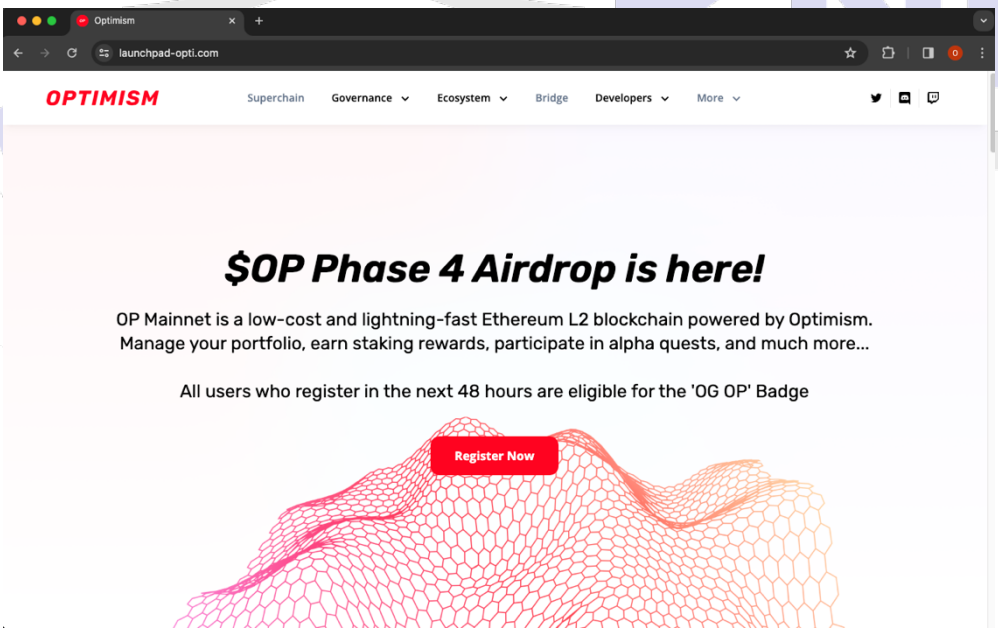
Kryptowaluty za darmo – Przejęcia kont na portalu Twitter/X

W obliczu dynamicznie rozwijającego się świata kryptowalut i technologii blockchain, pojawiła się nowa fala zagrożeń cybernetycznych, które wpływają zarówno na indywidualnych użytkowników, jak i na większe organizacje. Niniejszy raport koncentruje się na szczególnie niepokojącym zjawisku: wykorzystywaniu przejętych kont na Twitterze do fałszywych promocji projektów kryptowalutowych oraz kradzieży portfeli cyfrowych. Ta strategia, stosowana przez cyberprzestępców, wykorzystuje zarówno zaawansowane techniki socjotechniczne, jak i luki w świadomości użytkowników na temat bezpieczeństwa cyfrowego. Przeanalizujemy metody działania oszustów, ich wpływ na ofiary i społeczność kryptowalutową oraz strategie prewencyjne, które mogą być stosowane w celu ochrony przed takimi atakami.

Airdropy, drainery – co to jest?

W świecie kryptowalut, pojęcie 'Airdrop' odnosi się do praktyki dystrybucji tokenów lub monet bezpłatnie do szerokiej społeczności użytkowników, zwykle w celu promocji nowego projektu blockchain. Chociaż airdropy mogą być legalną i powszechną metodą marketingową, stały się one również narzędziem dla cyberprzestępców, którzy wykorzystują je do prowadzenia oszustw znanych jako 'Drainery'. Drainerzy, korzystając z fałszywych stron internetowych imitujących popularne airdropy lub projekty kryptowalutowe, zwabiają ofiary do podłączenia swoich portfeli cyfrowych pod pretekstem udziału w rzekomych airdropach. Celem takich działań jest przejęcie kontroli nad portfelami cyfrowymi i kradzież środków zgromadzonych przez użytkowników. Tym samym, w świecie, gdzie technologie blockchain oferują nowe możliwości, pojawia się równie nowe zagrożenie, które wykorzystuje zaufanie użytkowników.



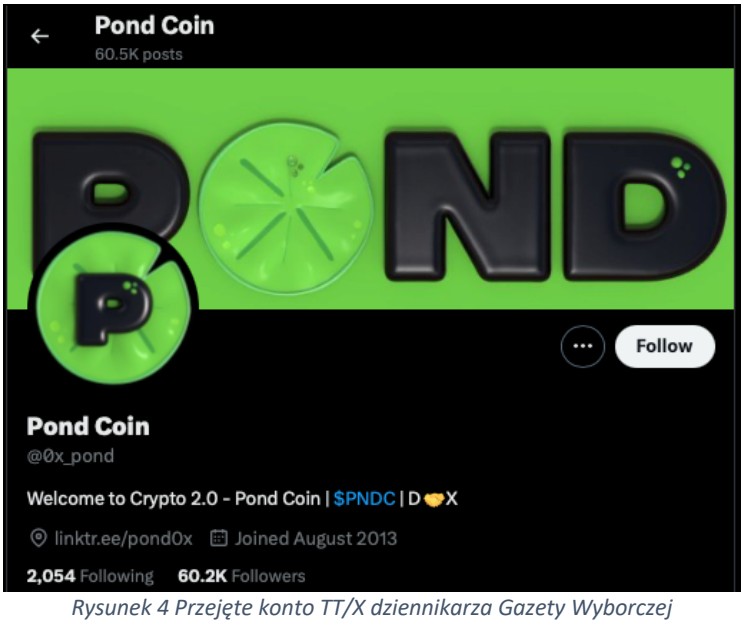
Rysunek 1 Fałszywy Airdrop wykorzystywany w ataku z dnia 12.01.2024: https://x.com/CSIRT_KNF/status/1745752088682865105?s=20

Telewizyjna gwiazda poleca AirDrop?

Przestępcy cyfrowi często przejmują lub tworzą fałszywe profile na Twitterze znanych osobistości, polityków, celebrytów czy wpływowych postaci ze świata kryptowalut. Robią to, by wykorzystać ich reputację i zasięg społecznościowy w celu nadania wiarygodności swoim fałszywym airdropom. Oszuści zdają sobie sprawę, że wiadomości pochodzące od renomowanych źródeł cieszą się większym zaufaniem przez nieświadomych użytkowników. Dzięki temu, fałszywe airdropy i linki do drainerów mogą być skuteczniej rozpowszechniane wśród większej liczby osób, zwiększając potencjalną liczbę ofiar.

Rysunek 2 Przejęte konto TT/X byłego Ministra Spraw Zagranicznych

Rysunek 3 Przejęte konto TT/X firmy Mandiant zajmującej się cyberbezpieczeństwem



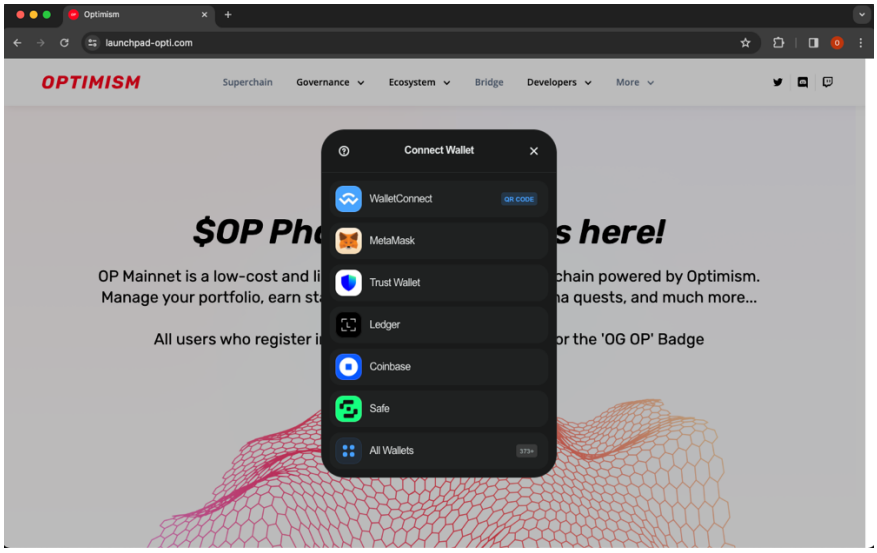
Rysunek 4 Przejęte konto TT/X dziennikarza Gazety Wyborczej

Po skutecznym przejęciu kont na Twitterze, cyberprzestępcy natychmiast przystępują do następnego etapu swojego oszustwa: publikowania fałszywych linków. Te linki prowadzą do stron internetowych, które są starannie zaprojektowane, aby wyglądały jak autentyczne kantory, giełdy czy firmy zajmujące się kryptowalutami. Celem tych stron jest przede wszystkim zachęcenie do transakcji lub podłączenia portfeli kryptowalutowych. Poprzez wykorzystanie dobrze znanego wizerunku i zaufania, które niesie ze sobą przejęte konto, przestępcy zwiększają szanse na skuteczność swoich fałszywych stron. Działają one na zasadzie zmyślonej oferty lub promocji, stwarzając iluzję lukratywnej okazji, która w rzeczywistości prowadzi do kradzieży aktywów cyfrowych i poufnych danych użytkowników.

Rysunek 5 Opublikowany post z fałszywym linkiem

Rysunek 6 Opublikowany post z fałszywym linkiem na koncie @Mandiant.

Drainer – jak działa?

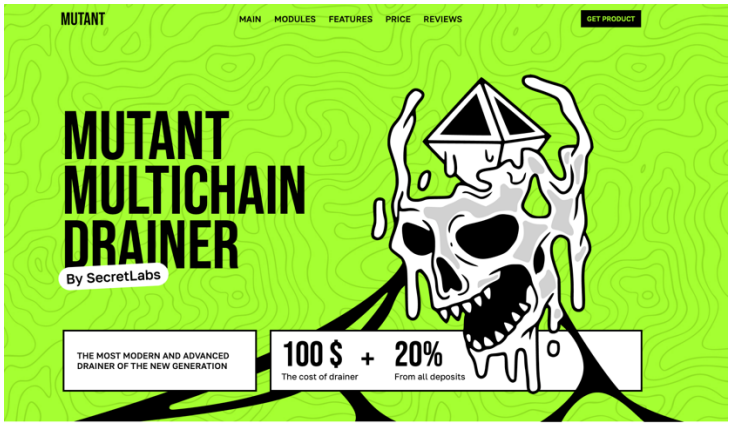


Rysunek 7 Portfele które są obsługiwane przez fałszywą stronę do ich kradzieży.

Oto kilka typowych sposobów działania i dystrybucji drainerów:

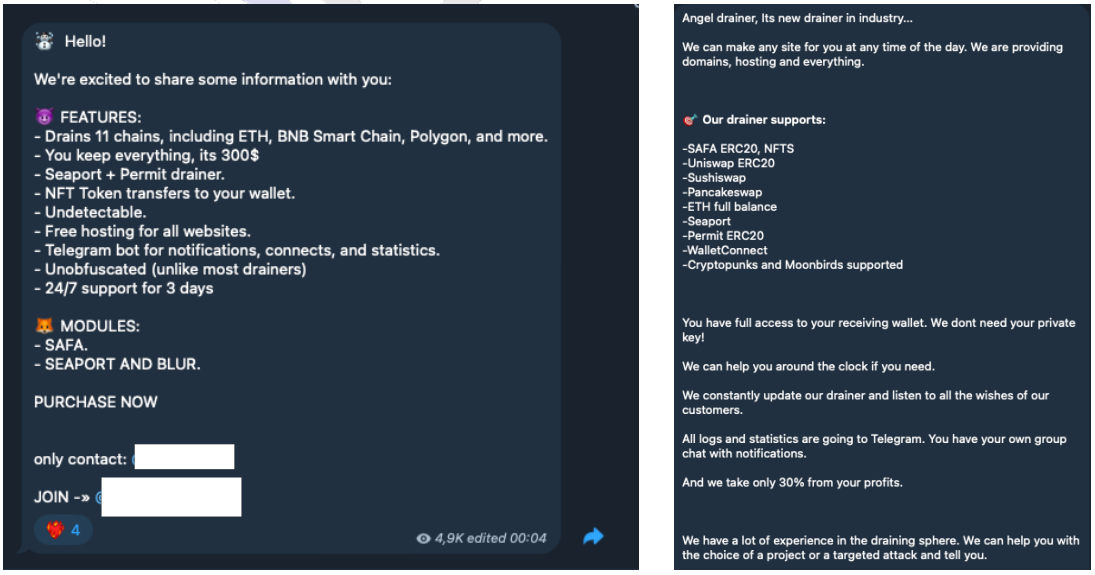
1. **Phishing**: Drainerzy często wysyłają fałszywe wiadomości e-mail, wiadomości tekstowe lub komunikaty na platformach społecznościowych, udając instytucje finansowe, giełdy kryptowalut lub inne wiarygodne źródła. W tych wiadomościach proszą ofiary o podanie swoich danych logowania lub poufnych informacji, co prowadzi do przejęcia konta i kradzieży środków.
2. **Fałszywe portfele i aplikacje**: Drainerzy mogą tworzyć fałszywe portfele kryptowalutowe lub aplikacje do zarządzania portfelami, które wyglądają jak oryginalne. Użytkownicy, którzy pobierają te aplikacje i przekazują swoje klucze prywatne, stają się ofiarami kradzieży.
3. **Socjotechnika**: Drainerzy mogą stosować socjotechnikę, czyli manipulowanie emocjami lub zaufaniem ofiar, aby uzyskać dostęp do ich informacji. Na przykład, mogą tworzyć wiadomości lub profile społecznościowe, które wydają się być zaufane.
4. **Złośliwe oprogramowanie**: Drainerzy mogą używać złośliwego oprogramowania, takiego jak keyloggery lub trojany, które instalują się na komputerach lub urządzeniach użytkowników i rejestrują ich aktywność, w tym klucze prywatne do portfeli kryptowalutowych.
5. **Inżynieria społeczna**: Drainerzy mogą zbierać informacje o swoich ofiarach, na przykład na forach internetowych lub mediach społecznościowych, a następnie wykorzystywać te informacje do personalizowanych ataków.

Kto stoi za kradzieżami?



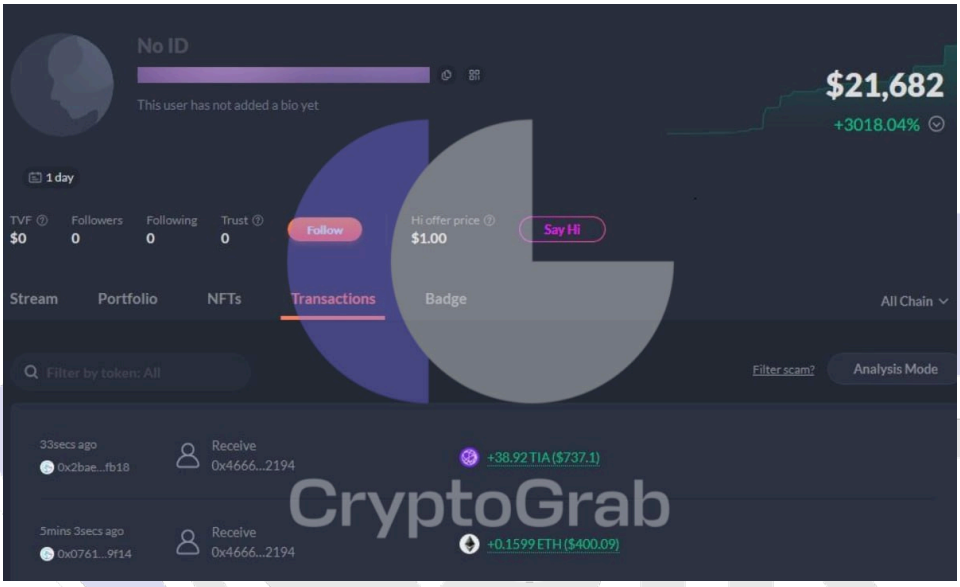
Rysunek 8 Strona z ofertą drainera w modelu DaaS

Przestępcy odpowiedzialni za kradzieże kont w mediach społecznościowych, które docelowo wykorzystywane są do publikacji fałszywych stron z AirDropami, często używają Drainerów w modelu Daas (Drainer as a Service). Wynajmują oni te złośliwe narzędzia wraz z gotowymi modułami do kradzieży portfeli kryptowalutowych, płacąc stałe stawki za korzystanie z usługi lub dzieląc się procentem z ukradzionych środków z dostawcą drainera. Ta praktyka pozwala cyberprzestępcom na skalowanie swoich operacji bez konieczności posiadania zaawansowanej wiedzy technicznej czy infrastruktury – wystarczy tylko przejąć kontrolę nad wiarygodnym kontem i rozpocząć rozsyłanie linków do zaprojektowanych przez siebie pułapek.

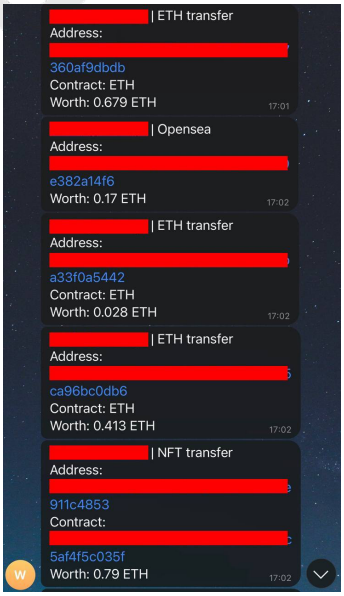


Rysunek 9 Treść oferty grupy, umożliwiającej wynajęcie infrastruktury do kradzieży portfeli kryptowalut.

Przestępcy, pragnąc wykazać skuteczność swoich działań, często dzielą się zrzutami ekranu dokumentującymi ich "sukcesy" na forach i w kanałach dedykowanych recenzjom narzędzi do kradzieży kryptowalut, czyli tzw. drainerów. Takie działanie, choć wydaje się być próżnością, dostarcza nam cennych informacji. Prezentując ekrany z bilansami ukradzionych środków, nieświadomie ujawniają one wielkość strat ponoszonych przez użytkowników portfeli kryptowalutowych każdego dnia. Analiza tych danych pozwala nie tylko oszacować skale problemu, ale również zidentyfikować trendy i potencjalne nowe techniki stosowane przez cyberprzestępców.



Rysunek 10 Dowód zarobków pochodzący od przestępcy używającego narzędzia typu DaaS



Rysunek 11 Dowód zarobków pochodzący od przestępcy używającego narzędzia typu DaaS

W świecie cyfrowym, gdzie nasza obecność online i aktywa wirtualne są ciągle zagrożone przez coraz bardziej wyrafinowane ataki, ochrona naszych kont społecznościowych oraz portfeli kryptowalutowych powinna być traktowana priorytetowo. Zabezpieczenie swojej cyfrowej tożsamości i inwestycji wymaga świadomego podejścia i wdrożenia serii najlepszych praktyk z zakresu cyberbezpieczeństwa. Oto kilka kluczowych kroków, które można podjąć, aby zminimalizować ryzyko nieautoryzowanego dostępu do naszych kont społecznościowych oraz kradzieży środków z portfeli kryptowalutowych.

Ochrona kont społecznościowych:

1. **Silne i unikalne hasła**: Używaj różnych haseł dla każdego konta społecznościowego i upewnij się, że są one skomplikowane.
2. **Weryfikacja dwuetapowa (2FA)**: Zawsze aktywuj weryfikację dwuetapową.
3. **Ostrzeżenia o logowaniu**: Ustaw powiadomienia o nowych logowaniach na swoje konto, abyś mógł szybko reagować na nieautoryzowany dostęp.
4. **Ograniczenie dostępu aplikacji**: Regularnie sprawdzaj i zarządzaj aplikacjami, które mają dostęp do Twoich kont społecznościowych i ograniczaj ich uprawnienia.

Ochrona danych do portfeli kryptowalutowych przed drainerami:

1. **Używaj zaufanych źródeł**: Pobieraj portfele kryptowalutowe wyłącznie z oficjalnych stron lub sklepów aplikacji.
2. **Phishing**: Bądź świadom technik phishingowych i nigdy nie klikaj w podejrzane linki ani nie podawaj swoich kluczy prywatnych online.
3. **Przechowywanie kluczy**: Klucze prywatne do twojego portfela kryptowalutowego przechowuj w bezpiecznym miejscu, najlepiej na sprzętowym portfelu (tzw. hardware wallet) lub w bezpiecznym menedżerze haseł.
4. **Unikaj nieznanych airdropów**: Bądź sceptycznie nastawiony do ofert airdropów, które wymagają podłączenia portfela lub wprowadzenia kluczy.
5. **Aktualizacje oprogramowania**: Regularnie aktualizuj oprogramowanie portfela, aby mieć najnowsze zabezpieczenia.
6. **Uważaj na socjotechnikę**: Nie daj się zwieść wiadomościom alarmującym lub "pilnym" prośbom, które mogą być próbą wyłudzenia danych.
7. **Wykorzystanie wielu podpisów (multisig)**: Jeśli to możliwe, skonfiguruj portfel kryptowalutowy, aby wymagał wielu podpisów do autoryzacji transakcji.
8. **Backup**: Utwórz bezpieczne kopie zapasowe swojego portfela, aby w przypadku ataku móc przywrócić dostęp do środków.
9. **Regularne audyty bezpieczeństwa**: Przeprowadzaj regularne audyty bezpieczeństwa swoich systemów i procedur związanych z kryptowalutami.