjant dysponuje jedynie fragmentarycznymi danymi – nickiem, adresem email, linkiem do kanału w komunikatorze – i potrzebuje specjalistycznego wsparcia w ich analizie. W takim przypadku z pomocą przychodzą wyspecjalizowane zespoły, takie jak Laboratorium Informatyki Śledczej i zespół OSINT Mediarecovery, które oferują ustandaryzowany proces realizacji usługi dla służb – od przyjęcia zgłoszenia po przygotowanie ekspertyzy dowodowej.
Typowy proces można opisać w czterech krokach.

1. **Zgłoszenie** – funkcjonariusz lub prokurator przekazuje posiadane informacje dotyczące celu i kontekstu sprawy oraz określa oczekiwany rezultat analizy, np. identyfikacja sprawcy, odtworzenie chronologii zdarzeń, ustalenie powiązań z innymi osobami.
2. **Weryfikacja możliwości** – eksperci Mediarecovery oceniają, jakie działania OSINT są możliwe w danej sprawie, w jakim horyzoncie czasowym oraz w jakiej formie można dostarczyć wyniki; na tym etapie doprecyzowywany jest zakres ekspertyzy.
3. **Analiza** – zespół przeprowadza właściwe działania: wykorzystuje najnowsze technologie i wiedzę ekspertów, aby wydobyć informacje z najgłębszych warstw sieci Internet i Darknet.
4. **Ekspertyza** – przygotowywany jest dokument zawierający opis przeprowadzonych czynności, pozyskane dane wraz z informacją o ich źródle, wyniki analizy, a także wnioski.

Ekspertyza może być następnie wykorzystana zarówno na etapie działań operacyjnych, jak i w postępowaniu sądowym.

Dyskretnie, ale profesjonalnie – rola Mediarecovery w śledztwach cyber

Mediarecovery od kilkunastu lat wspiera polskie służby w sprawach dotyczących cyberprzestępczości, oszustw internetowych, handlu ludźmi, zniknięć osób, a także przestępstw motywowanych nienawiścią – zarówno poprzez analizy OSINT, jak i usługi z zakresu informatyki śledczej oraz analizy transakcji kryptowalutowych.
Dzięki połączeniu kompetencji z obszaru białego wywiadu, analizy danych mobilnych i komputerowych oraz śledzenia przepływów kryptowalut możliwe jest zbudowanie pełnego obrazu sprawy. Dla służb oznacza to realne oszczędności czasu i zasobów: dobrze zaplanowana współpraca z zespołem OSINT redukuje liczbę fałszywych tropów i pozwala skupić się na najbardziej perspektywicznych wątkach.

Granice OSINT i znaczenie korelacji z innymi źródłami

Warto podkreślić, że sam OSINT rzadko daje stuprocentowe potwierdzenie tożsamości – najczęściej mówimy o hipotezach o wysokim prawdopodobieństwie, które wymagają weryfikacji poprzez dane niejawne, takie jak bilingi, dane abonenta czy logi operatorów telekomunikacyjnych i dostawców usług internetowych. Dlatego w dojrzałym podejściu śledczym OSINT traktowany jest jako element większej układanki, łączony z tradycyjnymi metodami operacyjnymi i procesowymi, a nie jako zamiennik klasycznego dochodzenia.
Z drugiej strony, dobrze przeprowadzona analiza OSINT może znacząco zawęzić krąg podejrzanych, wskazać nowe wątki, obalić alibi lub ujawnić powiązania między pozornie niezależnymi incydentami (np. seriami ataków phishingowych czy kampaniami mowy nienawiści prowadzonymi z różnych kont).
Tak rozumiany OSINT jest dziś jednym z kluczowych elementów w walce z przestępczością, cyberprzestępczością i przestępstwami motywowanymi nienawiścią – od pierwszego, pozornie anonimowego postu, aż po wyrok skazujący, oparty na solidnym, skorelowanym materiale dowodowym.

Summary

From nickname to verdict: de-anonymization cybercrime criminals using OSINT methods

The article presents the use of modern techniques for obtaining and analyzing information from widely available Internet sources. The Internet is a tool that, combined with traditional operational and procedural methods, is currently one of the key elements in the fight against crime, cybercrime, and hate crimes.

Tłumaczenie: Beata Pepłowska