[TLP: CLEAR]


2025
KRAJOBRAZ
CYBERZAGROŻEŃ
W POLSKIM SEKTORZE
FINANSOWYM

Spis treści

1. Wprowadzenie

Dokument ten ma na celu przedstawienie ogólnego przeglądu aktualnego krajobrazu zagrożeń w sektorze finansowym. Skupia się na identyfikacji i analizie najważniejszych zagrożeń, z którymi mogą się spotkać instytucje finansowe - w tym ataków cyberprzestępczych, działań złośliwych użytkowników wewnętrznych oraz technik wykorzystywanych przez cyberprzestępców. Celem jest dostarczenie wszechstronnych informacji, które mogą pomóc w przygotowaniu się do obrony przed tymi zagrożeniami oraz w opracowaniu skutecznych strategii zarządzania ryzykiem.

Zakres:

Dokument obejmuje główne rodzaje zagrożeń, aktorów oraz metody, które stanowią ryzyko dla instytucji finansowych i szerszego ekosystemu finansowego. W szczególności omówione zostaną:

- **Grupy sponsorowane przez państwa (APT):** Zaawansowane, długotrwałe ataki przeprowadzane przez grupy hakerskie wspierane przez rządy, mające na celu uzyskanie strategicznych informacji lub zakłócenie działalności innych państw.
- **Zorganizowane grupy cyberprzestępcze:** Organizacje przestępcze działające na dużą skalę, często angażujące się w różne formy cyberprzestępczości, takie jak ransomware, trojany bankowe i ataki na łańcuch dostaw.
- **Użytkownicy wewnętrzni:** Pracownicy lub współpracownicy, którzy wykorzystują swoje uprawnienia do działania na szkodę organizacji, na przykład poprzez kradzież danych lub sabotaż.
- **Ataki z wykorzystaniem narzędzi opartych o AI:** Ataki wykorzystujące zaawansowane technologie, takie jak deepfake, do przeprowadzania oszustw i manipulacji.
- **Rasnomware:** Złośliwe oprogramowanie zaprojektowane do szyfrowania danych ofiary najczęściej w celu wymuszenia okupu za ich odblokowanie.
- **Malware typu stealer:** Złośliwe oprogramowanie zaprojektowane do kradzieży poufnych informacji, takich jak dane logowania, hasła, dane karty kredytowej, informacje bankowe oraz inne dane osobowe.
- **Malware typu NFC relay:** Złośliwe oprogramowanie, wykradające wrażliwe dane z wykorzystaniem technologii NFC.

Każda sekcja zawiera szczegółowe opisy metod ataków, przykłady incydentów, motywacje aktorów. Dokument ma służyć jako kompleksowe źródło wiedzy, wspierające działania ochronne i prewencyjne w instytucjach finansowych.

2. Skrótowy przegląd Krajobrazu Zagrożeń (GTL).

2.1 Główne Typy Zagrożeń

- **Zagrożenia cyber**: Ataki DDoS, ransomware, phishing, złośliwe oprogramowanie, atak na łańcuch dostaw (supply chain attack), ataki z wykorzystaniem narzędzi opartych o AI (np. deepfake).
- **Zagrożenia fizyczne**: Sabotaż infrastruktury, kradzież sprzętu.
- **Zagrożenia wewnętrzne**: Pracownicy działający na szkodę firmy, błędy ludzkie.

2.2 Główne Typy Aktorów

- **Indywidualni cyberprzestępcy**: Indywidualni cyberprzestępcy lub grupy, które próbują włamać się do systemów w celu kradzieży danych lub pieniędzy.
- **Grupy sponsorowane przez państwa (APT)**: Zespoły działające na zlecenie rządów w celu uzyskania strategicznych informacji lub zakłócenia działalności innych państw.
- **Grupy przestępcze**: Organizacje przestępcze działające na dużą skalę, często angażujące się w różne formy cyberprzestępczości.
- **Użytkownicy wewnętrzni:** Pracownicy lub współpracownicy, którzy wykorzystują swoje uprawnienia do działania na szkodę organizacji.

2.3 Metody Ataku

- **Ataki socjotechniczne**: Manipulowanie pracownikami w celu uzyskania dostępu do systemów lub informacji.
- **Eksploitacja luk w zabezpieczeniach**: Wykorzystywanie znanych lub nieznanych luk (0-day) w oprogramowaniu do przeprowadzania ataków.
- **Ataki z użyciem złośliwego oprogramowania**: Wprowadzenie do systemu złośliwego oprogramowania w celu kradzieży danych, zaszyfrowania plików lub zakłócenia działania systemów.
- **Ataki fizyczne**: Bezpośrednie działania mające na celu uszkodzenie infrastruktury IT lub kradzież sprzętu.

4. Podsumowanie

Dokument "Generic Threat Landscape" przedstawia kompleksowy przegląd bieżących zagrożeń, z którymi borykają się instytucje finansowe. Analiza obejmuje zarówno cyberzagrożenia, jak i zagrożenia fizyczne oraz wewnętrzne, wskazując na różnorodność i złożoność metod stosowanych przez przestępców.

Wnioski płynące z analizy podkreślają potrzebę ciągłej adaptacji i doskonalenia strategii bezpieczeństwa w instytucjach finansowych. Rosnąca liczba i zaawansowanie technik ataków, takich jak ransomware czy wykorzystanie narzędzi AI, stawia przed sektorem finansowym nowe wyzwania. Konieczne jest nie tylko wdrażanie zaawansowanych technologii zabezpieczeń, ale także rozwijanie kultury bezpieczeństwa w organizacji poprzez regularne szkolenia i podnoszenie świadomości pracowników.

Współpraca między instytucjami finansowymi, organami ścigania oraz dostawcami technologii jest kluczowa dla skutecznego przeciwdziałania zagrożeniom. Wymiana informacji o zagrożeniach i najlepszych praktykach w zakresie ochrony przed cyberatakami może znacząco zwiększyć odporność sektora finansowego na różnorodne formy ataków.

Dokument wskazuje również na znaczenie monitorowania i analizy trendów w cyberprzestępczości. Szybka identyfikacja nowych zagrożeń oraz adaptacja do zmieniającego się krajobrazu zagrożeń pozwala na skuteczniejsze zarządzanie ryzykiem i minimalizowanie potencjalnych szkód.

Podsumowując, "Generic Threat Landscape" dostarcza instytucjom finansowym cennych wskazówek i narzędzi niezbędnych do ochrony przed aktualnymi i przyszłymi zagrożeniami. Przyjęcie proaktywnej postawy oraz inwestowanie w nowoczesne technologie i edukację pracowników to kluczowe elementy budowania bezpiecznego i odpornego ekosystemu finansowego.

5. Opis ataków i adwersarzy

5.1. Grupy sponsorowane przez państwa (APT)

5.1.1. Opis

Grupy sponsorowane przez państwa, znane również jako Advanced Persistent Threats (APT), to zespoły cyberprzestępcze działające na zlecenie rządów. Ich głównym celem jest uzyskanie strategicznych informacji, zakłócenie działalności innych państw, prowadzenie cyberszpiegostwa lub wpływanie na politykę i gospodarkę międzynarodową. APT często posiadają zaawansowane zasoby, technologie oraz wsparcie finansowe, co pozwala im na przeprowadzanie skomplikowanych i długotrwałych operacji cyber, które mogą znacząco wpływać na sektor finansowy.

5.1.2. Metody działania

- *Cyberszpiegostwo w sektorze finansowym*
  - **Opis:** Działania mające na celu zdobycie poufnych informacji finansowych, takich jak dane o transakcjach, informacje o klientach, strategie inwestycyjne czy dane dotyczące fuzji i przejęć.
  - **Przykład:** APT może włamać się do systemów bankowych lub giełdowych, aby wykradać informacje o dużych transakcjach finansowych lub planach inwestycyjnych, co może być użyte do manipulacji rynkiem lub szpiegostwa gospodarczego.
  - **Obrona:** Wzmacnianie systemów ochrony danych, monitorowanie aktywności sieciowej, szyfrowanie poufnych informacji, regularne testy penetracyjne.

- *Sabotaż w sektorze finansowym*
  - **Opis:** Ataki mające na celu zakłócenie działania infrastruktury finansowej, takich jak systemy płatności, bankomaty, platformy handlowe czy systemy księgowe.
  - **Przykład:** APT może przeprowadzić atak na systemy płatności elektronicznych, powodując przerwy w transakcjach finansowych, co prowadzi do chaosu i strat finansowych.
  - **Obrona:** Wdrażanie systemów redundancji i odzyskiwania danych, segmentacja sieci, monitorowanie systemów kontrolnych, szkolenie personelu w zakresie reagowania na incydenty.

- *Spear Phishing w sektorze finansowym*
  - **Opis:** Wysoce ukierunkowany rodzaj phishingu, w którym atakujący wysyłają spersonalizowane wiadomości e-mail do wybranych pracowników sektora finansowego, aby uzyskać dostęp do ich danych uwierzytelniających lub zainfekować ich systemy złośliwym oprogramowaniem.
  - **Przykład:** APT może wysłać e-mail podszywający się pod dyrektora finansowego, prosząc o kliknięcie w link lub pobranie załącznika, który zainfekuje komputer ofiary i umożliwi dostęp do wewnętrznych systemów bankowych.
  - **Obrona:** Szkolenie pracowników w zakresie rozpoznawania phishingu, korzystanie z filtrów antyphishingowych, wprowadzenie polityki zero-trust.

- *Wykorzystywanie luk zero-day w sektorze finansowym*
  - **Opis:** Ataki wykorzystujące nieznane wcześniej luki w oprogramowaniu, na które nie ma jeszcze dostępnych poprawek bezpieczeństwa.
  - **Przykład:** APT może wykorzystać lukę zero-day w popularnym oprogramowaniu, aby uzyskać dostęp do systemów transakcyjnych lub baz danych klientów przed wydaniem przez producenta poprawki.
  - **Obrona:** Regularne aktualizacje oprogramowania, szybkie wdrażanie poprawek bezpieczeństwa, monitorowanie i analiza ruchu sieciowego pod kątem nietypowych aktywności.

- *Ataki na łańcuch dostaw (Supply Chain Attacks)*
  - **Opis:** Ataki mające na celu kompromitację dostawców usług lub oprogramowania, aby uzyskać dostęp do danych lub systemów końcowych użytkowników.
  - **Przykład:** Grupa przestępcza może zaatakować firmę dostarczającą oprogramowanie księgowe dla banków, wprowadzając złośliwy kod do aktualizacji oprogramowania, co pozwala na uzyskanie dostępu do systemów bankowych.

- **Obrona:** Staranna weryfikacja dostawców, regularne audyty bezpieczeństwa, stosowanie zasad zero trust, monitorowanie aktualizacji oprogramowania.

5.1.3. Motywacje i cele w sektorze finansowym

Grupy sponsorowane przez państwa działają z różnych powodów, w tym:

- **Strategiczne:** Uzyskanie przewagi w zakresie informacji wywiadowczych, finansowych i gospodarczych nad innymi państwami.
- **Polityczne:** Zakłócenie działalności politycznej i gospodarczej wrogich państw, destabilizacja ich rynków finansowych.
- **Ekonomiczne:** Kradzież informacji finansowych, planów biznesowych i technologii w celu wsparcia własnej gospodarki.
- **Wojskowe:** Przygotowanie się do konfliktów zbrojnych poprzez osłabienie infrastruktury finansowej przeciwnika.

5.2. Zorganizowane Grupy Cyberprzestępcze

5.2.1. Opis

Grupy przestępcze, to zorganizowane zespoły działające na dużą skalę, które angażują się w różne formy cyberprzestępczości. Działają w sposób przypominający korporacje, z jasno określonymi strukturami, zasobami finansowymi i technologicznymi, a także podziałem ról. Ich głównym celem jest osiągnięcie zysków finansowych poprzez nielegalne działania w sieci.

5.2.2. Metody działania

- *Ransomware as a Service (RaaS)*
  - **Opis:** Model biznesowy, w którym grupy przestępcze tworzą i udostępniają ransomware innym cyberprzestępcom za opłatą lub za procent zysków z ataków.
  - **Przykład:** Grupa przestępcza rozwija ransomware i udostępnia go np. na forum w darkwebie, gdzie inni przestępcy mogą go kupić i używać do przeprowadzania ataków na firmy finansowe, żądając okupu za odszyfrowanie danych.
  - **Obrona:** Regularne kopie zapasowe, aktualizacje oprogramowania, stosowanie zaawansowanych narzędzi do wykrywania zagrożeń, edukacja pracowników.

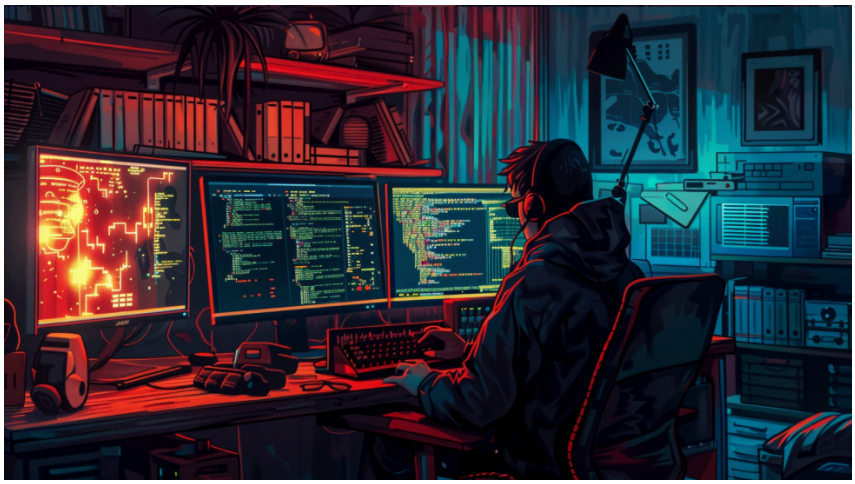
- *Trojany bankowe*
  - **Opis:** Złośliwe oprogramowanie zaprojektowane specjalnie do kradzieży danych uwierzytelniających do kont bankowych i informacji finansowych.
  - **Przykład:** Grupa przestępcza może rozprzestrzeniać trojany bankowe poprzez zainfekowane strony internetowe lub załączniki e-mail, które po zainstalowaniu na komputerze ofiary kradną dane logowania do bankowości internetowej.
  - **Obrona:** Korzystanie z oprogramowania antywirusowego, ostrożność przy otwieraniu załączników i linków w e-mailach, uwierzytelnianie dwuskładnikowe.
- *Kradzież danych kart płatniczych*
  - **Opis:** Proces kradzieży i sprzedaży danych kart kredytowych oraz debetowych na czarnym rynku.
  - **Przykład:** Grupa przestępcza może stosować phishing, aby uzyskać informacje o kartach od ofiar, a następnie sprzedawać te dane na forach przestępczych.
  - **Obrona:** Monitorowanie transakcji, edukacja użytkowników na temat bezpieczeństwa kart płatniczych.
- *Cryptojacking*
  - **Opis:** Proces nielegalnego wykorzystania zasobów komputerowych ofiary do wydobywania kryptowalut.
  - **Przykład:** Grupa przestępcza może infekować serwery bankowe złośliwym oprogramowaniem, które potajemnie wykorzystuje moc obliczeniową tych serwerów do kopania kryptowalut, co może prowadzić do spowolnienia działania systemów i zwiększenia kosztów operacyjnych.
  - **Obrona:** Regularne monitorowanie wydajności systemów, instalacja i aktualizacja oprogramowania zabezpieczającego, wykrywanie i usuwanie złośliwego oprogramowania.
- *Wykorzystanie wizerunku:*
  - **Opis**: Nieautoryzowane wykorzystanie logotypów i wizerunków oraz podszywanie się pod organizację finansową przez grupy przestępcze narusza jej wizerunek oraz reputację.
  - **Przykład:** Grupa przestępcza tworzy phishingową stronę łudząco podobną do strony podmiotu z sektora finansowego. Strona phishingowa może zostać promowana za pomocą kampanii SMS lub reklam w wyszukiwarkach.
  - **Obrona:** Monitorowanie wykorzystania nazw logotypów oraz wizerunku organizacji w internecie, social mediach.

5.2.3. Motywacje i cele w sektorze finansowym

Grupy przestępcze działają z różnych powodów, w tym:

- **Finansowe:** Głównym celem jest uzyskanie jak największych zysków finansowych poprzez kradzież danych, oszustwa i wymuszenia.
- **Ekonomiczne:** Zakłócanie działalności konkurencyjnych firm lub całych sektorów gospodarki w celu uzyskania przewagi na rynku.
- **Technologiczne:** Testowanie i rozwijanie nowych narzędzi oraz technik cyberprzestępczych, które mogą być sprzedawane innym grupom przestępczym.

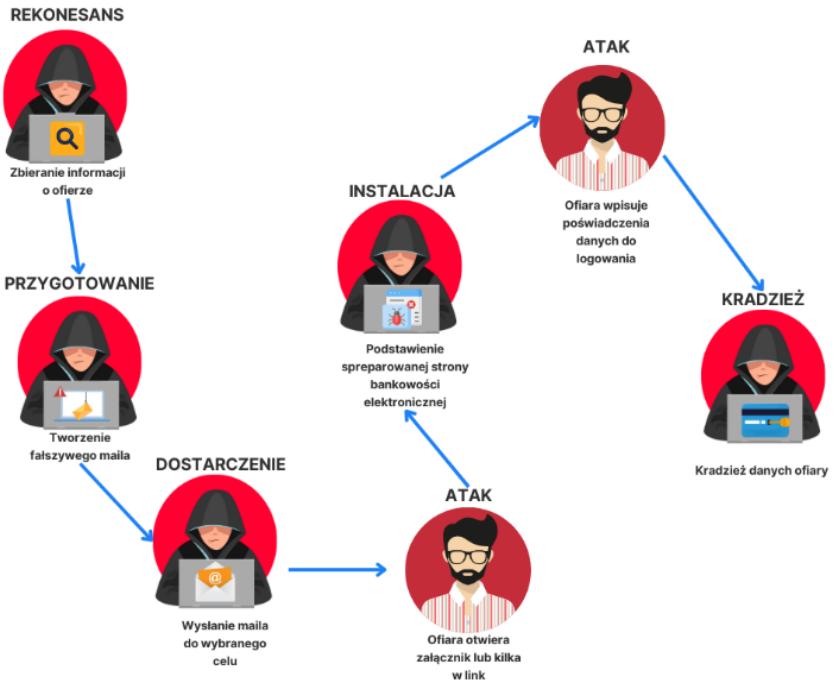
5.3. Indywidualni Cyberprzestępcy



5.3.1. Opis

Indywidualni cyberprzestępcy to pojedyncze osoby działające samodzielnie, które często kierują się motywacją finansową. Dzięki dostępowi do internetu i szerokiej gamie narzędzi dostępnych w sieci za darmo bądź za niewielką opłatą, są w stanie przeprowadzać ataki z dowolnego miejsca, często z własnego domu. Ich działalność może obejmować zarówno ataki na osoby prywatne, jak i na firmy oraz instytucje finansowe. Dzięki swoim umiejętnościom technicznym mogą wykorzystywać różnorodne techniki do osiągania swoich celów.

5.3.2. Metody działania



- *Phishing*
  - **Opis:** Phishing polega na wysyłaniu fałszywych wiadomości e-mail, SMS-ów lub tworzeniu stron internetowych, które naśladują legalne strony, takie jak banki czy serwisy społecznościowe. Celem jest nakłonienie ofiar do ujawnienia swoich danych osobowych, loginów, haseł czy informacji finansowych.
  - **Przykład:** Cyberprzestępca może wysłać e-mail podszywający się pod bank, informując ofiarę o rzekomym problemie z kontem bankowym i prosząc o zalogowanie się na fałszywej stronie w celu "potwierdzenia" swoich danych.
  - **Obrona:** Edukacja użytkowników na temat rozpoznawania podejrzanych wiadomości, korzystanie z uwierzytelniania dwuskładnikowego, filtrowanie wiadomości e-mail.

- *Malware*
  - **Opis:** Malware (złośliwe oprogramowanie) to programy stworzone w celu uszkodzenia systemów komputerowych, kradzieży danych lub przejęcia kontroli nad systemem ofiary.
  - **Przykład:** Cyberprzestępca może wysłać e-mail z załącznikiem zawierającym złośliwe oprogramowanie, które po otwarciu zainfekuje komputer ofiary, umożliwiając przestępcy dostęp do systemu i danych.
  - **Obrona:** Regularne aktualizacje oprogramowania i systemów operacyjnych, instalacja i aktualizacja programów antywirusowych, ostrożność w otwieraniu załączników i linków w e-mailach.

- *Ransomware*
  - **Opis:** Ransomware to rodzaj malware, który szyfruje pliki na komputerze ofiary, blokując do nich dostęp, a następnie żąda okupu za klucz deszyfrujący.
  - **Przykład:** Cyberprzestępca może rozprzestrzeniać ransomware poprzez załączniki e-mail lub zainfekowane strony internetowe. Po zainfekowaniu komputera ofiary, wszystkie pliki zostają zaszyfrowane, a przestępca żąda okupu w kryptowalutach w zamian za odblokowanie plików.
  - **Obrona:** Regularne wykonywanie kopii zapasowych, unikanie klikania na podejrzane linki i załączniki, korzystanie z oprogramowania zabezpieczającego.

- *Kradzież tożsamości*
  - **Opis:** Kradzież tożsamości polega na uzyskaniu dostępu do osobistych informacji ofiary w celu popełnienia oszustwa lub innych przestępstw.
  - **Przykład:** Cyberprzestępca może uzyskać dane osobowe ofiary poprzez phishing, a następnie używać tych informacji do otwierania rachunków bankowych, zaciągania pożyczek lub dokonywania zakupów na koszt ofiary.
  - **Obrona:** Ostrożność w udostępnianiu danych osobowych, korzystanie z silnych haseł, regularne monitorowanie rachunków bankowych i raportów kredytowych.

- *Ataki DDoS (Distributed Denial of Service)*
  - **Opis:** Ataki DDoS polegają na zalewaniu serwerów lub sieci ogromną ilością ruchu, co powoduje przeciążenie i uniemożliwia normalne funkcjonowanie usług.
  - **Przykład:** Cyberprzestępca może przeprowadzić atak DDoS na stronę internetową banku, powodując jej niedostępność dla klientów, co może prowadzić do strat finansowych i reputacyjnych.
  - **Obrona:** Wdrażanie systemów wykrywania i łagodzenia ataków DDoS, korzystanie z usług dostawców zabezpieczeń DDoS, dywersyfikacja infrastruktury sieciowej.

5.3.3. Motywacje i cele

Indywidualni cyberprzestępcy często działają z następujących powodów:

- **Finansowe:** Głównym celem jest zysk, osiągany poprzez kradzież danych, szantaż, sprzedaż informacji na czarnym rynku lub wyłudzenie okupu.
- **Personalne:** Motywacją może być zemsta, chęć zdobycia uznania w środowisku hakerskim lub poczucie wyższości.
- **Ideologiczne:** Czasami działania są motywowane przekonaniami politycznymi lub społecznymi, chociaż indywidualni hakerzy rzadziej mają takie motywacje w porównaniu do grup zorganizowanych lub sponsorowanych przez państwa.

5.4. Użytkownicy wewnętrzni

5.4.1 Opis

Użytkownicy wewnętrzni to pracownicy lub współpracownicy, którzy mają legalny dostęp do systemów i zasobów organizacji, ale wykorzystują swoje uprawnienia do działania na jej szkodę. Mogą działać z różnych powodów, takich jak korzyści finansowe, zemsta, ideologia czy presja ze strony zewnętrznych grup przestępczych. Użytkownicy wewnętrzni są trudni do wykrycia, ponieważ ich działania często wyglądają na rutynowe operacje w ramach ich obowiązków służbowych.

5.4.1. Rodzaje użytkowników wewnętrznych

- *Złośliwi użytkownicy wewnętrzni*
  - **Opis:** Pracownicy, którzy świadomie i celowo działają na szkodę organizacji, motywowani np. korzyściami finansowymi, zemstą czy ideologią.
  - **Przykład:** Pracownik banku, który kradnie dane klientów i sprzedaje je grupom przestępczym lub wykorzystuje te dane do oszustw finansowych.
  - **Obrona:** Regularne audyty bezpieczeństwa, monitorowanie aktywności pracowników, wprowadzenie zasad minimalnych uprawnień, edukacja na temat etyki i bezpieczeństwa.
- *Niedbali użytkownicy wewnętrzni*
  - **Opis:** Pracownicy, którzy nieświadomie narażają organizację na ryzyko poprzez zaniedbanie swoich obowiązków lub brak świadomości na temat bezpieczeństwa.

- **Przykład:** Pracownik, który przypadkowo wysyła poufne informacje na zewnętrzny adres e-mail lub korzysta z łatwego do złamania hasła, co prowadzi do wycieku danych lub konfiguruje mechanizmy niezgodnie ze sztuką.
- **Obrona:** Szkolenie z zakresu bezpieczeństwa, wdrożenie procedur dotyczących bezpiecznego zarządzania danymi, monitorowanie aktywności pracowników.

➢ *Skompromitowani użytkownicy wewnętrzni*

- **Opis:** Pracownicy, którzy zostali zmuszeni do działania na szkodę organizacji przez zewnętrzne grupy przestępcze, często przez szantaż lub groźby.
- **Przykład:** Pracownik banku, który zostaje szantażowany przez cyberprzestępców, aby udostępnić im dostęp do systemów bankowych.
- **Obrona:** Wsparcie psychologiczne i programy pomocy dla pracowników, monitorowanie nietypowych działań, wdrażanie polityki bezpieczeństwa dostępu.

➢ *Brak procesu zarządzania wytwarzanym oprogramowaniem*

- **Opis**: Brak monitorowania procesu wytwarzania oprogramowania, ale również integracji z zewnętrznymi komponentami przez niedoświadczonych lub źle motywowanych pracowników może doprowadzić do braku wycenienia ryzyk.
- **Przykład**: Programiści wykorzystują często różne biblioteki, których kody źródłowe mogą zostać podmienione na biblioteki zawierające złośliwy kod co może doprowadzić do ataku na łańcuch dostaw.
- **Obrona**: Wprowadzenie procesów CI/CD, testów SAST/DAST, centralnych repozytoriów.

➢ *Nieintencjonalne ujawnienie danych wrażliwych*

- **Opis:** W dobie możliwości synchronizowania narzędzi z rozwiązaniami chmurowymi (np. repozytoria kodu, asystenci AI, edytory dokumentów biurowych, serwisy współdzielenia danych), może spowodować to wyciek danych kluczowych dla organizacji.
- **Przykład:** Programista w celu dokończenia pracy w domu i wykorzystaniu pomocy modeli AI synchronizował wewnętrzne repozytorium ze swoim repozytorium w chmurze, przez co doszło do ujawnienia własności intelektualnej, ale również poświadczeń kont technicznych czy kluczy API.
- **Obrona**: Odpowiednie polityki, mechanizmy oraz podnoszenie kompetencji i awareness użytkowników.

5.4.2. Metody działania

➢ *Kradzież danych*

- **Opis:** Użytkownicy wewnętrzni mogą wykorzystywać swoje uprawnienia do kopiowania, kradzieży lub udostępniania poufnych danych, takich jak dane klientów, informacje finansowe czy strategie biznesowe.
- **Przykład:** Pracownik działu IT może skopiować bazę danych klientów i sprzedać ją na czarnym rynku.
- **Obrona:** Implementacja systemów monitorowania dostępu do danych, szyfrowanie danych, segmentacja sieci, regularne audyty bezpieczeństwa.

➢ *Oszustwa*

- **Opis:** Użytkownicy wewnętrzni mogą przeprowadzać oszustwa finansowe, korzystając ze swojego dostępu do systemów transakcyjnych lub kont bankowych.
- **Przykład:** Pracownik banku może manipulować transakcjami finansowymi, aby przekierować fundusze na swoje prywatne konto.

- **Obrona:** Segregacja obowiązków, monitorowanie i analiza transakcji, wdrożenie zasad etyki zawodowej, regularne audyty wewnętrzne.

➢ *Sabotaż*

- **Opis:** Użytkownicy wewnętrzni mogą celowo niszczyć dane, uszkadzać systemy lub zakłócać operacje organizacji w celu wyrządzenia szkody.
- **Przykład:** Pracownik IT może zainfekować sieć bankową złośliwym oprogramowaniem lub usunąć kluczowe dane z systemów.
- **Obrona:** Regularne kopie zapasowe, wdrożenie systemów wykrywania zagrożeń, restrykcyjne polityki dostępu, monitorowanie aktywności systemowej.

➢ *Cyberszpiegostwo*

- **Opis:** Użytkownicy wewnętrzni mogą zbierać poufne informacje i przekazywać je konkurencyjnym firmom lub zagranicznym rządom.
- **Przykład:** Pracownik banku może wykradać informacje o strategiach inwestycyjnych i przekazywać je konkurencyjnym instytucjom finansowym.
- **Obrona:** Szkolenie pracowników w zakresie ochrony informacji, monitorowanie aktywności pracowników, wprowadzenie zasad minimalnych uprawnień.

5.4.3. Motywacje i cele w sektorze finansowym

Użytkownicy wewnętrzni mogą działać z różnych powodów, w tym:

- **Finansowe:** Zysk finansowy poprzez kradzież danych, oszustwa lub sprzedaż informacji.
- **Zemsta:** Chęć wyrządzenia szkody organizacji z powodu niezadowolenia z pracy lub konfliktów personalnych.
- **Presja zewnętrzna:** Szantaż lub groźby ze strony grup przestępczych lub konkurencyjnych firm.
- **Ideologiczne:** Działania motywowane przekonaniami politycznymi, społecznymi lub etycznymi.
- **Brak świadomości:** Działania spowodowane brakiem kompetencji, wykonane nieintencjonalnie.

5.5 Haktywiści

5.5.1 Opis

Haktywiści to osoby lub grupy wykorzystujące swoje umiejętności techniczne do przeprowadzania cyberataków motywowanych ideologicznie, politycznie lub społecznie. W odróżnieniu od typowych cyberprzestępców, głównym celem haktywistów nie jest zysk finansowy, lecz promowanie określonej agendy, wyrażanie protestu lub wywieranie nacisku na organizacje i rządy. Grupy prorosyjskie stanowią znaczący segment tego środowiska, działając często w ramach nieoficjalnego wsparcia dla interesów rosyjskich.

5.5.2. Metody działania

- *Ataki DDoS (Distributed Denial of Service)*
  - **Opis:** Masowe ataki polegające na przeciążeniu infrastruktury IT celem czasowego zablokowania dostępu do usług lub stron internetowych.
  - **Przykład:** Grupy haktywistyczne przeprowadzają skoordynowane ataki DDoS na instytucje finansowe, powodując niedostępność serwisów bankowych i generując straty wizerunkowe.
  - **Obrona:** Implementacja rozwiązań anti-DDoS, monitorowanie ruchu sieciowego, korzystanie z usług CDN, geolokalizacyjna filtracja ruchu sieciowego.
- *Defacement*
  - **Opis:** Nieautoryzowana modyfikacja zawartości stron internetowych, polegająca na podmianie treści oficjalnych witryn na propagandowe komunikaty.
  - **Przykład:** Haktywiści włamują się na stronę banku i umieszczają na niej treści polityczne, symbole prorosyjskie lub oskarżenia wobec danej instytucji.
  - **Obrona:** Regularne aktualizacje CMS, audyty bezpieczeństwa aplikacji webowych, wdrożenie WAF (Web Application Firewall), monitoring treści witryn.
- *Doxing*
  - **Opis:** Gromadzenie i publikowanie prywatnych danych osób związanych z atakowaną instytucją, takich jak dane personalne, adresy, numery telefonów czy informacje o członkach rodziny.
  - **Przykład:** Haktywiści publikują dane osobowe kadry zarządzającej instytucji finansowej, która wspiera inicjatywy uznawane przez nich za wrogie, narażając te osoby na zagrożenia fizyczne.
  - **Obrona:** Ograniczanie informacji dostępnych publicznie, szkolenia z zakresu ochrony prywatności, monitoring dark webu i kanałów komunikacji haktywistów.
- *Operacje informacyjne i dezinformacyjne*
  - **Opis:** Rozpowszechnianie fałszywych informacji mających na celu destabilizację rynków finansowych lub podważenie zaufania do instytucji finansowych.
  - **Przykład:** Grupy haktywistyczne rozpowszechniają fałszywe informacje o niewypłacalności banku, co może wywołać panikę wśród klientów i doprowadzić do masowego wycofywania środków.
  - **Obrona:** Monitorowanie mediów społecznościowych, przygotowane plany kryzysowe, proaktywna komunikacja z klientami, współpraca z organami ścigania.
- *Hacktivism-as-a-Service*
  - **Opis:** Udostępnianie narzędzi, infrastruktury i wiedzy umożliwiających osobom bez zaawansowanych umiejętności technicznych uczestniczenie w działaniach haktywistycznych.
  - **Przykład:** Grupy haktywistyczne, tworzą dostępne dla szerokiego grona sympatyków platformy do przeprowadzania ataków DDoS na wybrane cele, w tym instytucje finansowe.
  - **Obrona:** Monitorowanie kanałów komunikacji haktywistów, analiza zagrożeń, współpraca z CERT i organami ścigania, wymiana informacji w ramach sektora.

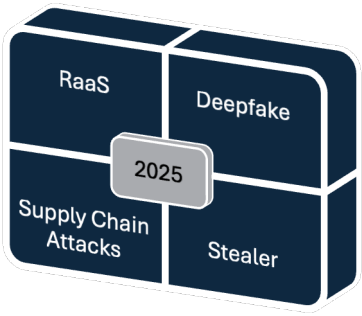
5.5.3. Motywacje i cele w sektorze finansowym

Haktywiści działają z różnych powodów:

- **Polityczne:** Ataki na instytucje finansowe krajów uznawanych za wrogie, w celu wywierania presji i destabilizacji.
- **Propagandowe:** Demonstracja siły i zdolności do przeprowadzania ataków, które mogą być wykorzystane w narracjach propagandowych.

- **Strategiczne:** Osłabianie zaufania do instytucji finansowych i systemów ekonomicznych.
- **Odwetowe:** Ataki w odpowiedzi na sankcje ekonomiczne lub działania postrzegane jako wrogie wobec interesów kraju atakującego.
- **Testowe:** Sprawdzanie skuteczności metod i narzędzi, które mogą być później wykorzystane w bardziej zaawansowanych operacjach.

6. Trendy w cyberprzestępczości w 2025 roku



W 2025 roku obserwujemy znaczący rozwój i ewolucję zagrożeń cyberprzestępczych. Przestępcy coraz częściej korzystają z zaawansowanych technologii oraz wyrafinowanych metod ataków, które stają się coraz trudniejsze do wykrycia i zwalczania. Wśród najważniejszych trendów wyróżniają się:

Ataki z wykorzystaniem narzędzi opartych o AI (np. deepfake)

- **Opis:** Cyberprzestępcy wykorzystują sztuczną inteligencję do tworzenia realistycznych, ale fałszywych obrazów, filmów i dźwięków. Narzędzia takie jak deepfake są używane do oszustw finansowych, kradzieży tożsamości i manipulacji, co stanowi poważne zagrożenie dla instytucji finansowych.

Ataki na łańcuch dostaw (Supply Chain Attacks)

- **Opis:** Przestępcy atakują dostawców usług lub oprogramowania, aby uzyskać dostęp do systemów i danych użytkowników końcowych. Tego rodzaju ataki mogą prowadzić do masowych wycieków danych i poważnych zakłóceń w działalności instytucji finansowych.

Ransomware as a Service (RaaS)

- **Opis:** Model biznesowy, w którym grupy przestępcze tworzą i udostępniają ransomware innym cyberprzestępcom za opłatą lub za procent zysków z ataków. RaaS zwiększa dostępność i częstotliwość ataków ransomware, stanowiąc poważne zagrożenie dla sektora finansowego.

Malware typu stealer

- **Opis:** Złośliwe oprogramowanie zaprojektowane do kradzieży poufnych informacji, takich jak dane logowania, hasła i dane finansowe. Stealery są coraz częściej wykorzystywane przez cyberprzestępców do uzyskiwania dostępu do kont bankowych i innych zasobów finansowych.

Wzrost zaawansowania technologicznego i ewolucja metod ataków wymagają od instytucji finansowych ciągłej adaptacji i doskonalenia strategii bezpieczeństwa. Świadomość obecnych trendów i zagrożeń jest kluczowa dla skutecznej ochrony przed cyberprzestępczością w 2025 roku.

6.1. Ataki z wykorzystaniem narzędzi opartych o AI (np. deepfake)

6.1.1. Opis

Ataki z wykorzystaniem narzędzi opartych o sztuczną inteligencję (AI) stają się coraz bardziej powszechne i zaawansowane. Jednym z przykładów jest technologia deepfake, która wykorzystuje AI do tworzenia realistycznych, ale fałszywych obrazów, filmów lub dźwięków. Deepfake może być używany do podszywania się pod osoby zaufane, co może prowadzić do oszustw finansowych, kradzieży tożsamości oraz innych form manipulacji.

6.1.2. Metody działania

- *Phishing z wykorzystaniem deepfake*
  - **Opis:** Cyberprzestępcy mogą używać technologii deepfake do tworzenia fałszywych wiadomości wideo lub audio, które wyglądają i brzmią jak autentyczne komunikaty od zaufanych osób, takich jak dyrektorzy banków czy pracownicy działu IT.
  - **Przykład:** Przestępcy mogą nawiązać połączenie przez wideokonferencję, gdzie za pomocą deepfake będą się podszywać pod dyrektora banku, prosząc pracownika o wykonanie pilnego przelewu na konto oszustów. Pracownik, widząc "dyrektora", może nie podejrzewać oszustwa i wykonać polecenie.
  - **Obrona:** Edukacja pracowników na temat zagrożeń związanych z deepfake, wprowadzenie procedur weryfikacji tożsamości przy ważnych transakcjach, korzystanie z technologii wykrywania deepfake.
- *Podszywanie się pod bank (spoofing)*
  - **Opis:** Cyberprzestępcy mogą używać technologii deepfake do podszywania się pod pracowników banku, takich jak konsultanci, których klienci znają, aby zdobyć zaufanie i wyłudzić dane.
  - **Przykład:** Przestępcy mogą stworzyć fałszywy głos konsultanta, którego klient zna z placówki bankowej i za jego pomocą przekonać klienta do podania danych logowania lub innych poufnych informacji. Taka rozmowa telefoniczna lub wiadomość głosowa może być bardzo przekonująca dla klienta.
  - **Obrona:** Wprowadzenie dodatkowych warstw weryfikacji tożsamości, takich jak pytania bezpieczeństwa, monitorowanie nietypowych działań na kontach, informowanie klientów o nowych formach oszustw.

- *Ataki reputacyjne*
  - **Opis:** Deepfake mogą być używane do tworzenia fałszywych materiałów kompromitujących osoby lub instytucje, co może prowadzić do utraty reputacji i zaufania publicznego.
  - **Przykład:** Przestępcy mogą opublikować fałszywy film, w którym dyrektor banku popełnia przestępstwo lub wypowiada kontrowersyjne opinie, co może prowadzić do spadku zaufania klientów i inwestorów.
  - **Obrona:** Szybka reakcja na incydenty związane z deepfake, monitorowanie mediów i sieci społecznościowych w poszukiwaniu fałszywych treści, wprowadzenie strategii zarządzania kryzysowego.

6.1.3. Motywacje i cele w sektorze finansowym

Ataki z wykorzystaniem narzędzi opartych o AI, takich jak deepfake, są motywowane różnorodnymi celami:

- **Finansowe:** Uzyskanie dostępu do środków finansowych poprzez oszustwa i manipulacje.
- **Polityczne:** Destabilizacja instytucji finansowych w celu osiągnięcia korzyści politycznych lub gospodarczych.
- **Osobiste:** Zemsta lub szantaż osób związanych z instytucjami finansowymi.
- **Reputacyjne:** Zniszczenie zaufania do instytucji finansowych poprzez publikowanie kompromitujących materiałów.

6.1.4. Analiza Ryzyka

- *Ocena Prawdopodobieństwa*

Częstotliwość ataków:

- **Opis:** Ataki z wykorzystaniem AI, w tym deepfake, są wciąż stosunkowo nowe, ale ich częstotliwość rośnie wraz z rozwojem technologii. Sektor finansowy jest jednym z głównych celów ze względu na potencjalne zyski finansowe.
- **Przykład:** W ostatnich latach odnotowano kilka incydentów związanych z użyciem deepfake w próbach oszustw finansowych, a liczba takich ataków ma tendencję wzrostową.

Trendy:

- **Opis:** Technologia deepfake staje się coraz bardziej dostępna i zaawansowana, co zwiększa ryzyko jej wykorzystania w atakach na sektor finansowy. Zwiększa się również świadomość przestępców o potencjalnych zyskach z takich ataków.
- **Obserwacja:** Wzrost liczby dostępnych narzędzi do tworzenia deepfake oraz rosnące zainteresowanie przestępców technologiami AI wskazują na rosnące ryzyko takich ataków w przyszłości.

- *Ocena Skutków*

- **Skutki:** Ataki z wykorzystaniem deepfake mogą prowadzić do poważnych strat finansowych, kradzieży tożsamości, oszustw oraz utraty reputacji instytucji finansowych. Długoterminowe konsekwencje mogą obejmować spadek zaufania klientów i inwestorów.
- **Przykład:** Udany atak phishingowy z użyciem deepfake może prowadzić do przekazania dużych sum pieniędzy oszustom, co może spowodować poważne straty finansowe dla banku i jego klientów.

➢ *Podsumowanie*

Ataki z wykorzystaniem narzędzi opartych o AI, takich jak deepfake, stanowią rosnące zagrożenie dla sektora finansowego. Chociaż są stosunkowo nowe, ich częstotliwość i złożoność rosną, co wymaga od instytucji finansowych stałego monitorowania, edukacji pracowników oraz wdrażania zaawansowanych systemów detekcji i obrony. Proaktywne podejście do zarządzania ryzykiem związanym z deepfake jest kluczowe dla minimalizacji potencjalnych skutków takich ataków.

6.2. Ataki na łańcuch dostaw (Supply Chain Attacks)

6.2.1. Opis

Ataki na łańcuch dostaw mają na celu kompromitację dostawców usług lub oprogramowania, aby uzyskać dostęp do danych lub systemów końcowych użytkowników. Tego typu ataki są szczególnie niebezpieczne, ponieważ mogą wpłynąć na wiele organizacji jednocześnie, poprzez wprowadzenie złośliwego oprogramowania na etapie produkcji lub aktualizacji oprogramowania dostarczanego przez zaufanych dostawców.

6.2.2. Metody działania

➢ *Kompromitacja dostawców oprogramowania*

- **Opis:** Cyberprzestępcy mogą zaatakować dostawców oprogramowania, aby wprowadzić złośliwy kod do produktów, które następnie są instalowane u końcowych użytkowników, takich jak banki.
- **Przykład:** Grupa przestępcza może zaatakować firmę dostarczającą oprogramowanie księgowe dla banków, wprowadzając złośliwy kod do aktualizacji oprogramowania, co pozwala na uzyskanie dostępu do systemów bankowych.
- **Obrona:** Staranna weryfikacja dostawców, regularne audyty bezpieczeństwa, stosowanie zasad zero trust, monitorowanie aktualizacji oprogramowania.

➢ *Ataki na infrastrukturę dostawców usług*

- **Opis:** Cyberprzestępcy mogą kompromitować infrastrukturę dostawców usług, takich jak dostawcy chmur czy dostawcy zarządzanych usług IT, aby uzyskać dostęp do danych i systemów klientów tych dostawców.
- **Przykład:** Atak na dostawcę usług chmurowych, który przechowuje dane bankowe, może umożliwić cyberprzestępcom dostęp do poufnych informacji klientów banku.
- **Obrona:** Wymóg silnych standardów bezpieczeństwa od dostawców, regularne przeglądy i audyty bezpieczeństwa, segmentacja danych i infrastruktury.

➢ *Infiltracja łańcucha dostaw sprzętu*

- **Opis:** Ataki polegające na kompromitacji sprzętu komputerowego lub sieciowego na etapie produkcji lub dostawy, aby wprowadzić złośliwe komponenty lub modyfikacje.
- **Przykład:** Wprowadzenie złośliwych układów scalonych do sprzętu sieciowego używanego przez banki, co pozwala cyberprzestępcom na monitorowanie i przechwytywanie danych przesyłanych przez te urządzenia.
- **Obrona:** Stosowanie certyfikowanych dostawców sprzętu, audyty sprzętowe przed wdrożeniem, ścisła kontrola łańcucha dostaw.

6.2.3. Motywacje i cele w sektorze finansowym

Ataki na łańcuch dostaw są motywowane różnorodnymi celami:

- **Finansowe:** Uzyskanie dostępu do danych finansowych, które mogą być wykorzystane do kradzieży lub szantażu.
- **Strategiczne:** Zakłócenie działalności finansowej instytucji wrogich państw lub konkurencyjnych firm.
- **Operacyjne:** Przejęcie kontroli nad infrastrukturą IT banków i innych instytucji finansowych w celu dalszej infiltracji i wykradania danych.

6.2.4. Analiza Ryzyka

➢ *Ocena Prawdopodobieństwa*

Częstotliwość ataków:

- **Opis:** Ataki na łańcuch dostaw stają się coraz bardziej powszechne i złożone, ponieważ przestępcy zdają sobie sprawę z potencjalnych korzyści z kompromitacji dostawców usług i oprogramowania. Wzrost globalnych powiązań biznesowych zwiększa ryzyko takich ataków.
- **Przykład:** W ostatnich latach odnotowano wzrost liczby ataków na dostawców oprogramowania i usług IT, które miały na celu kompromitację systemów bankowych i innych instytucji finansowych.

Trendy:

- **Opis:** Cyberprzestępcy coraz częściej koncentrują swoje wysiłki na łańcuchu dostaw, wiedząc, że udane ataki mogą umożliwić dostęp do wielu celów jednocześnie. Coraz więcej dostawców integruje zaawansowane technologie, co zwiększa powierzchnię ataku.
- **Obserwacja:** Rozwój technologii IoT (Internet of Things) i rosnące uzależnienie od usług zewnętrznych dostawców zwiększa ryzyko ataków na łańcuch dostaw.

➢ *Ocena Skutków*

- **Skutki:** Ataki na łańcuch dostaw mogą prowadzić do masowych wycieków danych, strat finansowych, zakłóceń w działalności operacyjnej i uszkodzenia reputacji instytucji finansowych. Skutki takich ataków są często długotrwałe i trudne do zaradzenia.
- **Przykład:** Kompromitacja oprogramowania księgowego używanego przez wiele banków może prowadzić do utraty danych finansowych, zakłóceń w obsłudze klienta i znaczących strat finansowych dla zaatakowanych instytucji.

➢ *Przykładowe ataki na łańcuch dostaw*

✓ Log4j

- **Opis:** Atakujący zidentyfikowali podatność w bibliotece Apache Log4j, z której korzysta wiele komercyjnych rozwiązań.
- **Przebieg ataku:** Atakujący wysyłali odpowiednio spreparowane żądania, które umożliwiały wykonanie komend na podatnym serwerze. Mogło to prowadzić do wycieku danych lub przejęcia części infrastruktury.

✓ Kaseya

- **Opis:** Kaseya VSA to platforma do zarządzania systemami IT, często wykorzystywana do zarządzania infrastrukturą przez firmy świadczące outsourcing IT.

- **Przebieg ataku:** Atakujący zidentyfikowali podatność w oprogramowaniu i wykorzystali ją do infekowania zarządzanych przez to oprogramowanie infrastruktur złośliwym oprogramowaniem typu ransomware. Atak spowodował, że Kaseya musiała wyłączyć część usług, aby ograniczyć skutki i rozprzestrzenianie się złośliwego oprogramowania.

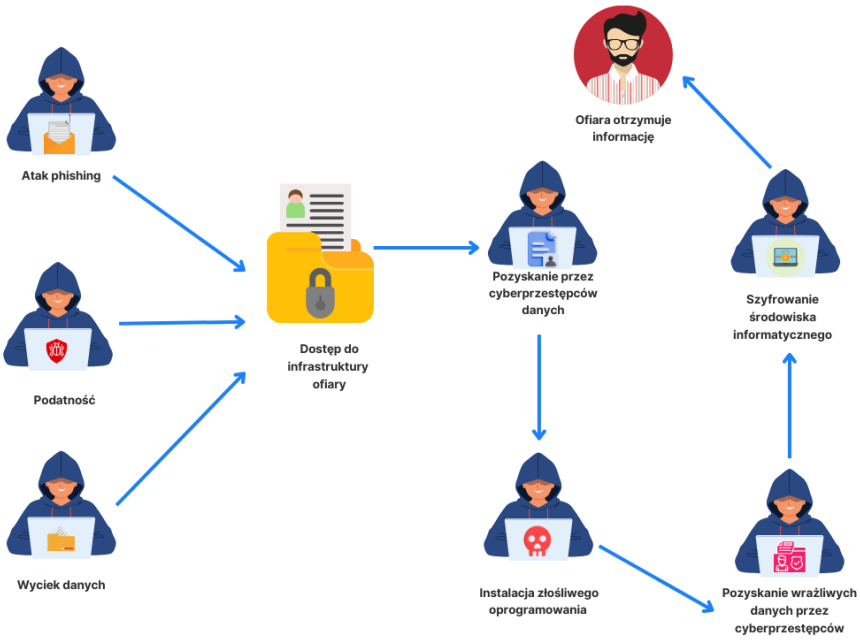
✓ SolarWinds
- **Opis:** Atakujący przejęli infrastrukturę firmy SolarWinds, dostawcy rozwiązania Orion, i dodali do jednej z aktualizacji złośliwy kod.
- **Przebieg ataku:** Dodany fragment kodu zbierał informacje o infrastrukturze i w wybranych przypadkach instalował backdoory, które pozwalały adwersarzom na utrzymanie persystencji w przejętych systemach.

✓ Polyfill.io
- **Opis:** Atakujący przejęli wygasłą domenę, na której hostowany był skrypt .js zaimplementowany w wielu rozwiązaniach webowych.
- **Przebieg ataku:** Adwersarze podmienili skrypt .js na taki, który zawierał złośliwy kod, co pozwoliło na infekowanie użytkowników stron, które w źródłach miały zaimplementowane skrypty z polyfill.io.

➢ *Podsumowanie*

Ataki na łańcuch dostaw stanowią poważne zagrożenie dla sektora finansowego ze względu na ich zdolność do kompromitacji wielu organizacji jednocześnie. Wzrost liczby powiązań z dostawcami oraz rozwój technologii zwiększa ryzyko takich ataków. Proaktywne podejście do zarządzania ryzykiem, w tym staranna weryfikacja dostawców, regularne audyty bezpieczeństwa oraz wdrażanie zasad zero trust, są kluczowe dla minimalizacji potencjalnych skutków ataków na łańcuch dostaw.

6.3. Ransomware as a Service (RaaS)



6.3.1. Opis

Ransomware as a Service (RaaS) to model biznesowy, w którym grupy przestępcze tworzą i udostępniają ransomware innym cyberprzestępcom za opłatą lub za procent zysków z ataków. Taki model umożliwia nawet osobom bez specjalistycznej wiedzy technicznej przeprowadzanie ataków ransomware, co znacząco zwiększa skalę i zasięg tych ataków.

6.3.2. Metody działania

- *Zwiększenie dostępności ransomware:*
  - **Opis:** Grupy przestępcze rozwijają złośliwe oprogramowanie i udostępniają je na forach w darkwebie, co umożliwia szerokiemu gronu przestępców przeprowadzanie ataków na różne sektory, w tym sektor finansowy.
  - **Przykład:** Przestępcy mogą kupić dostęp do gotowego ransomware i przeprowadzić atak na instytucję finansową, żądając okupu za odszyfrowanie danych.
  - **Obrona:** Regularne kopie zapasowe, aktualizacje oprogramowania, stosowanie zaawansowanych narzędzi do wykrywania zagrożeń, edukacja pracowników.

- *Usługi wsparcia technicznego dla cyberprzestępców:*
  - **Opis:** Dostawcy RaaS oferują swoim klientom wsparcie techniczne, pomagając im w skutecznym przeprowadzaniu ataków oraz w maksymalizacji zysków z okupu.
  - **Przykład:** Grupa przestępcza może oferować instrukcje, wsparcie na żywo oraz narzędzia do zarządzania atakami ransomware, co zwiększa efektywność i skuteczność ataków.
  - **Obrona:** Wprowadzenie polityk bezpieczeństwa, monitorowanie nietypowych działań w sieci, zastosowanie technik analizy behawioralnej.

- *Szyfrowanie danych i złożone metody ataku:*
  - **Opis:** Twórcy RaaS nie tylko dostarczają narzędzia ransomware, ale również oferują zaawansowane funkcje, takie jak złożone algorytmy szyfrowania i metody unikania wykrycia, które zwiększają skuteczność ataków.
  - **Przykład:** Przestępcy korzystający z RaaS mogą uzyskać dostęp do zaawansowanych metod szyfrowania danych, co utrudnia ofiarom odzyskanie danych bez zapłacenia okupu.
  - **Obrona:** Segmentacja sieci, wdrażanie zasad zero trust, regularne testy penetracyjne i audyty bezpieczeństwa.

6.3.3. Motywacje i cele w sektorze finansowym

Ransomware as a Service jest motywowane różnorodnymi celami:

- **Finansowe:** Głównym celem jest uzyskanie jak największych zysków finansowych poprzez wymuszanie okupów od ofiar.
- **Operacyjne:** Umożliwienie szerokiego dostępu do zaawansowanych narzędzi ransomware nawet mniej doświadczonym przestępcom, co zwiększa liczbę potencjalnych ataków.
- **Strategiczne:** Destabilizacja działalności finansowej instytucji poprzez blokowanie dostępu do kluczowych danych i systemów.

6.3.4. Analiza Ryzyka

- *Ocena Prawdopodobieństwa*

  Częstotliwość ataków:

- **Opis:** RaaS znacząco zwiększa dostępność i częstotliwość ataków ransomware, ponieważ pozwala przestępcom na łatwe przeprowadzanie ataków bez potrzeby posiadania zaawansowanej wiedzy technicznej.
- **Przykład:** Sektor finansowy, ze względu na swoje zasoby, jest częstym celem ataków ransomware.

Trendy:

- **Opis:** Trendy wskazują na dalszy wzrost popularności RaaS, co jest napędzane przez rozwój darkwebu i rosnące zapotrzebowanie na złośliwe oprogramowanie. Ataki stają się coraz bardziej zaawansowane i trudniejsze do wykrycia.
- **Obserwacja:** Wzrost liczby usług RaaS na darkwebie oraz rosnąca liczba ataków ransomware wskazują na rosnące ryzyko takich ataków w przyszłości.

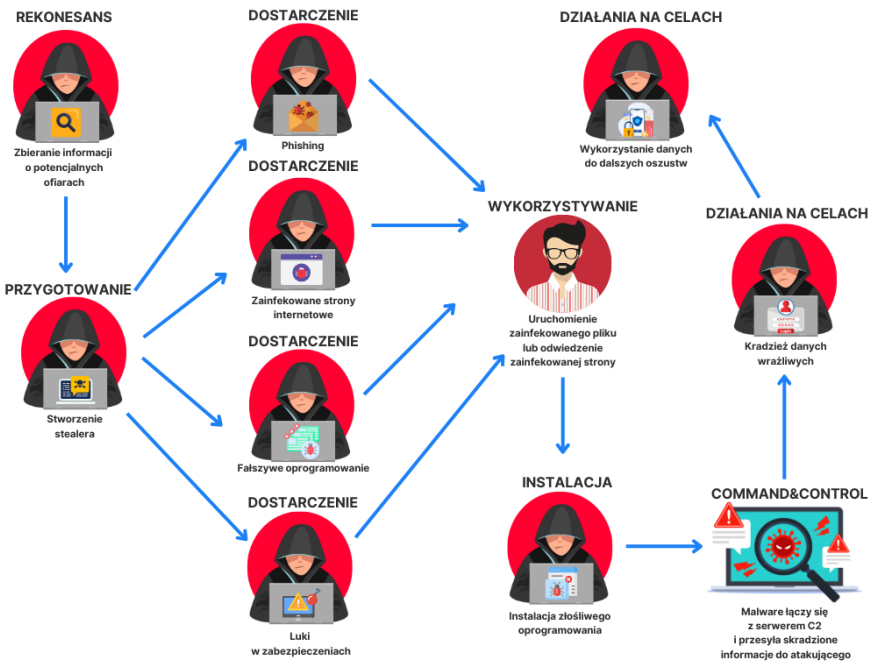
➢ *Ocena Skutków*

- **Skutki:** Ataki ransomware mogą prowadzić do utraty dostępu do kluczowych danych, wymuszania okupów, zakłóceń w działalności operacyjnej oraz uszkodzenia reputacji instytucji finansowych. Koszty związane z atakami obejmują zarówno bezpośrednie straty finansowe, jak i koszty odzyskiwania danych oraz wdrażania środków zapobiegawczych.
- **Przykład:** Udany atak ransomware na bank może sparaliżować jego operacje na kilka dni, prowadząc do ogromnych strat finansowych i reputacyjnych oraz konieczności inwestowania w zaawansowane systemy ochrony.

➢ *Podsumowanie*

Ransomware as a Service stanowi poważne zagrożenie dla sektora finansowego, umożliwiając szerokiemu gronu cyberprzestępców dostęp do zaawansowanych narzędzi ransomware. Wzrost popularności RaaS prowadzi do zwiększenia częstotliwości i złożoności ataków, co wymaga od instytucji finansowych stałego monitorowania, wdrażania zaawansowanych systemów ochrony oraz edukacji pracowników. Proaktywne podejście do zarządzania ryzykiem związanym z RaaS jest kluczowe dla minimalizacji potencjalnych skutków takich ataków.

6.4. Malware typu stealer



6.4.1. Opis

Stealery to złośliwe oprogramowanie zaprojektowane do kradzieży poufnych informacji, takich jak dane logowania, hasła, dane karty kredytowej, informacje bankowe oraz inne dane osobowe. Stealery mogą być rozpowszechniane poprzez różne metody, w tym phishing, zainfekowane strony internetowe oraz złośliwe załączniki e-mail. Dane zebrane przez stealer są często sprzedawane na czarnym rynku lub wykorzystywane do przeprowadzania dalszych ataków.

6.4.2. Metody działania

- *Dystrybucja poprzez phishing i złośliwe załączniki*
  - **Opis:** Cyberprzestępcy rozsyłają e-maile phishingowe zawierające złośliwe załączniki lub linki, które po kliknięciu instalują stealer na komputerze ofiary.
  - **Przykład:** Przestępcy mogą wysłać e-mail udający wiadomość od banku, zawierający złośliwy załącznik, który po otwarciu instaluje stealer, kradnący dane logowania do konta bankowego ofiary.
  - **Obrona:** Szkolenie pracowników na temat rozpoznawania phishingu, wdrażanie zaawansowanych filtrów antyphishingowych, regularne aktualizacje oprogramowania antywirusowego.

- *Dystrybucja poprzez zainfekowane pliki do pobrania*
  - **Opis:** Cyberprzestępcy mogą umieszczać złośliwe oprogramowanie w popularnych plikach do pobrania, takich jak darmowe programy lub aktualizacje oprogramowania, które po zainstalowaniu na komputerze ofiary kradną dane.
  - **Przykład:** Przestępcy mogą umieścić stealer w pliku do pobrania z fałszywej strony oferującej darmowe oprogramowanie lub aktualizacje, które po zainstalowaniu na komputerze ofiary kradną dane logowania do kont bankowych.
  - **Obrona:** Korzystanie z legalnych źródeł oprogramowania, wdrażanie systemów wykrywania zagrożeń w pobieranych plikach, regularne aktualizacje oprogramowania zabezpieczającego.

- *Stealery jako usługa (Stealer as a Service, SaaS)*
  - **Opis:** Podobnie jak w przypadku Ransomware as a Service (RaaS), stealery są dostępne jako usługa na czarnym rynku. Cyberprzestępcy mogą wynajmować lub kupować stealery od innych przestępców, co umożliwia im przeprowadzanie ataków bez potrzeby posiadania zaawansowanej wiedzy technicznej.
  - **Przykład:** Cyberprzestępca może wynająć stealer na czarnym rynku i użyć go do kradzieży danych logowania do kont bankowych z komputerów ofiar.
  - **Obrona:** Regularne monitorowanie sieci i systemów pod kątem nietypowych działań, wdrażanie zasad zero trust, segmentacja sieci.

6.4.3. Motywacje i cele w sektorze finansowym

Stealery są motywowane różnorodnymi celami:

- **Finansowe:** Głównym celem jest uzyskanie danych finansowych, które mogą być wykorzystane do kradzieży środków lub oszustw finansowych.
- **Operacyjne:** Umożliwienie szerokiego dostępu do poufnych informacji nawet mniej doświadczonym przestępcom, co zwiększa liczbę potencjalnych ataków.
- **Strategiczne:** Zbieranie danych, które mogą być wykorzystane w przyszłych atakach lub sprzedane na czarnym rynku.

6.4.4. Analiza Ryzyka

- *Ocena Prawdopodobieństwa*

Częstotliwość ataków:

- **Opis:** Ataki z wykorzystaniem stealerów są coraz częstsze, ponieważ złośliwe oprogramowanie staje się łatwiej dostępne i bardziej zaawansowane. Sektor finansowy jest szczególnie narażony ze względu na wysoką wartość przechowywanych danych.
- **Przykład:** Banki i inne instytucje finansowe są regularnie celem ataków z wykorzystaniem stealerów, co prowadzi do licznych przypadków kradzieży danych.

Trendy:

- **Opis:** Trendy wskazują na rosnącą popularność stealerów jako usługi (Stealer as a Service, SaaS), co zwiększa dostępność tego typu oprogramowania i prowadzi do wzrostu liczby ataków.
- **Obserwacja:** Wzrost liczby usług SaaS na czarnym rynku oraz rosnąca liczba ataków z wykorzystaniem stealerów wskazują na rosnące ryzyko takich ataków w przyszłości.

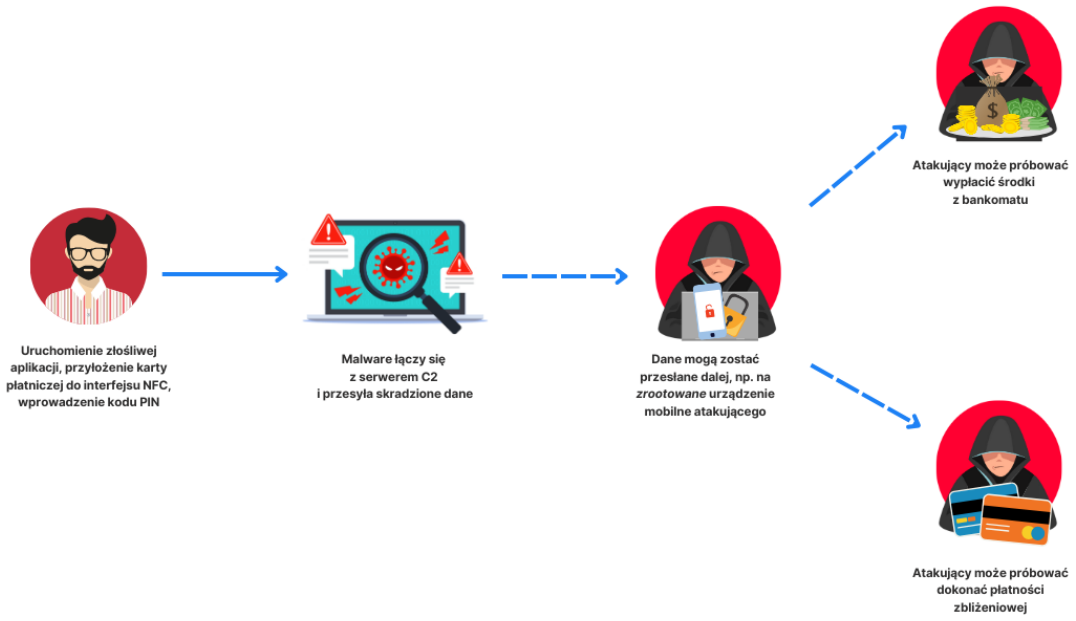
- *Ocena Skutków*

- **Skutki:** Ataki z wykorzystaniem stealerów mogą prowadzić do kradzieży poufnych danych, utraty zaufania klientów, strat finansowych oraz uszkodzenia reputacji instytucji finansowych. Koszty związane z atakami obejmują zarówno bezpośrednie straty finansowe, jak i koszty związane z odzyskiwaniem danych oraz wdrażaniem środków zapobiegawczych.
- **Przykład:** Udany atak z wykorzystaniem stealera może prowadzić do kradzieży danych logowania do kont bankowych klientów, co może skutkować znaczącymi stratami finansowymi dla banku oraz jego klientów.

- *Podsumowanie*

Stealery stanowią poważne zagrożenie dla sektora finansowego, umożliwiając cyberprzestępcom kradzież poufnych danych finansowych. Wzrost popularności Stealer as a Service (SaaS) prowadzi do zwiększenia częstotliwości i złożoności ataków, co wymaga od instytucji finansowych stałego monitorowania, wdrażania zaawansowanych systemów ochrony oraz edukacji pracowników. Proaktywne podejście do zarządzania ryzykiem związanym ze stealerami jest kluczowe dla minimalizacji potencjalnych skutków takich ataków.

6.5. Malware typu NFC relay



6.5.1. Opis

Atak NFC Relay wykorzystuje złośliwe oprogramowanie na urządzeniu mobilnym ofiary, umożliwiając odczytywanie, przesyłanie i wykorzystywanie na zdalnym urządzeniu agresora, danych pozyskanych z użyciem technologii NFC (ang. Near-Field Communication[1]). Przykład wykradanych informacji mogą stanowić dane przekazywane przez zbliżeniowe moduły kart płatniczych. Zebrane dane mogą zostać użyte przez atakujących np. do prób wypłaty środków z bankomatów oraz realizacji płatności zbliżeniowych.

6.5.2. Metody działania

➢ *Złośliwe oprogramowanie na urządzenia z systemem Android*

- **Opis:** Atakujący mogą przygotowywać niebezpieczne aplikacje mobilne, wykradające wrażliwe dane z wykorzystaniem technologii NFC.

- **Przykład:** Cyberprzestępcy przygotowują złośliwą aplikację mobilną, podszywającą się np. pod istniejący bank. Szkodliwa aplikacja, pod pozorem weryfikacji klienta, nakłania ofiarę do przyłożenia karty płatniczej do interfejsu NFC w urządzeniu mobilnym oraz wprowadzenia kodu PIN. Złośliwe oprogramowanie może następnie dokonać próby przekazania zebranych danych do serwera C2, celem dalszego wykorzystania, np. z użyciem zdalnego urządzenia atakującego.

- **Obrona:** Pobieranie oprogramowania wyłącznie z zaufanych źródeł oraz edukacja klientów na temat aktualnych trendów cyberzagrożeń.

[1] https://pl.wikipedia.org/wiki/Komunikacja_bliskiego_zasi%C4%99gu

6.5.3. Motywacje i cele w sektorze finansowym

- **Finansowe:** Głównym celem ataków NFC Relay jest pozyskanie wrażliwych danych dotyczących karty płatniczej, a następnie wykorzystanie ich przez atakujących w celu kradzieży środków.

6.5.4. Analiza Ryzyka

➢ *Ocena Prawdopodobieństwa*

Częstotliwość ataków:

- **Opis:** Ataki z użyciem techniki NFC Relay nie zdążyły upowszechnić się na terenie Polski.
- **Przykład:** Dotychczas w Polsce zaobserwowano jedno podszycie pod instytucję bankową z wykorzystaniem złośliwej aplikacji korzystającej z ww. techniki[2]. Próbka złośliwego oprogramowania została opublikowana w serwisie VirusTotal. Nie zaobserwowano kampanii dystrybuującej złośliwe oprogramowanie innymi kanałami.

Trendy:

- **Opis:** W miarę upływu czasu można spodziewać się upowszechnienia ww. techniki wśród atakujących ukierunkowanych na rynek polski.
- **Obserwacja:** Zbliżony model ataku, rozbudowany o wątek socjotechniczny oraz wykorzystanie technologii PWA w pierwszej fazie kampanii, obserwowano w 3 kwartale 2024 roku na terenie Czech[3].

➢ *Ocena Skutków*

- **Skutki:** Ataki z wykorzystaniem złośliwego oprogramowania korzystającego z techniki NFC Relay mogą prowadzić do kradzieży wrażliwych danych, utraty zaufania klientów, utraty środków finansowych oraz obniżenia reputacji instytucji finansowych pod które podszywają się atakujący. Koszty związane z atakami obejmują zarówno bezpośrednie straty finansowe, potencjalne straty wizerunkowe jak i koszty związane wdrażaniem środków zapobiegawczych.
- **Przykład:** Atak z wykorzystaniem złośliwego oprogramowania wykorzystującego NFC Relay może prowadzić do kradzieży danych z karty płatniczej klienta, odczytanej przy użyciu interfejsu NFC na zainfekowanym urządzeniu. Atakujący może rozszerzyć model działania o dodatkowy krok, polegający na próbie wyłudzenia kodu PIN do karty płatniczej. Konsekwencją ataku może być próba realizacji płatności zbliżeniowych lub wypłaty środków z bankomatu z wykorzystaniem przejętych danych.

➢ *Podsumowanie*

Złośliwe oprogramowanie korzystające z techniki NFC Relay stanowi noworozpoznane zagrożenie dla sektora finansowego, umożliwiając atakującym kradzież wrażliwych danych odczytywanych za pośrednictwem interfejsu NFC. Zaobserwowana technika może być łączona z innymi metodami atakujących, takimi jak malware PWA, scenariusze socjotechniczne, próby wyłudzenia kodów PIN do kart płatniczych. Wykradzione dane atakujący mogą próbować wykorzystać np. w celu realizacji płatności zbliżeniowych lub wypłaty środków z bankomatów.

[2] https://x.com/CSIRT_KNF/status/1887474108323037617

[3] https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT** , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).