KELA
CYBERWYWAID W DARKNET

Tomasz Goraziński

KELA

NETFORMERS

Cyberwywiad w DarkNet

Od wycieku dostępów sieciowych do ataku Ransomware

KELA

Agenda:

- Ekosystem cyberprzestępczości
- Wycieki dostępów sieciowych
- Czy da się połączyć atak z wyciekiem dostępów?
- Przykłady ...
- CTI - Proaktywna ochrona organizacji

KELA

Ekosystem cyberprzestępczości

Ekosystem cyberprzestępczości

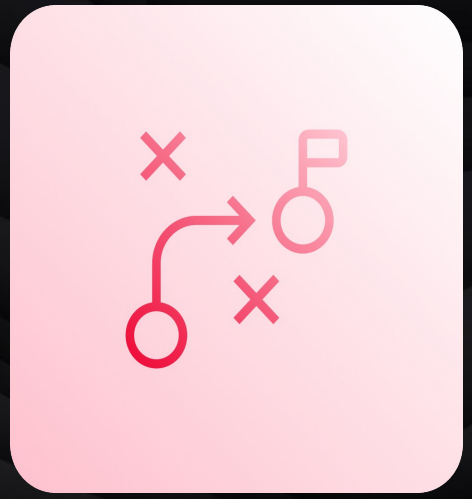
Chaotyczne podziemie pełne zagrożeń

KELA

Motywacja cyberprzestępców

WIZERUNKOWA

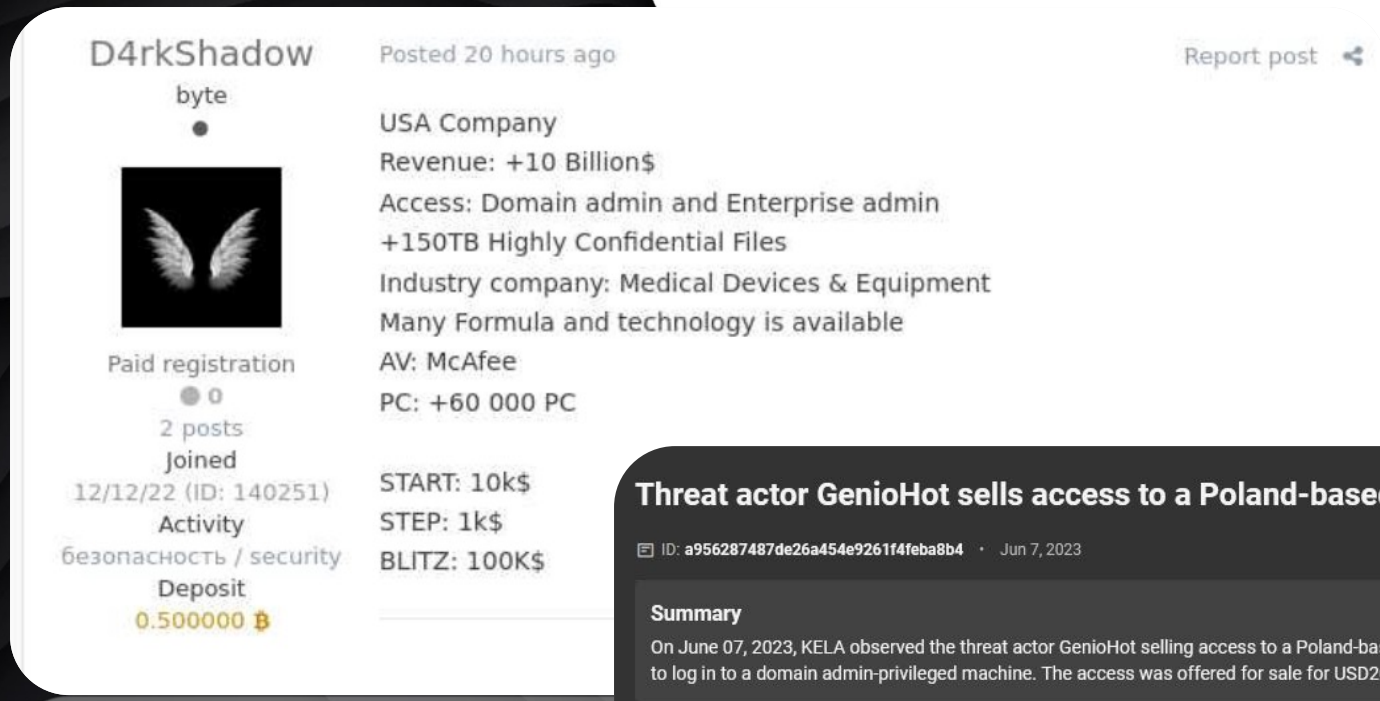
FINANSOWA



TECHNOLOGICZNA

KELA

Wycieki dostępów sieciowych



Threat actor GenioHot sells access to a Poland-based company from the consumer & retail sector

ID: **a956287487de26a454e9261f4feba8b4** • Jun 7, 2023

Summary

On June 07, 2023, KELA observed the threat actor GenioHot selling access to a Poland-based company from the consumer & retail sector, with USD118 million in revenue. The actor claimed the access enables to log in to a domain admin-privileged machine. The access was offered for sale for USD2000.

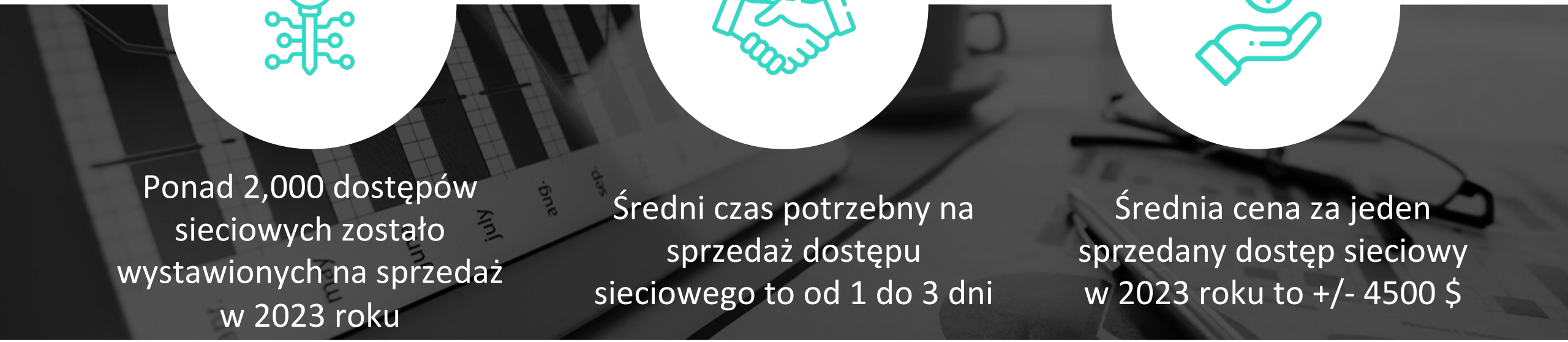
Details

TLP	**Green**
Category	**Network Access**
Sector	**Consumer & Retail**
Geography	**Poland**
Threat Actors	**GenioHot**
Internal References	**[Sell] Company Accesses**

KELA

Wycieki dostępów sieciowych

KELA 24/h na dobę, w sposób automatyczny, monitoruje dostępy sieciowe wystawione na sprzedaż



Ponad 2,000 dostępów sieciowych zostało wystawionych na sprzedaż w 2023 roku

Średni czas potrzebny na sprzedaż dostępu sieciowego to od 1 do 3 dni

Średnia cena za jeden sprzedany dostęp sieciowy w 2023 roku to +/- 4500 $

KELA

Brokerzy inicjalnych dostępów sieciowych

Threat actor yesdaddy sells access to a Romania-based electronics manufacturer

On June 16, 2023, KELA observed the threat actor yesdaddy selling access to a Romania-based electronics manufacturer, with USD35 million in re venue. The actor claimed the access is provided through VPN-RDP and enables to log in to a domain admin-privileged machine. The access was ...

Green Event Network Access Romania Manufacturing & Industrial Products • Jun 16, 2023

Threat actor GenioHot sells access to a Poland-based company from the consumer & retail sector

On June 07, 2023, KELA observed the threat actor GenioHot selling access to a Poland-based company from the consumer & retail sector, with US D118 million in revenue. The actor claimed the access enables to log in to a domain admin-privileged machine. The access was offered for sale f...

Green Event Network Access Poland Consumer & Retail • Jun 7, 2023

Threat actor sganarelle sells access to a Slovakia-based company

On June 01, 2023, KELA observed the threat actor sganarelle selling access to a Slovakia-based company, r claimed the access is provided through Citrix. The access was offered for sale for USD500.

Green Event Network Access Slovakia • Jun 1, 2023

Threat actor tsyko sells access to a Bulgaria-based security school

On May 26, 2023, KELA observed the threat actor tsyko selling access to a Bulgaria-based security school ed through VM and enables to log in to a local admin-privileged machine.

Green Event Network Access Bulgaria Education • May 26, 2023

Threat actor GridsNetwork sells access to a Poland-based company

On May 18, 2023, KELA observed the threat actor GridsNetwork selling access to a Poland-based company, with USD5 million in revenue. The acto r claimed the access is provided through RCE and enables to log in to a root-privileged machine. The access was offered for sale for USD500.

Green Event Network Access Poland • May 18, 2023

Threat actor GenioHot sells access to a Poland-based company from the consumer & retail sector

ID: a956287487de26a454e9261f4feba8b4 • Jun 7, 2023

Summary

On June 07, 2023, KELA observed the threat actor GenioHot selling access to a Poland-based company from the consumer & retail sector, with USD118 million in revenue. The actor claimed the access enables to log in to a domain admin-privileged machine. The access was offered for sale for USD2000.

Details

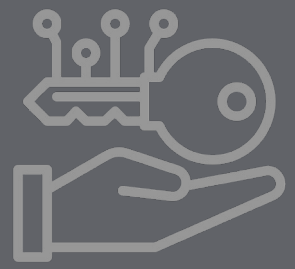
TLP	Green
Category	Network Access
Sector	Consumer & Retail
Geography	Poland
Threat Actors	GenioHot
Internal References	[Sell] Company Accesses

Brokerzy inicjalnych dostępów sieciowych

KELA zidentyfikowała

2,000+

dostępów sieciowych wystawionych na sprzedaż w 2023 roku



Brokerzy inicjalnych dostępów sieciowych, to kluczowy element funkcjonowania usług RaaS

KELA zidentyfikowała

+4,700

ofiar ataków Ransomware oraz prób wymuszenia okupu, co stanowi

66%

wzrost w stosunku do roku 2022

Czy da się połączyć atak Ransomware z wyciekiem dostępów sieciowych?

Wyzwanie…

- Brokerzy inicjalnych dostępów sieciowych nie podają nazw zaatakowanych organizacji, których dostępy wystawiają na sprzedaż

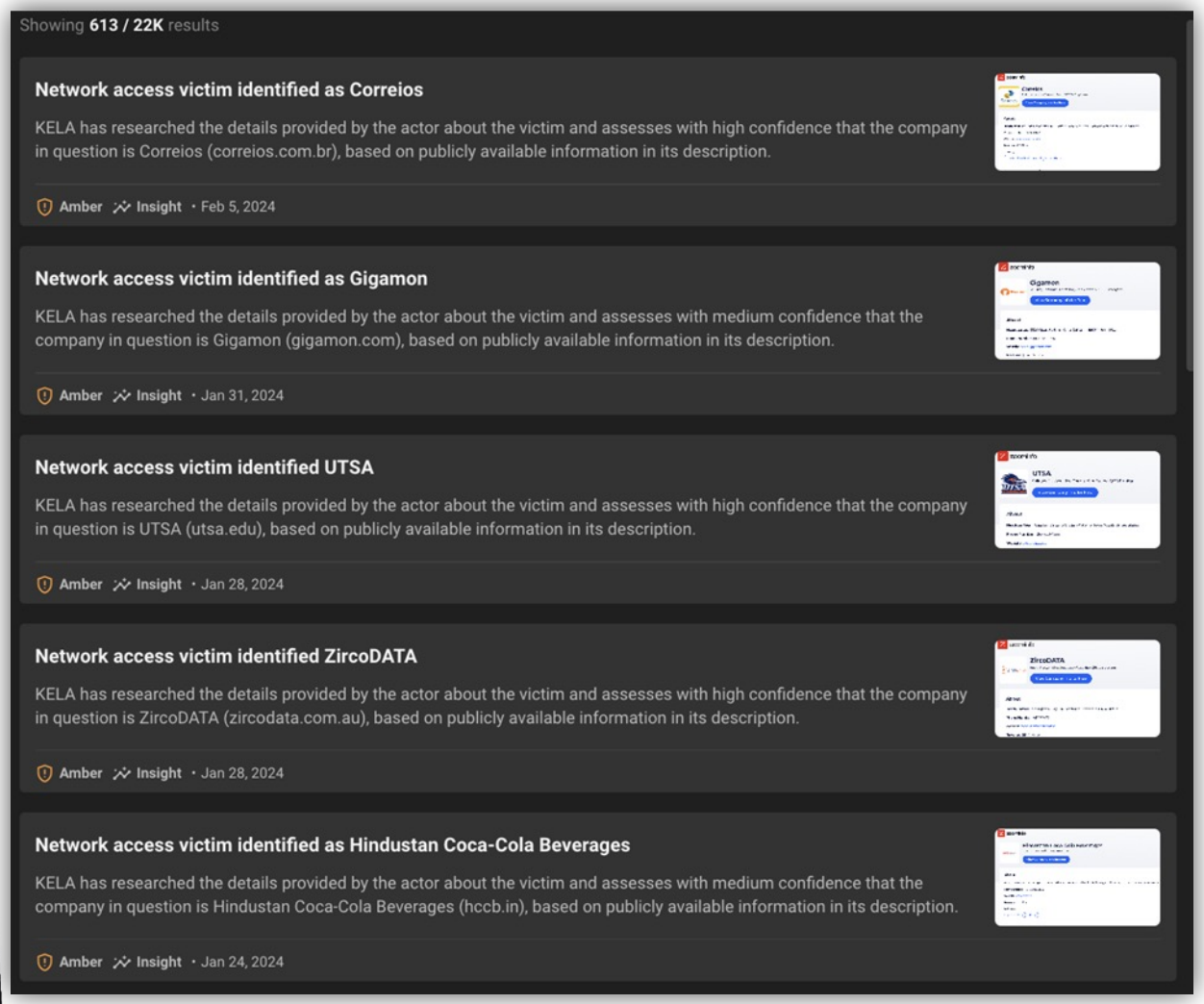
- Zamiast tego wymieniają właściwości lub metryki ofiar tj.:

Przychody, wielkość, branżę, sektor, opis działalności…

KELA

Metryki pomagają innym aktorom ekosystemu cyberprzestępców zrozumieć, czy ofiara jest wartościowa…

Na szczęście pomagają również klientom KELA ...



KELA

Identyfikacja...

D4rkShadow

byte

Paid registration

0

2 posts

Joined

12/12/22 (ID: 140251)

Activity

безопасность / security

Deposit

0.500000 ₿

Posted 20 hours ago

Report post

USA Company
Revenue: +10 Billion$
Access: Domain admin and Enterprise admin
+150TB Highly Confidential Files
Industry company: Medical Devices & Equipment
Many Formula and technology is available
AV: McAfee
PC: +60 000 PC

START: 10k$
STEP: 1k$
BLITZ: 100K$

Network access victim identified as Henry Schein Canada

Jan 23, 2023

KELA has researched the details provided by the actor about the victim and assesses with medium confidence that the company in question is Henry Schein Canada (henryschein.ca), based on the mentioning of the company by the actor on the post. Although the company's domain and name refer to Canada, this is a US company with headquarters in New York.

TLP: **Amber**

KELA

Powiązanie wycieków dostępów sieciowych z atakami

Jedynie w 2023 roku, co najmniej 4 operatorów Ransomware korzystało z zakupionych dostępów sieciowych!

1. **Akira**
2. **Alphv**
3. **Mallox**
4. **Knight (wcześniej Cyclops)**

We take access to mining at %

Publish date: **May 14, 2023** Author: **ransom** in Source: **RAMPForumResurrections** ID: **303544998**

We are interested in US, UK, CA companies (we will consider other options if the field of activity is interesting), we hire from 100kk to 3kkk.
We have the best advertisers, ready to work on stream.
TOX: 3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB08A2099A7F946664BBA2B0D30BFC

We are looking for an access provider. Cooperation\Implementation.

Publish date: **Sep 9, 2023** Author: **Mallx** in Source: **RAMPForumResurrections** ID: **310099985**

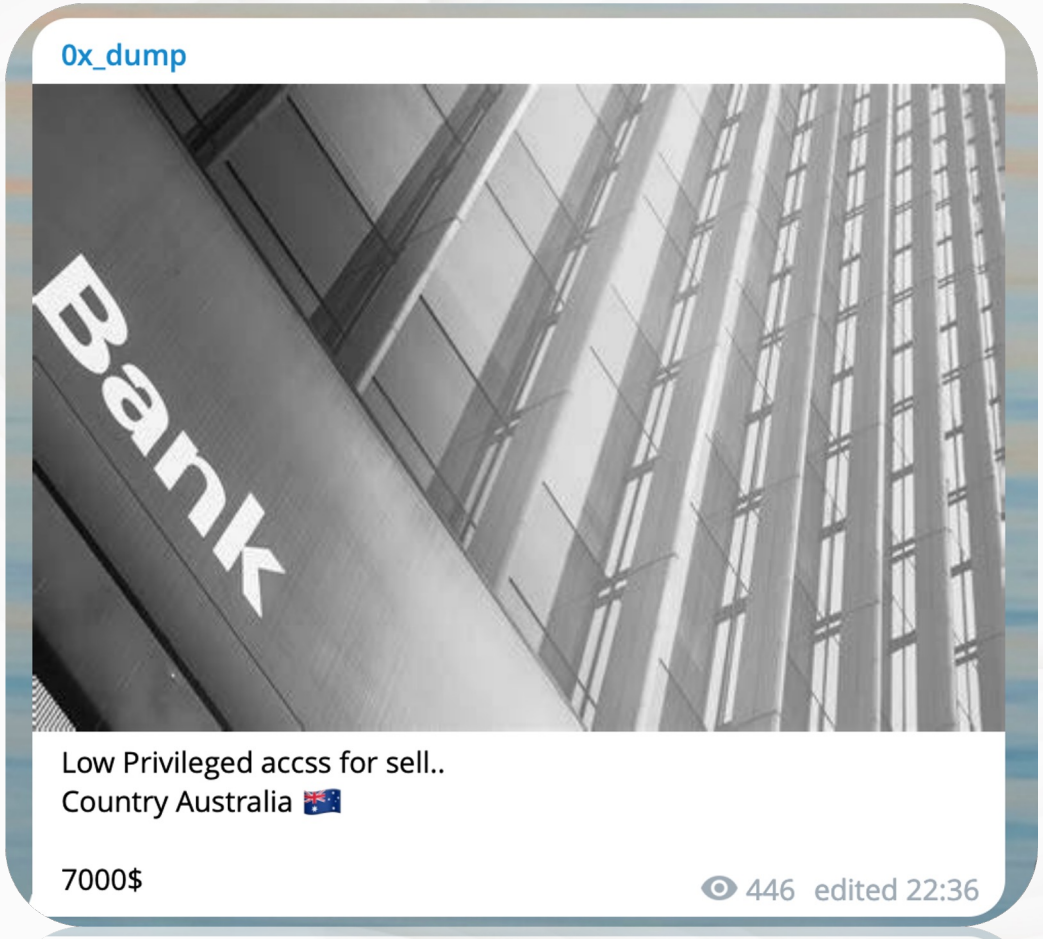
We will take away access for implementation. The terms of fellowship are negotiated personally.
- Interested in access: fortiki, Cisco VPN and others.
- Revenue от 10kk+
- User in the domain.
- AD.
- Geo US/CA/AU/UK/DE.
- Not interested: EDU/GOV
- The topic is considered individually; hospitals and educational institutions are not interested.
- We work honestly and clearly, the supplier will have access to the panel and chats and see everything with his own eyes.
- If there is a constant flow of TOP swearing, we are ready to provide you with the best conditions and take you private.

Jabber contacts: mall0@exploit.im

Przykłady ataków Ransomware opartych o wycieki dostępów sieciowych

Atak Ransomware grupy REvil na Medibank

Wystawienie dostępu sieciowego na sprzedaż

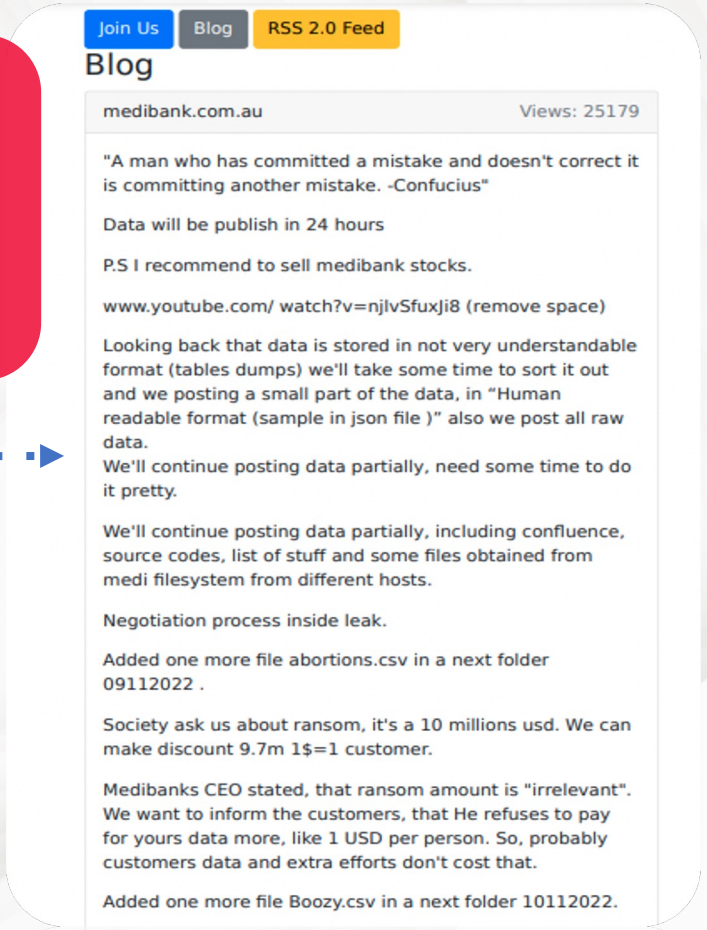


Wrzesień 2022

Niecały miesiąc od wystawienia dostępu sieciowego na sprzedaż Medibank publicznie ogłasza informacje o ataku

Październik 2022

Ogłoszenie o przeprowadzonym ataku



Listopad 2022

KELA

Atak Ransomware grupy REvil na Medibank

16 Września 2022 - Aktor **„c0xeec”** wystawia dostęp sieciowy na sprzedaż na kanale Telegram **„0x_dump”**

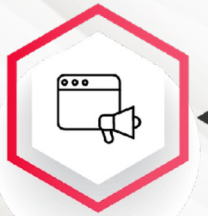
18 Września 2022 - Aktor **„c0xeec”** potwierdza sprzedaż dostępu sieciowego

Compromising the network

17 Października 2022 - Medibank publicznie potwierdza atak Ransomware

Pomiędzy **18 Października, a 5 Listopada 2022** mają miejsce negocjację pomiędzy atakującym a ofiarą

6 Listopada 2022 – Medibank ogłasza, że nie zapłaci okupu
7 Listopada 2022 – Revil ogłasza Medibank jako ofiarę ataku Ransomware na swoim blogu i zaczyna upubliczniać wykradzione dane



KELA

Atak Ransomware grupy LockBit na linie lotnicze Bangkoku

Wystawienie dostępu sieciowego na sprzedaż:
Lipiec 2021

Sprzedaż dostępu sieciowego:
Sierpień 2021

Wykrycie ataku przez ofiarę:
Sierpień 2021

Ogłoszenie o przeprowadzonym ataku:
Sierpień 2021

Atak Ransomware grupy LockBit na linie lotnicze Bangkoku

20 Lipca 2021 - Aktor **„babam”** wystawia dostęp sieciowy na sprzedaż

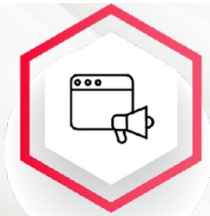
5 Sierpnia 2021 - Aktor **„ellis.J.douglas”** oferuje chęć zakupu po cenie **„buy-out” = 1000USD**. Brak potwierdzenia ww. transakcji.

Compromising the network

23 Sierpnia 2021 – Linie lotnicze Bangkoku wykrywają atak Ransomware

Nie są znane dokładne szczegóły dotyczące negocjacji pomiędzy atakującym, a ofiarą

25 Sierpnia 2021 – LockBit ogłasza, Linie lotnicze Bangkoku, jako ofiarę ataku Ransomeware na swoim blogu
28 Sierpnia 2021 – LockBit zaczyna upubliczniać wykradzione dane (dwa dni przed terminem zapłaty okupu!)



KELA

Cyber Threat Intelligence (CTI)

Proaktywna ochrona organizacji

Inwestycja w przyszłość Twojej organizacji

Zabezpieczenie budżetu na rozwiązania Cyber Threat Intelligence (CTI) w 2024 roku to konieczność

Do końca 2025 roku prawie 1/3 krajów ureguluje kwestię reagowania na ataki Ransomware, w tym negocjacje okupów z cyberprzestępcami

Do końca 2025 roku 70% CEO zbuduje strategię odporności, aby chronić się przed zagrożeniami związanymi z cyberprzestępczością

KELA

Gartner

Cyber Threat Intelligence w 2024 roku to konieczność

- Wycieki poświadczeń i dostępów sieciowych
- Kompromitacja kart kredytowych i fraudy finansowe
- Skompromitowane przez Malware końcówki (End-Point's)
- Ataki Ransomware i APT
- Wycieki kodów źródłowych aplikacji
- Wycieki danych osobowych i kradzież tożsamości

KELA


KELA
dostarcza informacje wywiadowcze,
które są dla Ciebie najważniejsze

Cyber Threat Intelligence

Pełna widoczność zagrożeń oraz możliwość mitygacji zdarzeń zanim przyjmą postać incydentów bezpieczeństwa

Ekosystem Cyberprzestępców

Grupy Telegram i Discord

Blogi Ransomware

Zautomatyzowane sklepy

Nielegalne markety

Podziemne fora

Zrzuty baz danych

Fraudy finansowe

Społeczności cyberprzestępców

Brokerzy Inicjalnych dostępów sieciowych

Platforma Cyberwywiadowcza KELA

Bezpiecznie nawigowanie w internetowym podziemiu

Informacje wywiadowcze w 100% ukierunkowane na zasoby organizacji 24/h 365

Usługi ekspertów Izraelskiego wywiadu

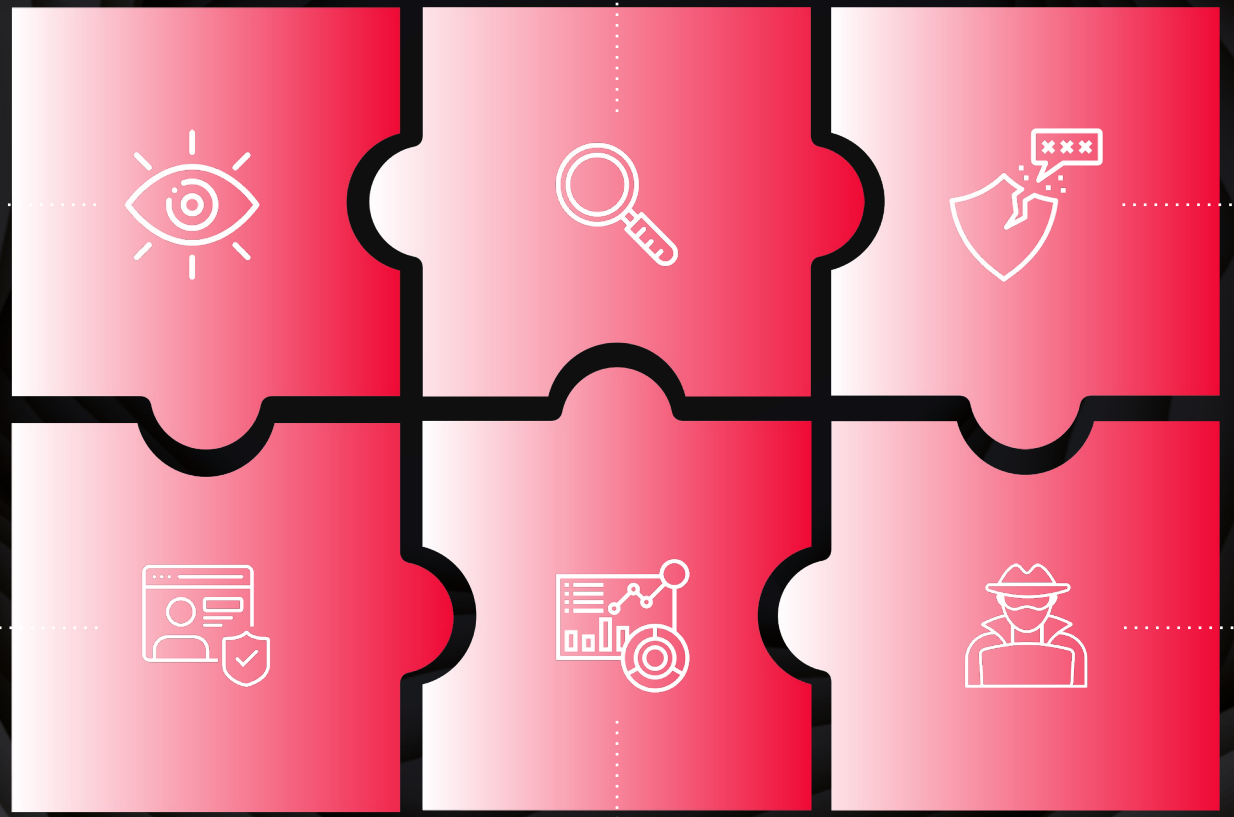
Automatyzacja i pełna integracja API z SIEM/SOAR

Platforma Cyberwywiadowcza KELA

Moduły Platformy Cyberwywiadowczej adresują cztery poziomy wykorzystania Cyberwywiadu

Investigate

Monitor



Technical Intelligence

Identity Guard

Threat Actors

Threat Landscape

Klienci na całym świecie:

KELA

Jak oceniają nas nasi klienci

5.0 ★★★★★ Feb 5, 2024

Review Source: ⓘ

Easy dark-web Intelligence

Reviewer Function: IT Security and Risk Management

Company Size: <50M USD

Industry: IT Services Industry

The product and services ar

5.0 ★★★★★ Feb 4, 2024

Review Source: ⓘ

Great Tool for Investigations related to Darkweb and Underground Forum Intelligence

Reviewer Function: IT Security and Risk Management

great intelligence tool and customer

5.0 ★★★★★ Jan 31, 2024

Review Source: ⓘ

Great for Dark Web Investigations

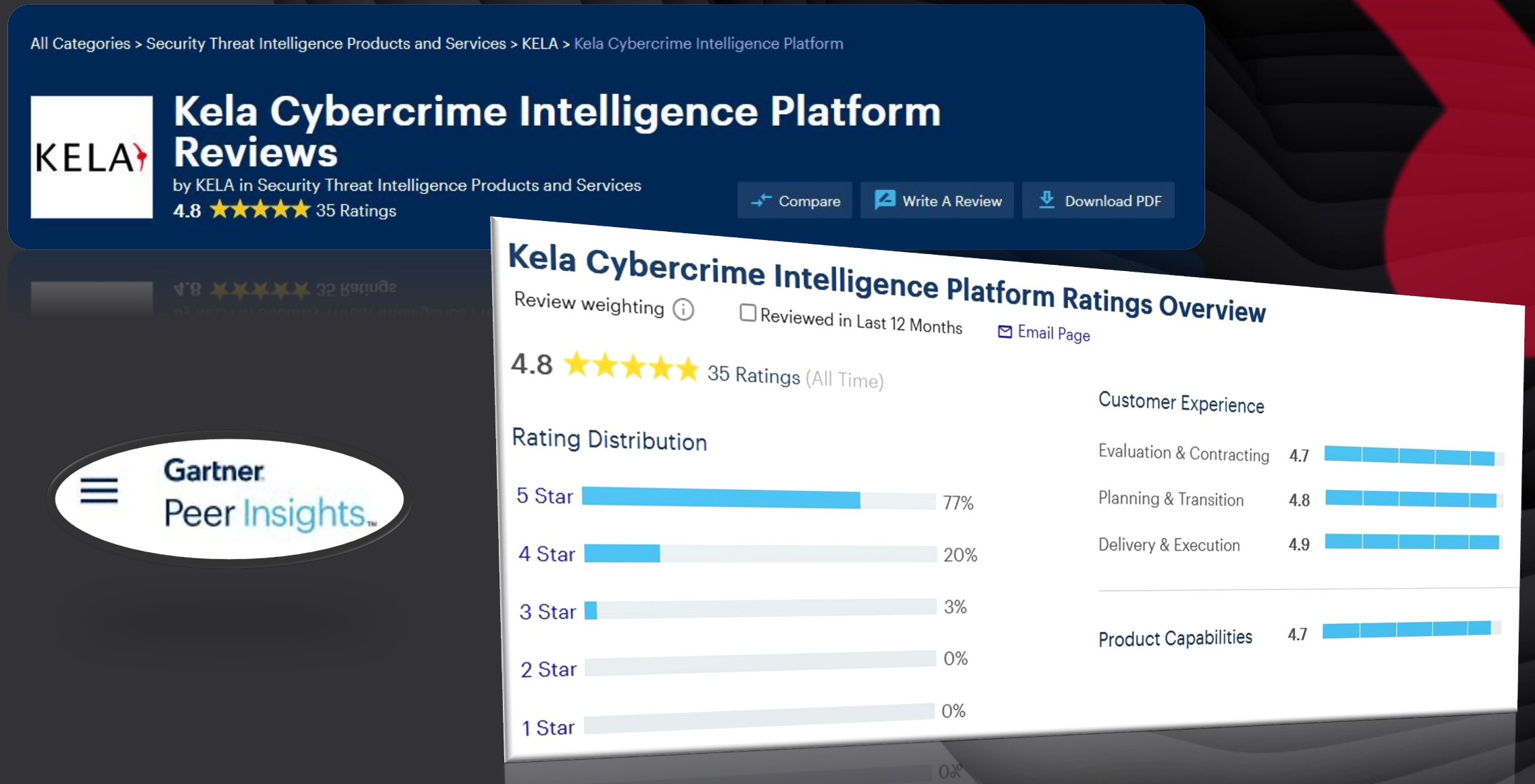
Reviewer Function: IT Security and Risk Management

Company Size: Gov't/PS/ED <5,000 Employees

Industry: Government Industry

The Platform is intuitive to use and does not require much training to onboard new team members. It provides a wide range of very helpful intelligence. The support team is also great. Overall, this is one of the best intelligence tools I have used.

Gartner Peer Insights – 4.8*



Gartner Peer Insights

NETFORMERS
Engineering Your Future

Praktyczne warsztaty z wykorzystania Platformy Cyberwywiadowczej KELA

KELA

20.06.2024

Ilość miejsc ograniczona!

KELA

Odkryj ekosystem cyberprzestępczości

Już dziś!

Z

KELA

KELA

Dziękuje!

www.kelacyber.com