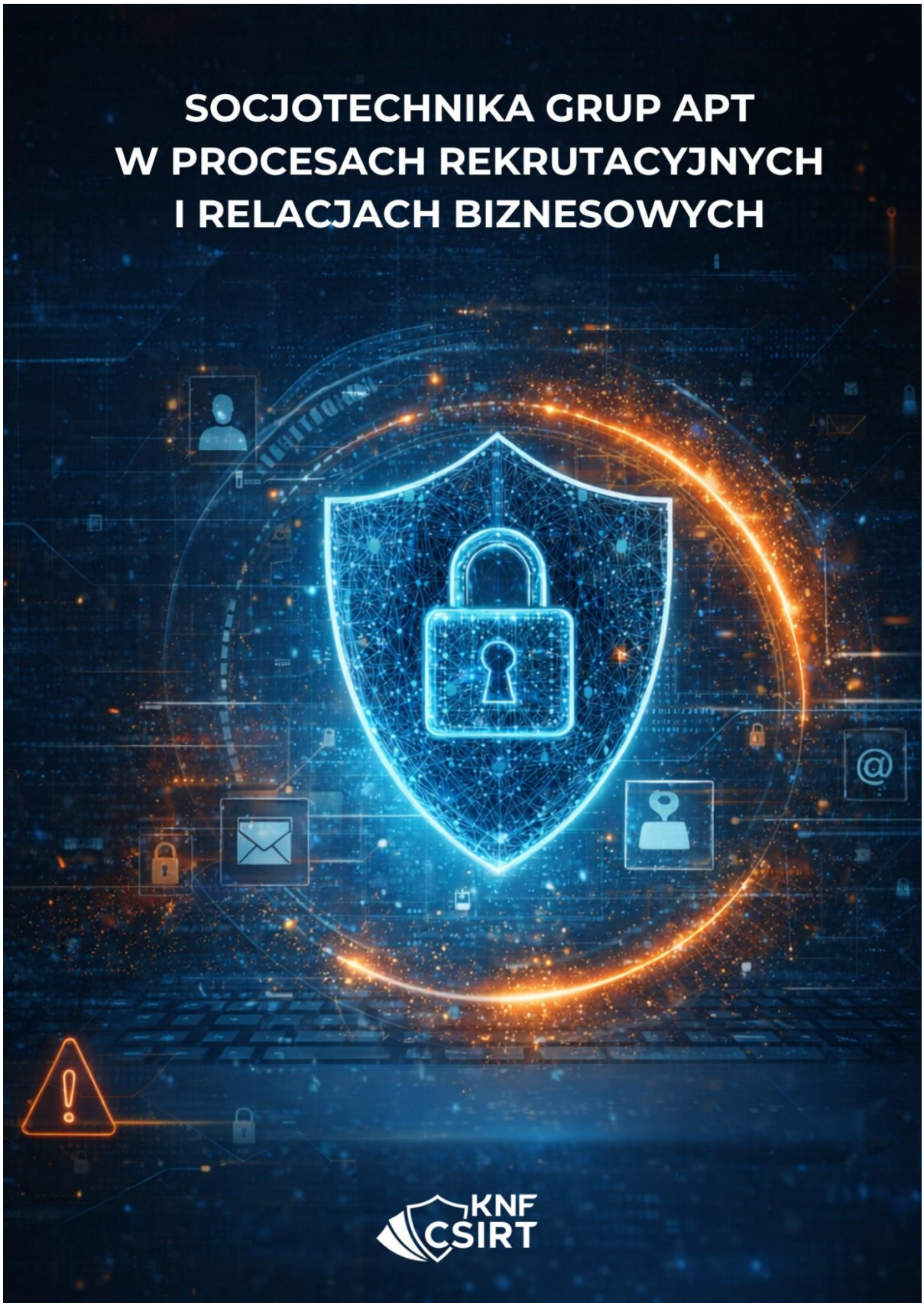
# SOCJOTECHNIKA GRUP APT W PROCESACH REKRUTACYJNYCH I RELACJACH BIZNESOWYCH



# Socjotechnika grup APT w procesach rekrutacyjnych i relacjach biznesowych

Kwiecień 2026

## 1. WPROWADZENIE

W listopadzie 2025 roku zespół CSIRT KNF przekazał ostrzeżenie podmiotom rynku finansowego, dotyczące zagrożeń związanych z fałszywymi rekrutacjami prowadzonymi przez grupy APT. Są to dobrze zorganizowane, często wspierane przez rządy grupy cyberprzestępcze, które specjalizują się w długofalowych i zaawansowanych cyberatakach (Advanced Persistent Threat). Z czasem działania tych grup stały się intensywniejsze. Wprowadzono nowe techniki ataków, a atakujący stale rozszerzają obszar działań.

Kierunek ataku dotyczy przede wszystkim firm zatrudniających pracowników IT w modelu zdalnym, jednak metody atakujących wyszły już poza same fałszywe rekrutacje. Obecnie działania grup APT można podzielić na cztery główne schematy:

- **Fałszywi pracownicy IT:** wprowadzanie do organizacji rzekomych programistów i inżynierów posługujących się skradzionymi tożsamościami.
- **Zaawansowana socjotechnika:** kampanie ukierunkowane na przejmowanie komunikacji oraz wykorzystywanie stron phishingowych podszywających się pod znane platformy do wideokonferencji.
- **Infiltracja biznesowa:** długoterminowe budowanie wiarygodności, w tym fizyczna obecność pośredników na konferencjach branżowych.
- **Ataki ukierunkowane:** personalizowane operacje wymierzone bezpośrednio w badaczy i analityków cyberbezpieczeństwa.

Z tego powodu podjęliśmy decyzję o publikacji zaktualizowanej wersji dokumentu. Poniżej prezentujemy aktualny obraz zagrożenia, opis zidentyfikowanych metod ataku oraz dostarczenie zbioru rekomendacji dla organizacji i zespołów bezpieczeństwa.

## 2. JAK DZIAŁAJĄ GRUPY APT

Grupy APT stosują kilka różnych metod infiltracji:

### 2.1. Fałszywi pracownicy IT

Schemat polega na budowaniu sieci tzw. IT Workers, czyli osób podszywających się pod programistów, administratorów i inżynierów systemowych. Jest to operacja o charakterze przemysłowym, prowadzona na dużą skalę i generująca znaczne przychody, z których część jest przekazywana na finansowanie programów zbrojeniowych.

**Budowanie fałszywej tożsamości**

Kandydaci występują pod fałszywą lub skradzioną tożsamością, dysponując profesjonalnie przygotowanym profilem zawodowym, podrobionymi dokumentami oraz fikcyjną historią zatrudnienia. Dokumenty tożsamości pozyskiwane są z rynków darknetu oraz od pośredników. W jednej ze spraw prowadzonych przez Departament Sprawiedliwości USA pośredniczka wykorzystała dziesiątki skradzionych tożsamości w celu infiltracji ponad 300 firm amerykańskich,

za co została skazana na ponad 8 lat pozbawienia wolności.[1] W innej sprawie obywatel Ukrainy zarządzał setkami fałszywych tożsamości i prowadził tysiące fikcyjnych kont na platformach freelancerskich oraz w mediach społecznościowych.[2]
Zdjęcia profilowe generowane są za pomocą narzędzi AI. Unit 42 (Palo Alto Networks) wykazał, że osoba bez doświadczenia technicznego jest w stanie stworzyć w pełni funkcjonalną syntetyczną tożsamość ze zdjęciem i deepfake wideo działającym w czasie rzeczywistym w krótkim czasie, na standardowym komputerze.[3] Część operatorów posługuje się również oprogramowaniem do zmiany głosu oraz wkładkami dousznymi z coachingiem w czasie rzeczywistym podczas wideorozmów.[4]

**Farmy laptopów**

Po zatrudnieniu firma wysyła laptop służbowy na adres podany przez kandydata. W rzeczywistości adres ten należy do pośrednika, który odbiera sprzęt i instaluje na nim narzędzia zdalnego dostępu lub sprzętowe urządzenia KVM. Operatorzy łączą się z urządzeniem zdalnie, maskując połączenie za pomocą VPN. W ramach skoordynowanych działań w 2025 roku FBI przeszukało dziesiątki takich farm na terenie USA.[5] CrowdStrike potwierdził istnienie analogicznych farm laptopów w również w Europie, w tym w Polsce i Rumunii.[6]

**Proces rekrutacji**

Operatorzy skutecznie przechodzą przez większość etapów rekrutacji, w szczególności, gdy proces prowadzony jest w pełni zdalnie i opiera się wyłącznie na wideorozmowach oraz przesłanych dokumentach. Pojedynczy operator może jednocześnie posługiwać się kilkoma tożsamościami w różnych organizacjach, natomiast jedną tożsamość może obsługiwać wymiennie kilka osób. W 2024 roku firma KnowBe4[7], zajmująca się szkoleniami z zakresu cyberbezpieczeństwa, potwierdziła zatrudnienie fałszywego pracownika IT, który przeszedł pełen proces rekrutacyjny, włącznie z formalną weryfikacją historii zatrudnienia i tożsamości oraz kilkoma wideorozmowami kwalifikacyjnymi. Zagrożenie zostało wykryte dopiero po zaobserwowaniu nietypowej aktywności sieciowej, operator podjął próbę instalacji złośliwego oprogramowania niemal natychmiast po otrzymaniu sprzętu służbowego.

**Po uzyskaniu zatrudnienia**

Po uzyskaniu zatrudnienia osoby te otrzymują legalny dostęp do infrastruktury organizacji. Wykonują przydzielone zadania, uczestniczą w spotkaniach i starają się nie wzbudzać podejrzeń, stosując m.in. oprogramowanie symulujące aktywność i chatboty AI do odpowiadania na wiadomości. Szkodliwa aktywność zaczyna się dopiero po pewnym czasie, gdy uzyskają dostęp do większej liczby zasobów. Obejmuje ona pobieranie danych, analizę środowisk produkcyjnych, próby wyprowadzenia środków finansowych (w tym kryptowalut), instalację backdoorów oraz przekazywanie informacji do operatorów APT.

[1] *Źródło: https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue*

[2] *Źródło: https://www.securityweek.com/ukrainian-gets-5-years-in-us-prison-for-aiding-north-korean-it-fraud/*

[3] *Źródło: https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/*

[4] *Źródło: https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/*

[5] *Źródło: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote*

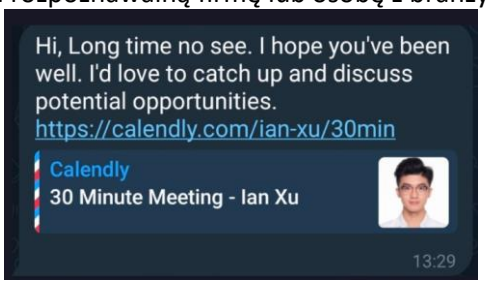
[6] *Źródło: https://fortune.com/2025/08/04/north-korean-it-worker-infiltrations-exploded/*

[7] *Źródło: https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us*

## 2.2. Fałszywe spotkania Zoom i Microsoft Teams

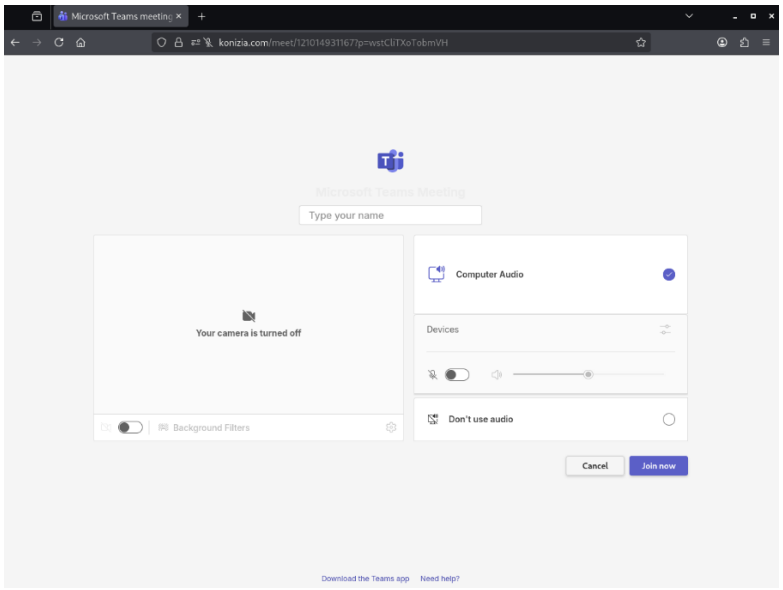
W kwietniu 2026 organizacja SEAL (Security Alliance) opublikowała advisory dotyczące grupy UNC1069 (BlueNoroff) [8], która prowadzi kampanie socjotechniczne z wykorzystaniem fałszywych spotkań wideo. Od lutego do kwietnia 2026 zidentyfikowano 164 domeny używane w tych atakach. Schemat działania wygląda następująco:

1. **Nawiązanie kontaktu.** Atakujący wykorzystuje przejęte konto osoby znanej ofierze np. kontaktu z konferencji, partnera biznesowego, współpracownika. Dysponuje pełną historią konwersacji, więc może wznowić rozmowę w naturalny sposób. Gdy przejęte konto nie jest dostępne, podszywa się pod wiarygodne marki na LinkedIn, Slacku lub Telegramie, podszywając się pod rozpoznawalną firmę lub osobę z branży.




*Screen 1. Nawiązanie kontaktu,*
*źródło: https://radar.securityalliance.org/advisory-on-dprk-unc1069-fake-microsoft-teams-and-zoom-calls/*

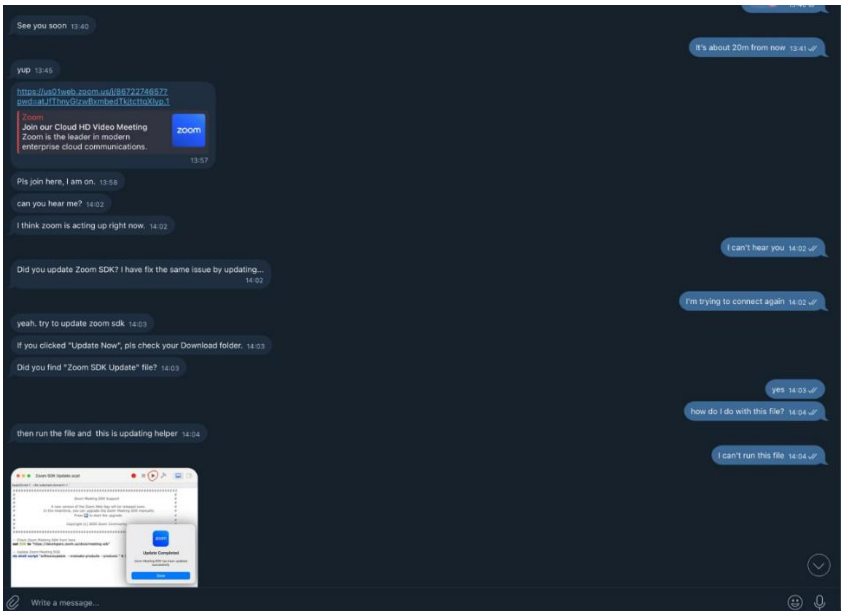
2. **Zaplanowanie spotkania.** Następnie proponuje spotkanie wideo, zaplanowane z 1-2 tygodniowym wyprzedzeniem. Długi czas normalizuje interakcję i zmniejsza czujność ofiary. Krótko przed spotkaniem ofiara otrzymuje link do fałszywej strony.
3. **Fałszywy interfejs spotkania.** Strona załadowana w przeglądarce jest wizualnie identyczna z prawdziwym Zoom lub Teams. Jest zbudowana na oficjalnych SDK tych platform i wyświetla nagrania wideo rzekomych uczestników (pozyskane np. z wystąpień konferencyjnych). Nie wymaga instalacji żadnej aplikacji.




*Screen 2. Strona podszywająca się pod Microsoft Teams, źródło: Strona zidentyfikowana przez CSIRT KNF*

4. **Wykorzystanie rzekomego problemu z dźwiękiem.** Ofiara nie słyszy rozmowy. Interfejs wyświetla komunikat sugerujący konieczność aktualizacji. Równolegle atakujący kontaktuje się przez Telegram lub Slack, oferując pomoc techniczną i instruując ofiarę krok po kroku.

[8] *Źródło i IOC: https://radar.securityalliance.org/advisory-on-dprk-unc1069-fake-microsoft-teams-and-zoom-calls/*




*Screen 3. Schemat ataku z wykorzystaniem fałszywego spotkania i rzekomej aktualizacji SDK, źródło: https://radar.securityalliance.org/advisory-on-dprk-unc1069-fake-microsoft-teams-and-zoom-calls/*

5. **Dostarczenie złośliwego oprogramowania.** Pod pretekstem rozwiązania rzekomego problemu, atakujący nakłania ofiarę do uruchomienia złośliwego skryptu lub wklejenia komendy bezpośrednio w terminalu. Działanie to uruchamia tzw. dropper, który następnie pobiera z sieci malware. Złośliwe oprogramowanie instaluje się na urządzeniu i nawiązuje regularną komunikację z serwerem zarządzającym (C2) operatorów APT.

Od tego momentu atakujący mają w zasadzie pełną kontrolę nad tym, co dzieje się na komputerze. W praktyce oznacza to, że mogą bez przeszkód realizować takie operacje jak:

a) **Kradzież danych dostępowych:** Pozyskują loginy i hasła do serwisów internetowych, w tym dane przechowywane w menedżerach haseł.
b) **Rejestrowanie aktywności klawiatury:** Przechwytuje wszystkie naciśnięcia klawiszy - w tym wpisywane hasła, kody jednorazowe oraz treści wiadomości.
c) **Przejmowanie sesji komunikatorów**: Kradzież tokenów sesyjnych Telegrama, Slacka czy Discorda, co pozwala odczytywać konwersacje i wysyłać wiadomości w imieniu ofiary.
d) **Przechwytywanie schowka systemowego**: Monitorowanie wszystkiego co ofiara kopiuje i wkleja, w tym hasła, kody 2FA, dane bankowe czy fragmenty kodu. Malware może również podmieniać zawartość schowka, np. zamieniając skopiowany numer konta bankowego lub adres portfela kryptowalutowego na adres kontrolowany przez atakującego.

## 2.3. Infiltracja przez relacje biznesowe

Zagrożenie nie ogranicza się do zdalnych rekrutacji. Przypadek platformy Drift Protocol[9] (kwiecień 2026, straty ponad 280 mln USD) pokazuje, że grupy APT są gotowe prowadzić wielomiesięczne operacje obejmujące fizyczną obecność na konferencjach branżowych.

Atakujący podszywali się pod firmę zajmującą się handlem algorytmicznym i podchodzili do współtwórców platformy osobiście na konferencjach kryptowalutowych, prowadząc tę operację przez co najmniej sześć miesięcy. Założyli grupę na Telegramie, prowadzili rozmowy o strategiach tradingowych, przeszli formalny proces onboardingu jako klient i wpłacili ponad 1 mln USD własnego kapitału na platformę, budując w ten sposób wiarygodność.

[9] *Źródło: https://www.bleepingcomputer.com/news/security/drift-280m-crypto-theft-linked-to-6-month-in-person-operation/*

Wektory ataku obejmowały złośliwe repozytorium kodu (wykorzystujące podatność w edytorach VSCode/Cursor, która umożliwiała ciche uruchomienie kodu przy samym otwarciu projektu) oraz fałszywą aplikację mobilną dystrybuowaną przez platformę TestFlight. Atak został przypisany grupie UNC4736 (AppleJeus/Citrine Sleet). Co istotne, osoby spotykające się z ofiarami na żywo nie były bezpośrednio powiązane z grupą APT. W operacji wykorzystano zewnętrznych pośredników.

### 2.4. Celowanie w badaczy i specjalistów bezpieczeństwa

Operatorzy APT rozszerzają zakres celów również na osoby zajmujące się analizą zagrożeń. W kwietniu 2026 niezależny badacz cyberbezpieczeństwa opisał[10], jak stał się celem spersonalizowanej kampanii rekrutacyjnej. Operatorzy monitorowali jego publikacje, a następnie wysłali email z ofertą pracy, który cytował jego artykuły po nazwie i używał jego własnej terminologii. Treść wiadomości wskazywała na wygenerowanie jej przez model językowy na podstawie publikacji ofiary.

Oferta prowadziła do strony ze sfabrykowanym profilem dyrektora nieistniejącej firmy, ze zdjęciem wygenerowanym przez AI i fałszywym życiorysem powołującym się na istniejące firmy. Domena została zarejestrowana zaledwie 5 dni wcześniej. Strona była hostowana na platformie Vercel, którą Microsoft zidentyfikował jako standardową infrastrukturę kampanii Contagious Interview.[11]

Gdy badacz rozpoczął analizę infrastruktury i podzielił się wynikami z grupą badawczą, operator dezaktywował konto pocztowe wykorzystane do kontaktu i zablokował wszelką komunikację.

## 3. SKALA I ZASIĘG

Opisane metody nie mają charakteru incydentalnego. Dane z 2025 i 2026 roku wskazują na systematyczną, państwową operację o zasięgu globalnym.

Według raportu Mandiant (Google Cloud) z 2025 roku ponad 3 000 podejrzanych pracowników powiązanych z grupami APT działa w zachodnich firmach. Szacowane przychody z tych operacji przekraczają 600 milionów dolarów rocznie.[12] Według amerykańskich służb część tych środków jest wykorzystywana do finansowania dalszych operacji cybernetycznych. W marcu 2026 Departament Skarbu USA (OFAC) nałożył sankcje na sześć osób i dwa podmioty zaangażowane w te operacje.[13]

Problem nie ogranicza się do Stanów Zjednoczonych. W wyniku nasilonych działań organów ścigania w USA operatorzy APT rozszerzyli działalność na **Europę, w tym Wielką Brytanię, Niemcy, Portugalię, Polskę i Rumunię**. Firma CrowdStrike potwierdza obserwacje analogicznych schematów w tych krajach[14]. Raport CSIS z marca 2026 opisuje przypadek w Serbii, gdzie pracownik powiązany z grupą APT ukradł kryptowaluty o wartości ok. 175 000 USD z firmy, do której się infiltrował[15].

Zmienia się też profil ryzyka. FBI potwierdziło w styczniu 2025, że zwolnieni pracownicy IT powiązani z grupami APT zaczęli **wymuszać okupy od byłych pracodawców, grożąc ujawnieniem skradzionych danych**[16]. Zagrożenie dotyczy więc nie tylko wynagrodzeń przekazywanych operatorom, ale także bezpośredniej kradzieży danych i szantażu.

---

[10] *Źródło: https://maythethreathuntsbewithyou.substack.com/p/they-were-watching-me-before-i-was*

[11] *Źródło: https://www.microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews/*

[12] *Źródło: https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale*

[13] *Źródło: https://thehackernews.com/2026/03/ofac-sanctions-dprk-it-worker-network.html*

[14] *Źródło: https://www.politico.com/news/2025/05/12/north-korea-remote-workers-us-tech-companies-00340208*

[15] *Źródło: https://www.csis.org/analysis/responding-evolution-and-global-expansion-dprk-it-worker-threat*

[16] *Źródło: https://www.ic3.gov/PSA/2025/PSA250123*

## 4. JAK ROZPOZNAĆ ZAGROŻENIE ZWIĄZANE Z FAŁSZYWĄ REKRUTACJĄ

Wykrycie fałszywego pracownika na etapie rekrutacji jest trudne, ponieważ operatorzy grup APT profesjonalnie przygotowują tożsamości, dokumenty i historie zatrudnienia swoich kandydatów. Mimo to analiza znanych przypadków pozwala wskazać powtarzające się sygnały ostrzegawcze. Poniżej przedstawiamy wskaźniki, które mogą świadczyć o próbie infiltracji poprzez zatrudnienie.

**Tożsamość i lokalizacja**

| Kategoria | Wskaźniki behawioralne | Wskaźniki techniczne |
|---|---|---|
| Tożsamość / Lokalizacja | • Niechęć do włączenia kamery lub obraz budzący wątpliwości (możliwy deepfake).<br>• Odmowa spotkania na żywo lub wizyty w biurze, nawet gdy lokalizacja to umożliwia.<br>• Prośba o wysłanie sprzętu na adres inny niż deklarowany. | • Logowania z wielu adresów IP w krótkim czasie (różne kraje).<br>• Nietypowe zmiany geolokalizacji w trakcie sesji.<br>• Logowania przez hosty VPS lub komercyjne VPN. |

**Wydajność i zachowanie w pracy**

| Kategoria | Wskaźniki behawioralne | Wskaźniki techniczne |
|---|---|---|
| Wydajność / Jakość pracy | • Znacząca różnica między poziomem wiedzy na rozmowie a tym widocznym w codziennej pracy.<br>• Kandydat pisze dobry kod, ale nie potrafi wyjaśnić swojego toku rozumowania. | • Korzystanie z narzędzi zdalnego pulpitu (AnyDesk, RustDesk, TinyPilot/PiKVM).<br>• Stałe połączenia przez zagraniczne VPN.<br>• Narzędzia symulujące aktywność (mouse jiggler). |

**Komunikacja i dokumenty**

| Kategoria | Wskaźniki behawioralne | Wskaźniki techniczne |
|---|---|---|
| Komunikacja / Dokumenty | • Niskie zaangażowanie, unikanie spotkań, częste wymówki.<br>• Niespójna komunikacja między kolejnymi rozmowami (możliwa zmiana operatora). | • Te same wzory dokumentów, numery identyfikacyjne lub skany w wielu profilach.<br>• Metadane dokumentów wskazujące na inny kraj lub autora niż deklarowany. |

> *W* kwietniu 2026 popularność zyskało niestandardowe podejście do weryfikacji tożsamości kandydatów podczas rozmów kwalifikacyjnych. Szeroko komentowane nagranie opublikowane przez badacza tanuki42 pokazuje kandydata, który nie przeszedł takiej weryfikacji i opuścił rozmowę. Długoterminowa wartość tego podejścia jest ograniczona, ponieważ operatorzy mogą się do niego dostosować. Nie powinno być traktowane jako samodzielne narzędzie weryfikacji.[17]

[17] *Źródło: https://x.com/tanuki42_/status/2041096021300928759*

# 5. REKOMENDACJE

## 5.1. Rekrutacja i onboarding

CSIRT KNF rekomenduje przegląd procedur związanych z rekrutacją zdalną, onboardingiem i monitorowaniem aktywności nowych pracowników. Poniżej przedstawiamy zalecane działania w podziale na etapy.

**Weryfikacja kandydatów**

- Prowadzić rozmowy z włączoną kamerą. Zwracać uwagę na nienaturalne pauzy, opóźnienia, wyciszenia dźwięku w momentach, gdy kandydat powinien mówić.
- Przy podwyższonym ryzyku lub podejrzeniu nadużycia uwzględnić analizę dostępnych danych telemetrycznych i diagnostycznych połączenia, realizowaną przez uprawnionych administratorów.
- Potwierdzać historię zatrudnienia bezpośrednio u poprzednich pracodawców, a nie tylko na podstawie CV i profilu LinkedIn.
- Przy rolach o podwyższonym ryzyku rozważyć weryfikację tożsamości na żywo.

**Pierwsze tygodnie pracy**

- Poprosić pracownika o odczytanie numeru seryjnego urządzenia, co potwierdza fizyczny dostęp do sprzętu.
- Monitorować aktywność użytkownika pod kątem nietypowych godzin pracy.
- Nadawać uprawnienia stopniowo (least privilege). Monitorować próby eskalacji.

**Po wykryciu podejrzenia lub incydentu**

- Niezwłocznie zablokować konto i dostęp do wszystkich systemów.
- Przeprowadzić analizę zachowania użytkownika: historię logowań, używane narzędzia, ostatnie działania na repozytoriach i w systemach.
- Skontaktować się z CERT Polska lub właściwym zespołem sektorowym, żeby skonsultować sytuację i zlecić jej dalszą analizę.

## 5.2. Spotkania wideo i linki

- Weryfikować domeny linków do spotkań**.** Prawidłowe adresy to zoom.us i teams.microsoft.com. Każda inna domena (np. teamslivc[.]com, ms-meet[.]xyz, micrusoft[.]us) stanowi sygnał ostrzegawczy.
- Nie pobierać plików ani nie uruchamiać poleceń terminalowych sugerowanych przez interfejs spotkania lub rozmówcę w trakcie połączenia wideo.
- Jeśli podczas spotkania wystąpią „problemy z dźwiękiem” i rozmówca proponuje „aktualizację” lub „naprawę” wymagającą pobrania pliku lub wklejenia komendy, należy natychmiast przerwać połączenie.
- Uwrażliwiać pracowników, że atakujący mogą kontaktować się z przejętych kont osób, które ofiara zna. Sam fakt, że wiadomość pochodzi od znanego kontaktu, nie oznacza, że jest bezpieczna.
- Zgłaszać podejrzane domeny i linki do CERT Polska poprzez stronę: https://incydent.cert.pl.

## 5.3. Konferencje i relacje biznesowe

- Kontakty nawiązane osobiście na konferencjach nie są automatycznie wiarygodne. Należy weryfikować firmy i osoby, które proponują współpracę techniczną lub integrację z systemami.
- Nie otwierać projektów z nieznanych repozytoriów bez wcześniejszej analizy.
- Nie instalować aplikacji dystrybuowanych poza oficjalnymi kanałami, na prośbę nowo poznanych kontaktów biznesowych.
- Zachować ostrożność wobec nowych partnerów, którzy szybko budują wiarygodność przez wpłaty własnych środków lub formalne procesy onboardingowe.

- Ograniczyć dostęp do repozytoriów i systemów wewnętrznych dla partnerów zewnętrznych. Stosować zasadę minimalnych uprawnień również wobec kontrahentów.

### 5.4. Ochrona pracowników technicznych i badaczy

- Informować pracowników technicznych (programistów, analityków bezpieczeństwa, badaczy) o tym, że są potencjalnymi celami spersonalizowanych kampanii rekrutacyjnych. Oferty pracy mogą być generowane przez AI na podstawie ich publikacji i aktywności online.
- Traktować z ostrożnością niezamówione oferty pracy, szczególnie jeśli: pochodzą z adresów Gmail lub innych darmowych skrzynek, odwołują się do firm, których nie można zweryfikować w publicznych źródłach lub kierują na strony zarejestrowane w ostatnich dniach.
- Weryfikować tożsamość osób proponujących współpracę badawczą, szczególnie jeśli propozycja wiąże się z uruchomieniem kodu, zainstalowaniem narzędzi.
- Rozważyć stosowanie izolowanych środowisk do analizy nieznanych projektów i narzędzi otrzymanych od osób spoza organizacji.

## 6. PODSUMOWANIE

Grupy APT traktują procesy rekrutacyjne jako pełnoprawny wektor ataku. Stosowane metody obejmują fałszywe tożsamości i deepfake w rekrutacjach zdalnych, spreparowane interfejsy Zoom i Teams nakłaniające ofiary do uruchomienia złośliwego kodu, wielomiesięczne operacje z fizyczną obecnością na konferencjach branżowych, a także spersonalizowane kampanie wymierzone w pracowników technicznych i badaczy bezpieczeństwa. Metody te ewoluują i są systematycznie dostosowywane do wykrytych mechanizmów obronnych.

Opisane w dokumencie techniki nie są ograniczone do jednej grupy ani regionu. Stosują je różne podmioty państwowe i niepaństwowe, a metody te są stale adaptowane i udoskonalane. Obecna sytuacja geopolityczna dodatkowo zwiększa ekspozycję instytucji na tego typu zagrożenia. Zagraniczne grupy APT będą poszukiwać nowych sposobów infiltracji organizacji, nie tylko technicznych, ale również opartych na socjotechnice i manipulacji zaufaniem. Rozszerzenie zasięgu tych operacji na Europę oraz wzrost ich złożoności sprawia, że prawdopodobieństwo objęcia nimi polskich organizacji rośnie. Zachęcamy do przeglądu wewnętrznych procedur rekrutacji zdalnej, onboardingu, weryfikacji kontrahentów oraz monitorowania aktywności nowych pracowników i współpracowników zewnętrznych. Czujność każdego z nas pozostaje pierwszą linią obrony.

Dziękujemy za zapoznanie się z raportem. CSIRT KNF pozostaje do dyspozycji w zakresie konsultacji, wymiany informacji oraz zgłaszania sytuacji budzących wątpliwości. W przypadku potrzeby uzyskania wsparcia prosimy o kontakt: csirt@knf.gov.pl

O nowych sposobach działania oszustów informujemy również za pośrednictwem mediów społecznościowych. Zachęcamy do obserwowania kont CSIRT KNF w serwisach Twitter, LinkedIn oraz Facebook.

Z poważaniem, Zespół

# ŹRÓDŁA


1. U.S. Department of Justice, Arizona Woman Sentenced for $17M IT Worker Fraud Scheme
https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue

2. SecurityWeek, Ukrainian Gets 5 Years in US Prison for Aiding North Korean IT Fraud
https://www.securityweek.com/ukrainian-gets-5-years-in-us-prison-for-aiding-north-korean-it-fraud/

3. Unit 42 (Palo Alto Networks), North Korean Synthetic Identity Creation
https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/

4. Microsoft Security Blog, Jasper Sleet: North Korean Remote IT Workers Evolving Tactics, czerwiec 2025
https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

5. U.S. Department of Justice, Coordinated Nationwide Actions to Combat North Korean Remote Workers
https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

6. Fortune, North Korean IT Worker Infiltrations Exploded, sierpień 2025
https://fortune.com/2025/08/04/north-korean-it-worker-infiltrations-exploded/

7. KnowBe4, How a North Korean Fake IT Worker Tried to Infiltrate Us
https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

8. SEAL (Security Alliance), Advisory on DPRK (UNC1069) Fake Microsoft Teams and Zoom calls, kwiecień 2026
https://radar.securityalliance.org/advisory-on-dprk-unc1069-fake-microsoft-teams-and-zoom-calls/

9. BleepingComputer, Drift $280M crypto theft linked to 6-month in-person operation, kwiecień 2026
https://www.bleepingcomputer.com/news/security/drift-280m-crypto-theft-linked-to-6-month-in-person-operation/

10. May the Threat Hunts Be With You, They were Watching me before I was Watching them, kwiecień 2026
https://maythethreathuntsbewithyou.substack.com/p/they-were-watching-me-before-i-was

11. Microsoft Security Blog, Contagious Interview: malware delivered through fake developer job interviews, marzec 2026
https://www.microsoft.com/en-us/security/blog/2026/03/11/contagious-interview-malware-delivered-through-fake-developer-job-interviews/

12. Google Threat Intelligence Group (Mandiant), DPRK IT Workers Expanding in Scope and Scale, kwiecień 2025
https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale

13. OFAC / The Hacker News, OFAC Sanctions DPRK IT Worker Network Funding WMD Programs, marzec 2026
https://thehackernews.com/2026/03/ofac-sanctions-dprk-it-worker-network.html

14. Politico, North Korea remote workers US tech companies, maj 2025
https://www.politico.com/news/2025/05/12/north-korea-remote-workers-us-tech-companies-00340208

15. CSIS, Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat, marzec 2026
https://www.csis.org/analysis/responding-evolution-and-global-expansion-dprk-it-worker-threat

16. FBI IC3, Public Service Announcement, styczeń 2025
https://www.ic3.gov/PSA/2025/PSA250123

17. TechCrunch / tanuki42, How a job interviewer exposes a North Korean fake IT worker, kwiecień 2026
https://techcrunch.com/2026/04/06/watch-this-video-of-how-a-job-interviewer-exposes-a-north-korean-fake-it-worker/