Inżynieria społeczna i złośliwe oprogramowanie jako bardzo skuteczna mieszanka ataku.

Bankowe Trojany – to, co się dzieje teraz i to, co nadchodzi.
Jak walczyć z oszustwami za pomocą rozwiązań opartych na danych i sztucznej inteligencji?

Marta Łąpieś, Regional Sales Director, Cleafy

Cleafy

Złośliwe oprogramowanie nie należy do przeszłości.

Jest to część coraz bardziej dynamicznie zmieniającej się przyszłości.

All rights reserved - Cleafy ©2024

All rights reserved - Cleafy ©2024

All rights reserved - Cleafy ©2024

Dane liczbowe

W 2023 r. naruszono bezpieczeństwo 1103 aplikacji bankowych (60% zaatakowanych).

Według liczby zaatakowanych banków, najczęściej używanymi złośliwymi programami były: **Hook, Godfather and Teabot.**

Według kraju (liczba atakowanych aplikacji):

US	UK	Turkey	Spain
109 apps	48 apps	109 apps	48 apps

Trendy w 2023:

ATS
Automatic transfer system

TOAD
Telephone based Attack Delivery

RAT
Screen sharing abuse

Sources:Zimperium's 2023 Mobile Banking Heists Report

All rights reserved - Cleafy ©2024

Co to takiego?

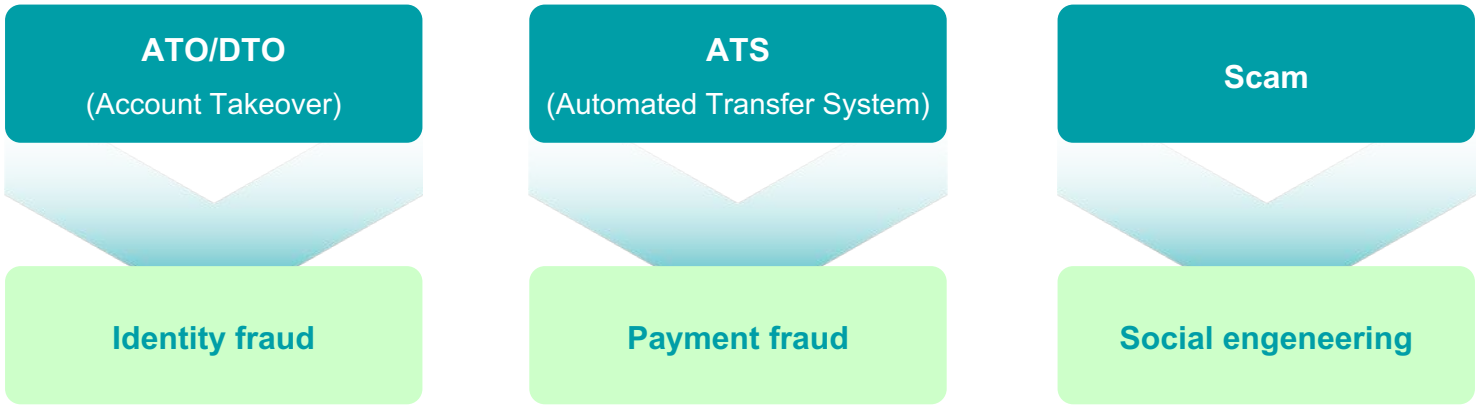
Pozornie legalne aplikacje zawierające złośliwe oprogramowanie.

Stanowią środek do atakowania użytkownika końcowego.

Mogą być aktualizowane zdalnie, a nawet mają taktykę pozwalającą uniknąć wykrycia przez program antywirusowy.

All rights reserved - Cleafy ©2024

Trzy rodzaje ataków dla trzech rodzajów transakcji oszukańczych



All rights reserved - Cleafy ©2024

Złośliwe oprogramowanie jako usługa / Malware as a service

- Ułatwia dostęp do złośliwego oprogramowania, nie trzeba umieć programować.
- Ostatnio ten, kto tworzy złośliwe oprogramowanie, nie wykorzystuje go. Dwa różne modele biznesowe.
- Można go kupić lub subskrybować za pośrednictwem dark net'u.
- Zestawy do wyłudzania informacji - Phishing kits.
- Narzędzia dowodzenia i kontroli, które pozwalają zarządzać różnymi możliwościami wspomnianego złośliwego oprogramowania:
    - Dystrybucja;
    - Aktualizacja funkcjonalności;
    - Aktywowanie ich

All rights reserved - Cleafy ©2024

Narzędzia

Wykorzystują zaawansowane narzędzia do zarządzania i przeprowadzania ataków:

- Złośliwe oprogramowanie o różnych możliwościach i ukierunkowane na różne oszustwa.
- Dowodzenie i kontrola kampanii phishingowej.
- Zestawy do wyłudzania informacji - Phishing kits.
- Lokalni operatorzy.
- Szkolenia dla operatorów.
- Podszywanie się pod numery telefonów instytucji finansowych.
- Kanały dystrybucji: e-mail, SMS, Whatsapp, a nawet oficjalne sklepy z aplikacjami.
    - Dostępne dla Androida.
    - Apple już wkrótce z nową funkcją sideload.

All rights reserved - Cleafy ©2024

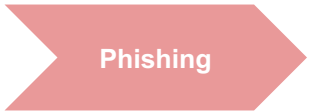
Kampanie: W jaki sposób atakują?

- Kampanie złośliwego oprogramowania działają bardzo szybko i koncentrują się tam, gdzie istnieje luka w zabezpieczeniach.
- Faza dystrybucji, faza walidacji i faza działania.
- Łączą one różne narzędzia i metody w celu zwiększenia skuteczności i wydajności.

All rights reserved - Cleafy ©2024

Kampanie: Faza rozpoznania i przygotowania

- Oszuści pozyskują bazy danych na różne sposoby, w tym kupując je w dark necie.
- Segmentują bazę danych, aby skupić się na konkretnych klientach określonych podmiotów.
- Zarządzają kampaniami phishingowymi, segmentując je według instytucji finansowych.



All rights reserved - Cleafy ©2024

Kampanie: Faza dystrybucji i instalacji

1. Odnoszą się do klientów instytucji finansowych jak do leadów o różnych statusach.
2. Wykorzystują lokalnych operatorów do przeprowadzania ataków socjotechnicznych:
    - Podszywają się pod oficjalne numery telefonów tych podmiotów (spoofing)
    - Personalizują wiadomości i przeprowadzają ataki podzielone na segmenty.
    - Dzwonią do klientów końcowych ze sprawa, która wywołuje poczucie pilności.
        - Aplikacje, które zwiększą bezpieczeństwo użytkowników jako uzupełnienie oficjalnej aplikacji banku.
        - Nowe aplikacje, które zastępują te już przestarzałe.
        - Rozszerzenie funkcji telefonu (i.e. 5G), etc.
    - Używają oni zestawów phishingowych do generowania złośliwych aplikacji dostosowanych do podmiotu, który zamierzają zaatakować.
3. Istnieją złośliwe oprogramowanie wyspecjalizowane w określonych podmiotach finansowych.
4. Nakłaniają do dobrowolnego pobrania i zainstalowania złośliwego oprogramowania bankowego.

All rights reserved - Cleafy ©2024

Kampanie: Faza walidacji i realizacji

Kampania obejmuje wstępną fazę walidacji i udoskonalania:

- Weryfikują one stan bezpieczeństwa instytucji finansowej na różnych poziomach (zachowania transakcyjne, behawioralne, biometryczne itp.).
- Systematycznie sprawdzają niewielką liczbę użytkowników, dopóki nie znajdą wektora ataku.
- Wykonują iteracje, aby lepiej wykorzystać luki w zabezpieczeniach

Realizacja:

- Wcześniej potwierdzili skuteczność swojego ataku i przygotowują się do jego eskalacji.
- Szybko przeprowadzają atak.
- Mają zdolność do adaptacji w czasie rzeczywistym, aby kontynuować atak tak długo, jak to możliwe.

All rights reserved - Cleafy ©2024

Prawdziwe przypadki

Chociaż może się wydawać, że złośliwe oprogramowanie nigdy nas nie zaatakuje i nie ma wpływu, jest to medium, które nigdy nie znika i stale ewoluuje:

SharkBot	ATS
PixPirate	ATS and comm. intersection
TeaBot	OFD/ATO and comm. intersection
SpyNote	RAT/ATO
Copybara	Poznajmy szczegóły

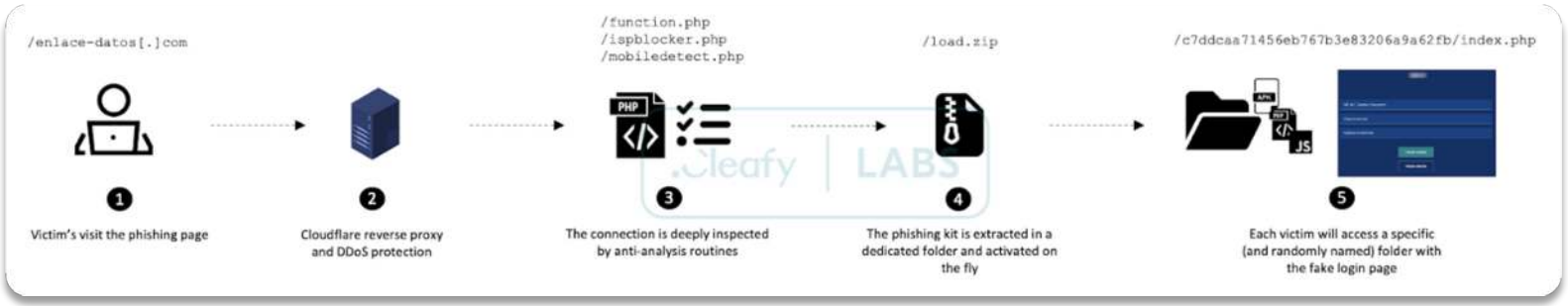
All rights reserved - Cleafy ©2024

Copybara: dowództwo i kontrola (c2)

Oszuści dostarczają te narzędzia z technologią unikania, aby uniknąć wykrycia nowych domen do phishingu.

Zazwyczaj mają różne techniki uniemożliwiające wykrycie, między innymi:

- Kontrola geofencingu
- Device fingerprinting
- Czarna lista określonych ASN i/lub zakresów sieci
- Korzystanie z legalnych usług, ocmo CDN i reverse-proxy, w celu zamaskowania lokalizacji serwera WWW.
- Dynamiczne generowanie zawartości



All rights reserved - Cleafy ©2024

Copybara: dowództwo i kontrola (c2)

All rights reserved - Cleafy ©2024

Copybara: dowództwo i kontrola (c2)

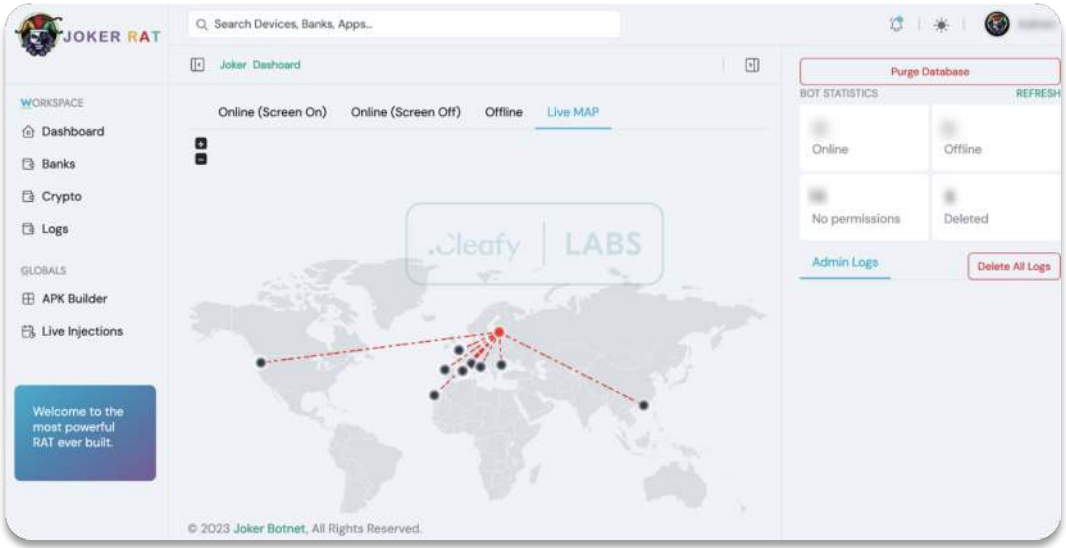
- Segmentacja użytkowników
- mapa w czasie rzeczywistym
- Informacje o urządzeniu
- Malware update

Dodatkowe działania

- Cichy łącznik (Silent Connect)
- (wyświetlanie i manipulowanie ekranem urządzenia)
- Wstrzyknięcie nakładki strony

Zdolności:

- Podsłuchiwanie wiadomości SMS - SMS sniffing
- Overlay
- Keylogging
- Przekierowywanie ruchu
- Fałszywe powiadomienia
- APK Builder



All rights reserved - Cleafy ©2024

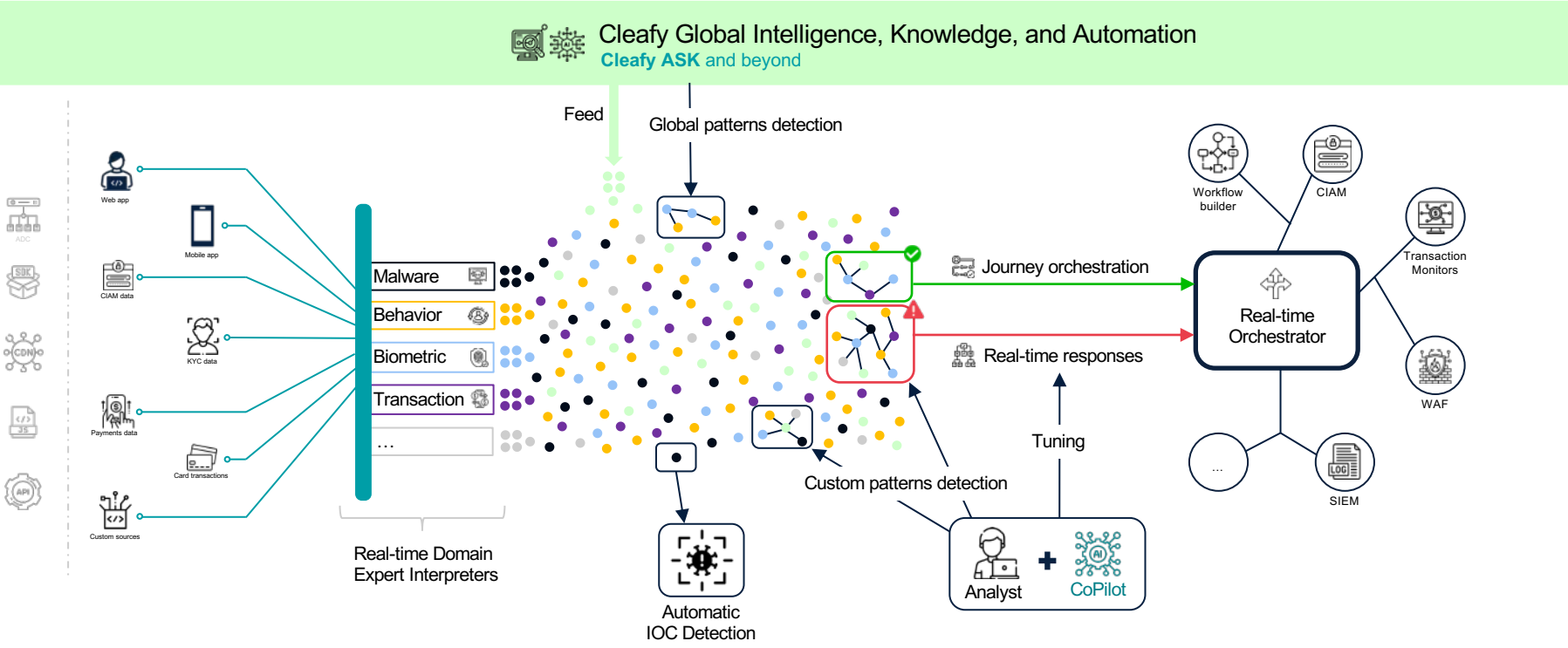
Wnioski

- Złośliwe oprogramowanie powinno być priorytetem dla zespołów bezpieczeństwa:
    - Każdego dnia z biegiem czasu dostęp do złośliwego oprogramowania i korzystanie z niego jest coraz łatwiejsze.
    - coraz łatwiejsze do wykonania, zaprogramowania → Narzędzia, które ułatwiają projektowanie, zarządzanie i wykonanie.
    - Łatwa skalowalność, szybkość i możliwość iteracji.
- Istotne jest, aby przyjąć proaktywną rolę przeciwko oszustwom i mieć wgląd w to, co się dzieje w czasie rzeczywistym.
- Naucz użytkowników, aby unikali phishingu, pobierania aplikacji z nieznanych witryn, a nawet udzielania uprawnień aplikacjom pobranym z oficjalnego rynku bez ich weryfikacji.
- Nie wystarczy być przygotowanym na złośliwe oprogramowanie, trzeba być przygotowanym na złośliwe oprogramowanie typu zero-day:
    - Złośliwe oprogramowanie stale ewoluuje, znacznie szybciej niż rozwiązania dostępne dla FI.
    - Zestawy phishingowe umożliwiają zmianę nazw aplikacji, pakietów i podpisów w ciągu kilku sekund.
    - Bazy sygnatur złośliwego oprogramowania są zawsze w tyle i wymagają potwierdzonego przypadku oszustwa aby zadziałać.

All rights reserved - Cleafy ©2024

Cleafy VISION

The full picture



All rights reserved - Cleafy ©2024

cleafy.com