www.4sync.pl
sales@4sync.pl tel.:22 299 17 00

KARTA DANYCH TECHNICZNYCH

Fidelis Deception™

Duży wybór wabików — od maszyn VM z prawdziwym OS po maszyny z emulacją: sposób na precyzję alertów

Okazja

Cyberprzestępcy poszukują haseł i danych logowania użytkowników, aby uzyskiwać dostęp do sieci oraz aplikacji, a następnie monitorować i wykradać dane. Z obserwacji konkursów typu „zdobądź flagę" wynika, że w poszukiwaniu danych logowania włamywacze analizują pocztę e-mail, pliki, dokumenty i nieustrukturyzowane informacje, podczas gdy zautomatyzowane złośliwe oprogramowanie koncentruje się na ustrukturyzowanych danych w przeglądarkach internetowych i aplikacjach. Dla włamywaczy najważniejsze są dane logowania, które umożliwiają przedostawanie się do sieci i podejmowanie działań rozpoznawczo-szpiegujących. Każdy udany krok pomaga włamywaczom lub złośliwym osobom z wewnątrz działać po cichu, bez powodowania cyfrowego „hałasu", który mógłby zdradzić ich poczynania. *Wiedząc, na czym zależy włamywaczom, można stworzyć system obrony dezinformacyjnej złożony z „okruszków chleba" i wabików, który pełni funkcje przynęty, detekcji i ochrony.*

Wyzwanie

- Wykrywanie włamywaczy, złośliwych użytkowników z wewnątrz oraz złośliwego oprogramowania w sieciach i chmurach
- Wysyłanie precyzyjnych alertów z minimalną liczbą fałszywych alarmów
- Automatyzacja zadań z zakresu analiz śledczych i reagowania
- Poprawa efektywności i wydajności pracy analityków bezpieczeństwa
- Poznawanie technik, taktyk i procedur hakerów w celu doskonalenia zabezpieczeń

Rozwiązanie

- Utworzenie rozmaitych wabików i „okruszków chleba" w środowisku lokalnym lub w chmurze
- Wdrożenie wabików z prawdziwym systemem operacyjnym lub emulacji usług i systemów operacyjnym, w tym firmowych urządzeń IoT
- Wabiki z działającymi aplikacjami i usługami, które angażują cyberprzestępców i zajmują im czas
- Wykrywanie na podstawie analiz dostępu do wabików, danych logowania usługi AD, skażonych danych i ruchu
- Brak zagrożeń dla zasobów i danych oraz negatywnego wpływu na użytkowników bądź działalność operacyjną

Rozpoznawanie

- Stałe mapowanie sieci, chmury i zasobów
- Tworzenie i aktualizacja profili pod kątem lokalizacji zasobów, ich wykorzystania, typu itp.
- **Wyniki:** automatyczne opanowanie technik tworzenia realistycznych warstw dezinformacji

Wabiki

- Automatyczne tworzenie dezinformujących wabików na podstawie rozpoznania
- Dezinformacja oparta na różnorodnych wabikach
- **Wyniki:** przekonujące wabiki z prawdziwym systemem operacyjnym

Dystrybucja

- Automatyczne wdrażanie wabików w sieciach i chmurach
- Osadzanie „okruszków chleba" w rzeczywistych zasobach i Active Directory
- **Wyniki:** szybkie wdrożenie i błyskawiczna skuteczność

Wykrywanie

- Alerty o dostępie do wabików i związanej z nimi aktywności
- Analizy i alerty dotyczące wykorzystania skażonych danych
- **Wyniki:** precyzyjne alerty z minimalną liczbą fałszywych alarmów

Adaptacja

- Rozpoznawanie nowych zasobów oraz topologii sieci i chmury
- Automatyczne aktualizacje map rozpoznania i wabików
- **Wyniki:** inteligentny i aktywny system obrony dezinformacyjnej

„Rozwiązanie Fidelis do dezinformacji cyberprzestępców okazało się bardzo skuteczne. Wabiki umożliwiły doskonałe wykrywanie anomalii bez analizowania tak wielu danych jak w przypadku innych technik".

Weston Nicolls, starszy wiceprezes, menedżer ds. bezpieczeństwa informacji, First Midwest Bank

Jak działa dezinformacja

Dezinformacja działa deterministycznie za sprawą „okruszków chleba" rozmieszczanych na prawdziwych zasobach w celu doprowadzenia włamywaczy, złośliwych osób z wewnątrz i automatycznie działającego złośliwego oprogramowania do wabików. Dzięki dezinformacji można wyprowadzić cyberprzestępców w pole. Zamiast nadaremnie poszukiwać włamywaczy w oceanie dobrych danych, mechanizmy dezinformacyjne wysyłają przydatne w praktyce alerty i zdarzenia generowane na podstawie analiz dostępu do wabików, danych logowania usługi AD, skażonych danych oraz ruchu. Alerty te są wyjątkowo precyzyjne i rzadko stanowią fałszywe alarmy. Mechanizmy dezinformacyjne w środowisku lokalnym i chmurze oraz świeże dane o aktywności tworzą przekonujące warstwy dezinformacji, które obejmują urządzenia, dane i zachowania mające wyprowadzać cyberprzestępców w pole. Łapiąc przynętę, włamywacze trafiają do wabików, co umożliwia ich wykrycie oraz ochronę danych.

Profile wabików

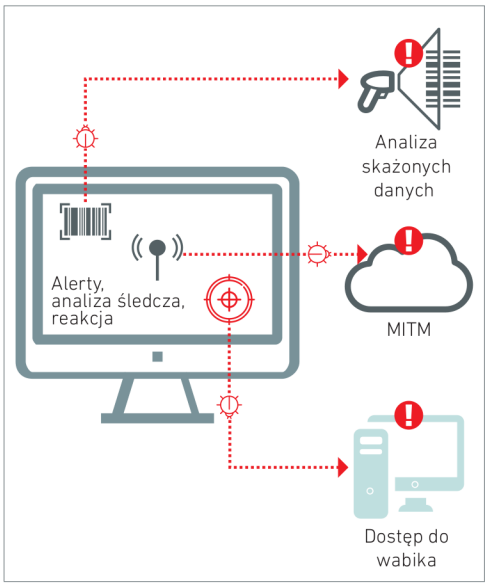
- Sprzęt — laptopy, serwery, routery, przełączniki, kamery, drukarki, urządzenia IoT itp.
- Oprogramowanie — systemy operacyjne, porty, usługi, aplikacje, zasoby w chmurze i podobne dane
- Wabiki są zasobami nieznanymi i ukrytymi, aby pracownicy nie mieli powodu uzyskiwać do nich dostępu
- Wysoce interaktywne wabiki zajmują czas włamywaczom i odwracają uwagę od rzeczywistych zasobów

Profile „okruszków chleba" i pułapek

- Pułapki: z wykorzystaniem plików, aplikacji, sieci lub danych logowania
- „Okruszki chleba": pliki, dokumenty, e-maile, zasoby systemowe itp.
- Skażone dane, dane logowania i profile używane przez włamywaczy

Wykrywanie ataków po włamaniu

- Dostęp do wabików jako nieznanych zasobów (np. ze strony włamywaczy zewnętrznych i wewnętrznych)
- Analiza przedstawiająca wykorzystanie skażonych danych (np. danych logowania)
- Monitorowanie działań włamywaczy podejmowanych wobec wabików i „okruszków chleba"
- Analiza ruchu w sieci związanego z wabikami oraz alerty dotyczące dostępu do danych



Precyzyjne alerty z minimalną liczbą fałszywych alarmów — lokalne lub w chmurze

Aktywna dezinformacja

- Automatyzuje i dostosowuje wdrożenie wabików oraz „okruszków chleba"
- Wykrywa działania związane z rekonesansem i przenikaniem do sieci, komunikacją C&C oraz przygotowywaniem danych do wyprowadzenia na zewnątrz
- Zapewnia wgląd w informacje i dane śledcze umożliwiające poznanie taktyk, technik, procedur i poszukiwanych zasobów
- Udostępnia jedną konsolę z pełnymi danymi telemetrycznymi umożliwiającymi analizę i tropienie zagrożeń oraz podejmowanie działań
- Brak negatywnego wpływu na działalność operacyjną i użytkowników oraz zagrożeń dla danych i zasobów

Dlaczego warto wybrać rozwiązanie Fidelis?

- ✓ Profilowanie i klasyfikacja zasobów w celu ustalenia warstw dezinformacji
- ✓ Pełna automatyzacja wabików, obejmująca adaptację i świeżość danych
- ✓ Wabiki w postaci maszyn VM z prawdziwym systemem operacyjnym, wabiki oparte na złotych obrazach OS lub inne wybrane przez klienta
- ✓ Wabiki z emulacją do interakcji i przesyłania plików z niskim poziomem ryzyka
- ✓ Wabiki w formie firmowej infrastruktury IoT oraz ładowanie stron WWW do wabików HTTP
- ✓ Wysyłanie przesłanych plików do środowiska sandboxingu Fidelis w chmurze
- ✓ Obraz drogi włamywacza i zabezpieczeń uzyskiwany dzięki bardzo szybkim sensorom
- ✓ Spoofing adresów MAC wabików w celu wzmocnienia wrażenia autentyczności
- ✓ Płynna współpraca z Fidelis Network i Endpoint
- ✓ Zgodność ze standardem FIPS 140-2

Aby dowiedzieć się więcej, skontaktuj się z nami

Fidelis Cybersecurity | 800 652 4020 | info@fidelissecurity.com

Fidelis Cybersecurity jest czołowym dostawcą rozwiązań do wykrywania i tropienia zagrożeń oraz reagowania na nie. Fidelis zwalcza całą gamę cyberprzestępstw, w tym kradzież danych i szpiegostwo, zapewniając pełny obraz środowisk hybrydowych z infrastrukturą chmurową i lokalną, automatyzując wykrywanie zagrożeń i kradzieży danych, wspomagając tropienie zagrożeń i optymalizując reakcje na incydenty dzięki kontekstom, szybkości i dokładności. Rozwiązania Fidelis są używane jako ostatnia linia obrony przez wiele firm z grupy Global 1000 oraz władz państwowych. Zapraszamy na wspólne łowy. Więcej informacji: www.fidelissecurity.com.

