

Dark Web Monitoring Webinar

13. & 19. März 2024

AVANTEC
Competence. Security. Trust.



Dark Web Monitoring – Sind Ihre Firmendaten im Dark Web?

Christian Grob
Head of Security Services
grob@avantec.ch

Robin Helbling
Cyber Defense Specialist
helbling@avantec.ch

Agenda

AVANTEC
Competence. Security. Trust.

1	Einleitung	Christian Grob
2	Einführung in das Dark & Deep Web	Robin Helbling
3	Grundlagen - Dark & Deep Web Monitoring	Robin Helbling
4	Herausforderungen & Best Practices bei der Datenermittlung	Robin Helbling
5	Trends	Robin Helbling
6	Q&A	Alle

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Einleitung
Today's Webinar

AVANTEC
Competence. Security. Trust.

Cyber Defense Portfolio

Managed EDR (CROWDSTRIKE)

- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen mittels schlankem Endpoint Agent
- Next GEN AV, EDR, Threat Hunting
- Umfangreiche Handlungsoptionen, direkter Eingriff auf Endpoints

Managed NDR (VECTRA)

- Erkennung & Verhinderung der Ausbreitung von Cyberangriffen durch Überwachung des Netzwerkverkehrs
- Kombination verschiedener Analyse-Verfahren u.a. ML/AI
- Ohne Agent auf den Endpoints

Managed Security Analytics (Hunters)

- Korrelation & Analyse von sicherheitsrelevanten Daten auf Basis der Hunters SOC Plattform
- Moderne SOC Plattform mit «Detection Engineering als Service» - 75-95%
- Keine Limiten für Log Ingestion

Dark Web Monitoring (KADUU)

- Überwachung des Dark Web auf Daten Leaks, Account Leaks & auffällige Erwähnungen in Foren
- Überwachung von Paste Sites, Onion Sites, Git
- Überwachung Ransomware Extortion Sites

Threat Intelligence (Recorded Future)

- Bereitstellung hochwertiger Threat Intelligence
- Unternehmensspezifische Threat Landscape
- Betrieb einer MISP Instanz inkl. Bereitstellung von Feeds - Indicators of Compromise (IOC)

Vulnerability Scanning (tenable)

- Identifikation von Schwachstellen mit regelmässigen Scans von extern oder intern
- Verwaltung der Scan Policies
- Regelmässiges Reporting mit Empfehlungen
- Verwalten der False-Positives

Einführung in das Dark & Deep Web
Definition of the "World Wide Webs"

AVANTEC
Competence. Security. Trust.

- Surface Web** = Indexiert von Suchmaschinen
- Deep Web** = nicht indexiert von Suchmaschinen und erfordert Authentisierung
- Dark Web** = Teilmenge von Deep Web, welcher nur mit spez. Software zugänglich ist. (TOR, I2P, Hyphanet, GUNet, ZeroNet, dn42, eD2k etc.)

The diagram illustrates the World Wide Web as an iceberg. The visible tip above the water represents the Surface Web, which is indexed by search engines and accounts for 4% of the total. The large, submerged part of the iceberg represents the Deep Web, which is not indexed and requires authentication, accounting for 90%. Within the submerged part, the Dark Web is also indicated, which is only accessible with specific software like TOR, I2P, etc., and accounts for 6% of the total.

Dark Web Monitoring Webinar

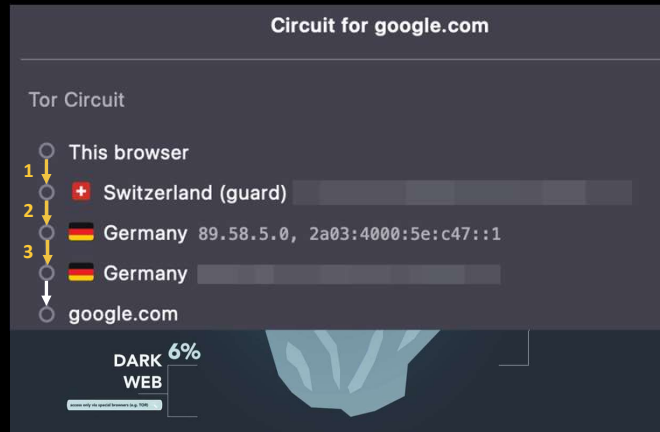
13. & 19. März 2024

Einführung in das Dark & Deep Web

Definition of the “World Wide Webs”

AVANTEC
Competence. Security. Trust.

- **Surface Web** = Indexiert von Suchmaschinen
- **Deep Web** = nicht indexiert von Suchmaschinen und erfordert Authentisierung
- **Dark Web** = Teilmenge von Deep Web, welcher nur mit spez. Software zugänglich ist. (TOR, I2P, Hyphanet, GNUet, ZeroNet, dn42, eD2k etc.)



Einführung in das Dark & Deep Web

Facts & Figures of TOR

AVANTEC
Competence. Security. Trust.

- 1995 US-Navy (Naval Research Laboratory)
 - Idee von «Onion Routing» war Schutz vor Spionage bzw. Geheimdiensten
- Ab ca. 2003 frei verfügbar, Transparenz/Dezentralisierung, 12 Nodes
 - Jeder konnte das TOR-Netzwerk nutzen
- 2008-2009 Entwicklung TOR Browser
- Seit 2009 wächst das TOR-Netzwerk und ist der «De-facto-Standard» für anonymen Datenaustausch via Internet
- **Nach wie vor ist das Ziel des TOR-Netzwerks:**
 - Verschleierung des Standorts, Schutz vor Identifikation sowie der Datenüberwachung
 - Zugang zu blockierten/zensierten Inhalten(BBC, Washington Post, NY Times uvm.)

Dark Web Monitoring Webinar

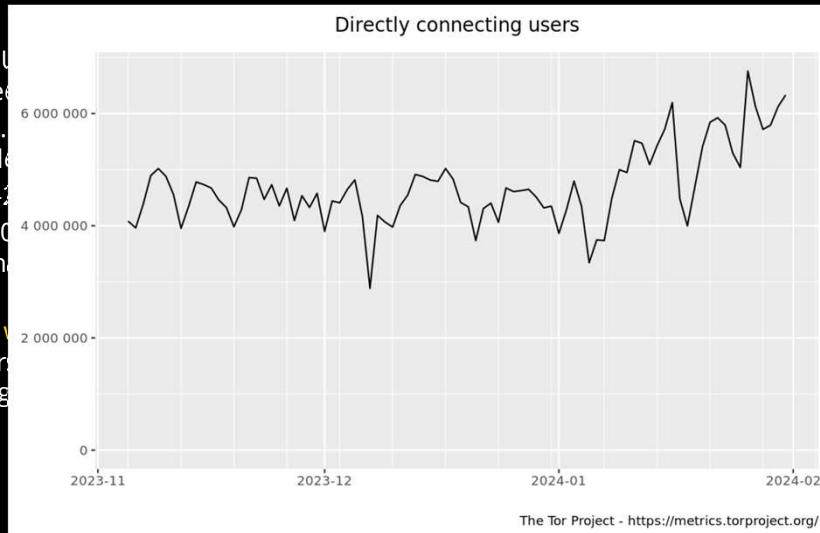
13. & 19. März 2024

Einführung in das Dark & Deep Web

Facts & Figures of TOR

AVANTEC
Competence. Security. Trust.

- 1995 U...
→ Ide...
- Ab ca...
→ Jed...
- 2008-2...
- Seit 20...
Daten...
- Nach V...
→ Ver...
→ Zug...



onymen

berwachung
es uvm.)

Einführung in das Dark & Deep Web

Abuse of Dark Web

AVANTEC
Competence. Security. Trust.

```
Replying to InterSystems's message: @FBI
#BF @ 🏴‍☠️ FBI: you run a forum but can't even set your own firewall up
#BF @ 🏴‍☠️ FBI: is it truly worth me monitoring it
Replying to FBI's message: you run a forum but can't even set your own firewall up
#BF @ 🌟 InterSystems: I'm still trying to control everything
#BF @ 🏴‍☠️ 0BITS: imagine a forum of hackers , using a free licensed commercial google collab of statics and asking to be anonymous
#BF @ 🌟 InterSystems: sorry, I'm taking care of everything " " from domain, firewall, cdn aaaa
Replying to InterSystems's message: I'm still trying to control everything
#BF @ 🏴‍☠️ FBI: your hosting provider is the true controller. and we already rooted them
#BF @ 🏴‍☠️ FBI: be a man and host it in grandma's basement
Replying to FBI's message: your hosting provider is the true controller. and we already rooted them
#BF @ 🌟 InterSystems: Can it?
#BF @ 🏴‍☠️ 0BITS: fr fr
Replying to FBI's message: you run a forum but can't even set your own firewall up
#BF @ C12OW: Hahahahaha
```

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Einführung in das Dark & Deep Web

Showcase: Abuse of Dark Web

AVANTEC
Competence. Security. Trust.




Chat to AI now..

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

AVANTEC
Competence. Security. Trust.

- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web



REC WEA DEL EXP INS C&C ACT

Cyber Kill Chain

Dark Web Monitoring Webinar

13. & 19. März 2024

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment



- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web

ID	Name	Description
G1011	EXOTIC LILY	EXOTIC LILY has searched for information on targeted individuals on business databases including RocketReach and CrunchBase. ^[3]



Cyber Kill Chain

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment



- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web

Initial access

DEV-0537 uses a variety of methods that are typically focused on compromising user identities to gain initial access to an organization including:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens from criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval
- Searching public code repositories for exposed credentials



Cyber Kill Chain

Dark Web Monitoring Webinar

13. & 19. März 2024

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

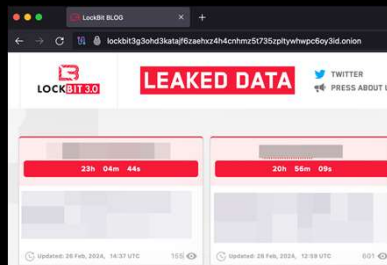
AVANTEC
Competence. Security. Trust.

- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web

Initial access

DEV-0537 uses a variety of methods that are typically focused on compromising user identities to gain initial access to an organization including:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens from criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval
- Searching public code repositories for exposed credentials



Cyber Kill Chain

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

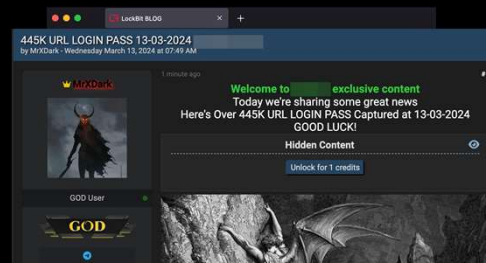
AVANTEC
Competence. Security. Trust.

- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web

Initial access

DEV-0537 uses a variety of methods that are typically focused on compromising user identities to gain initial access to an organization including:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens from criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval
- Searching public code repositories for exposed credentials



Cyber Kill Chain

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Top Use-Cases

AVANTEC
Competence. Security. Trust.

- Proaktive Suche nach abhandengekommenen Daten
- Ebenfalls einzusetzen für proaktives Threat Hunting (Bspw. Phishing Kampagnen sowie geplante Cyberangriffe) oder Schwachstellenanalysen usw.

- Credentials
- Remote Access Users
- Credit Cards
- Data Leak Detection (Company/Supply Chain)
- Threat Intelligence Source



NIST Cyber Security Framework

Grundlagen - Dark & Deep Web Monitoring

Showcase: Protect Remote Access Users

AVANTEC
Competence. Security. Trust.

```
"subject": "ch\\[REDACTED]",
"dumps": {
  {
    "name": "Stealer Malware Logs 2023-[REDACTED]",
    "description": "This credential data was derived from stealer malware logs. These logs are",
    "downloaded": "2023-[REDACTED]T12:26:50.996Z",
    "compromise": {
      "exfiltration_date": "2023-[REDACTED]T13:44:33.000Z",
      "os": "Windows 10",
      "os_username": "[REDACTED]",
      "malware_file": "C:\\Users\\[REDACTED]\\AppData\\Local\\Programs\\NvNode\\Speech\\dwm.exe",
      "timezone": "UTC-06:00",
      "computer_name": "[REDACTED]"
    },
    "infrastructure": {
      "ip": "189-[REDACTED]",
      "location": {
        "country": "MX"
      }
    }
  }
},
"first_downloaded": "2023-[REDACTED]T12:26:50.996Z",
"latest_downloaded": "2023-[REDACTED]T12:26:50.996Z",
"exposed_secret": {
  "type": "clear",
  "hashes": [
    {
      "algorithm": "SHA1",
      "hash_prefix": "3900"
    },
    {
      "algorithm": "SHA256",
      "hash_prefix": "857b"
    },
    {
      "algorithm": "NTLM",
      "hash_prefix": "438b"
    },
    {
      "algorithm": "MD5",
      "hash_prefix": "c285"
    }
  ]
}
```

```
"compromise": {
  "exfiltration_date": "2023-[REDACTED]T13:44:33.000Z"
},
"authorization_service": {
  "url": "https://auth.[REDACTED]com/vpn/tmindex.html",
  "domain": "[REDACTED]com",
  "fqdn": "auth.[REDACTED]com",
  "technology": [
    {
      "name": "Citrix NetScaler Access Gateway",
      "id": "[REDACTED]",
      "category": "[REDACTED]"
    },
    {
      "name": "vpn",
      "id": "[REDACTED]"
    }
  ],
  "protocols": [
    "https"
  ]
},
"malware_family": {
  "name": "Vidar",
  "id": "[REDACTED]"
},
"cookies": [
  {
    "dns": "[REDACTED]com",
    "name": "_ga",
    "http": true,
    "expiration": "2024-[REDACTED]T17:32:58.000Z",
    "secure": true
  }
],
}
```

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Data Leak Detection (Supply Chain)

AVANTEC
Competence. Security. Trust.

- 06.03.2024 - Kunde informierte das AVANTEC CDC aufgrund eines mutmasslichen Datenabflusses bei seinem Lieferanten «AlgoSec» - Befürchtung war, dass alle Firewall-Rulesets und dadurch die gesamte Netzwerktopologie veröffentlicht werden könnte.
- Dieser Lieferant war zu diesem Zeitpunkt noch nicht im Scope des automatisierten Dark Web Monitorings. → Manuelle Datenermittlung begann

AlgoSec Data Breach after:2024-02-02

X · H4ckManac
18+ „Gefällt mir“-Angaben

HackManac

DataBreach Alert ⚠️ Network Security Software AlgoSec Allegedly Breached A 227 GB database belonging to AlgoSec, containing customer data and contact ...

HackManac @H4ckManac

#DataBreach Alert ⚠️

Network Security Software AlgoSec Allegedly Breached

A 227 GB database belonging to AlgoSec, containing customer data and contact records, is for sale on a hacking forum. ←


"I am selling 227GB of A32 customer data and 7K .xlsx rows of contact records taken from AlgoSec," said the cyber criminal.

The threat actor with the alias "Ddarknotevil" publishes various samples as proof of the data exfiltration and is selling them for \$2500. ←

AlgoSec is a network security software company based in New Jersey in the United States. The organization provides software for network security policy management, also known as firewall policy management.

The confirmation or denial of these claims has yet to be verified.

#USA #DataBreach



Grundlagen - Dark & Deep Web Monitoring


Showcase: Data Leak Detection (Supply Chain)

AVANTEC
Competence. Security. Trust.

- USA AlgoSec.com Clients - 227GB
by Ddarknotevil - Monday March 4, 2024 at 08:03 PM

9 hours ago

Ddarknotevil



Thank me later

GOD

X · H4ckManac
18+ „Gefällt mir“-Angaben

HackManac

DataBreach Alert ⚠️ Network Security Software AlgoSec Allegedly Breached A 227 GB database belonging to AlgoSec, containing customer data and contact ...

algosec

Hello **BreachForums** Community,

I am selling 227GB of A32 customers data & 7K .xlsx rows Contact record Taken from AlgoSec, which serves many companies from around the world across different sectors such as banks, governments, education, and more.


*AlgoSec is a network security software company headquartered in Ridgefield Park, New Jersey, United States. Established in 2004, they specialize in providing solutions for network security policy management, also known as firewall policy management. Led by CEO Yuval Baron/Annual Revenue \$75M - \$100M

\$2500 Contact Telegram & PM for TOX - Secrow - MM accepted

Samples:

A32 Customers Data Part1.zip
A32 Customers Data Part2.zip
A32 Customers Data Part3.zip

#USA #DataBreach



Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Data Leak Detection (Supply Chain)

AVANTEC
Competence. Security. Trust.

breachforums.cx/Thread-SELLING-USA-AlgoSec-com-Clients-227GB?pid=464411

Databases Upgrades Search Hidden Service Escrow Extras

BreachForums Board Message

BreachForums

The specified thread does not exist.

Breach Forums Contact Us Rules & Policies Changelog Canary

Current time: 03-06-2024, 06:42 PM

algosec

Grundlagen - Dark & Deep Web Monitoring

Showcase: Data Leak Detection (Supply Chain)

AVANTEC
Competence. Security. Trust.

- Daraufhin erhielten wir die Benachrichtigung, dass ein weiterer betroffener Kunde das Leak wohl bereits erwerben konnte und «nur» Teile der Netzwerkarchitektur unseres Kunden beinhaltet.
- Lessons Learned: Unser Kunde erweiterte die gewünschten Suchbegriffe für den Dark Web Monitoring Service um seine gesamte Supply Chain.

Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

AVANTEC
Competence. Security. Trust.

- **08.03.2024** - Kunde kontaktierte das AVANTEC CDC aufgrund dutzenden fehlgeschlagenen VPN Logins (Webportal) an der Perimeter Firewall, welche zur **Abteilung A** gehört.
- **Alle** für die Logins verwendeten Benutzernamen existieren - jedoch nur auf der Firewall der **Abteilung B** und konnten dadurch nicht funktionieren.

```
Message meets Alert condition
The following critical firewall event was detected: SSL VPN login fail.
date=2024- time=10:22:52 devname= eventtime= tz="+0100" logid="
type="event" subtype="vpn" level="alert" vd="" logdesc="SSL VPN login fail" action="ssl-login-fail" tunneltype="ssl-web" tunnelid=0
remip=185. user="" group="" dst_host="N/A" reason="sslvpn_login_unknown_user" msg="SSL user failed to logged in"
```

- Zu diesem Zeitpunkt war nicht klar, ob der Angreifer im Besitz von gültigen Passwörtern/Cookies ist, jedoch der falsche «Entry Point» erwischt hat. Dies galt es schnellstmöglich zu klären, um geeignete Response Massnahmen einzuleiten.

Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

AVANTEC
Competence. Security. Trust.

Tags: Dark Web Monitoring, Account Leaks

Description

Matched Search Query: `AND createdAt:[2024-01-25 TO *]`

This Finding contains 63 items.

New Account Leak with ID: `...`

Dates
Published: '2024-01-18'
Discovered: '2024-02-28'

User Account	Password	Website	Risk Score	Notified
'...@...'	'...@...'	'...@...'	7.0	no

- Keine zutreffenden Account Leaks gefunden. Vielmehr konnten wir «User-Collections» auffinden, welche alle verwendeten Benutzernamen enthielten. Es konnte deshalb davon ausgegangen werden, dass keine Zugangsdaten geleakt wurden und deshalb kein Passwortwechsel initiiert werden muss.

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

AVANTEC
Competence. Security. Trust.

The screenshot shows a web interface for monitoring threat intelligence. It features a search bar with a query, a list of findings, and a detailed view of a finding. A large yellow box is overlaid on the screenshot with the text "MTTR = 15min".

- Keine zutreffenden Account Leaks gefunden. Vielmehr konnten wir «User-Collections» auffinden, welche alle verwendeten Benutzernamen enthielten. Es konnte deshalb davon ausgegangen werden, dass keine Zugangsdaten geleakt wurden und deshalb kein Passwortwechsel initiiert werden muss.

Grundlagen - Dark & Deep Web Monitoring

Our approach to monitor the Dark Web

AVANTEC
Competence. Security. Trust.

Surface, Deep &
Dark Web



Chats &
Forums



Other Feeds



Data
Providers



Customer
Search Filters



Dedup & Data
Processing



SIRP &
Context



Alert
Pipeline



Security Analyst

AVANTEC
Competence. Security. Trust.

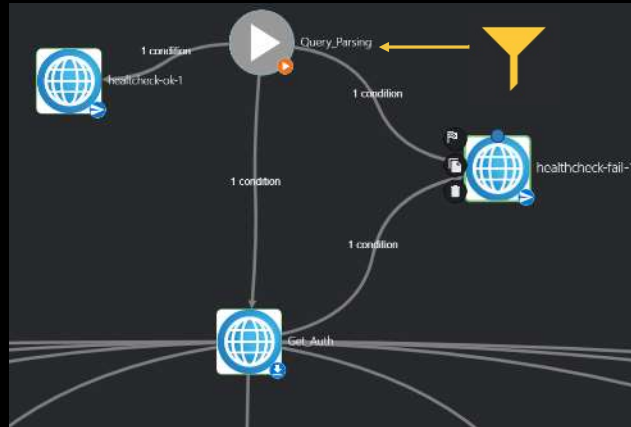
Dark Web Monitoring Webinar

13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Our approach to monitor the Dark Web

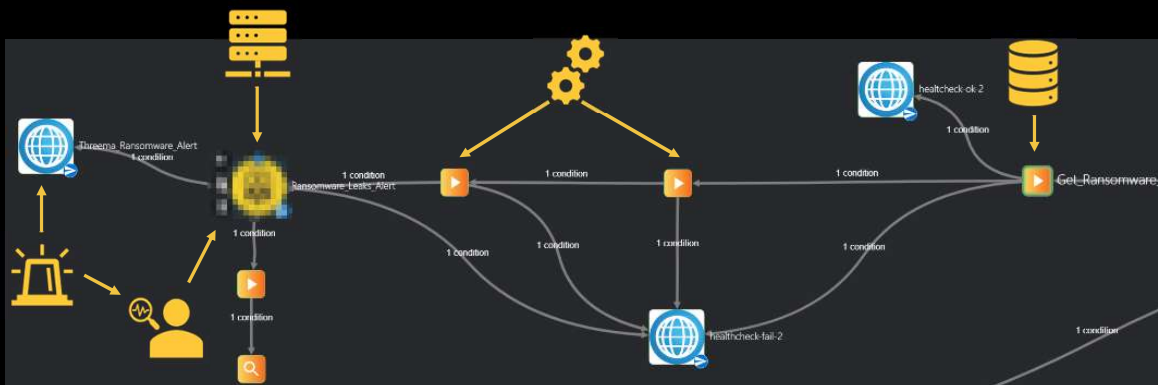
AVANTEC
Competence. Security. Trust.



Grundlagen - Dark & Deep Web Monitoring

Our approach to monitor the Dark Web

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar

13. & 19. März 2024

Herausforderungen & Best Practices bei der Datenermittlung

Challenges & Best Practices



- **Cha:** Identifikation von sensitiven Informationen
BP: Klassifizierte und sensitive Daten markieren/Kennzeichnen
- **Cha:** Response Prozesse für die unterschiedlichen Datenklassen entwickeln
BP: Vorbereitung Dark Web Access inkl. Workstation, Accounts und Krypto Wallets etc.
- **Cha:** Reaktionszeit bei Findings
BP: Überwachung von Social Media Kanälen und Chatgruppen
Implementierung einer Alert-Pipeline und vorbereitende Massnahmen treffen
- **Cha:** Handling der False-Positives
BP: Eindeutig identifizierbare Suchbegriffe/Strings definieren
Prozess für Deduplizierung implementieren
Blacklist einbetten
- **Cha:** Aufrechterhaltung der Datenquellen
BP: Recherche nach neuen sowie Verifikation der genutzten Quellen
- **Cha:** Implementierung des Datenschutzkonzept
BP: Maskierung, Pseudonymisierung, Archivierung oder Löschen

Trends

Latest Dark Web Trends



- Vermehrte Nutzung von «closed sources» im Deep sowie Surface Web
Motivation: Aufgrund der Zugänglichkeit und Erreichbarkeit zu Käufern
- Supply Chain Compromise ist weiterhin auf dem Vormarsch
Motivation: Attraktives Ziel, da oftmals grosse Auswirkung und viel zahlungsbereite Kundschaft
- InfoStealer Malware wird beliebter
Motivation: Valide Credentials/Session Tokens sind erfolgsversprechend für Cyber Operations und hard-to-detect während der unautorisierten Nutzung

Notably, posts offering Redline stealer logs, a popular malware family, tripled from an average of 370 per month in 2022 to 1,200 in 2023. Overall, the volume of various malware log files, containing compromised user data and freely posted on the dark web, rose by almost 30 percent in 2023, compared to the previous year.

Source: «Dark web market trends: last year in review and projections for 2024, Kaspersky»



Dark Web Monitoring Webinar

13. & 19. März 2024

Trends

Latest Dark Web Trends

AVANTEC
Competence. Security. Trust.

- Vermehrte Nutzung von «close»
Motivation: Aufgrund der Zugänglichkeit
- Supply Chain Compromise ist...
Motivation: Attraktives Ziel, da... Kundenschaft
- InfoStealer Malware wird...
Motivation: Valide Credentials für Cyber Operations

Notably, posts offering...
2022 to 1,200 in 2023...
freely posted on the dark web...
Source: «Dark web market trends: last year»

MALWARE-FREE
ACTIVITY
>>
75% 2023
71% 2022
62% 2021
51% 2020
40% 2019

Access Broker Advertisements by Month

Month	Count
JAN	150
FEB	89
MAR	352
APR	160
MAY	134
JUNE	211
JULY	172
AUG	392
SEPT	194
OCT	449
NOV	450
DEC	239
TOTAL	2,902

Source: «Global Threat Report 2024, CrowdStrike»

Trends

Latest Dark Web Trends

AVANTEC
Competence. Security. Trust.

- Vermehrte Nutzung von «close»
Motivation: Aufgrund der Zugänglichkeit
- Supply Chain Compromise ist...
Motivation: Attraktives Ziel, da... Kundenschaft
- InfoStealer Malware wird...
Motivation: Valide Credentials für Cyber Operations und h...

Notably, posts offering Redline stealer log...
2022 to 1,200 in 2023. Overall, the volume...
freely posted on the dark web, rose by...
Source: «Dark web market trends: last year»

Security Recommendations

Detect Leaked Passwords
Your Mac can securely monitor your passwords and alert you if they appear in known data leaks. [About Passwords & Privacy...](#)

Show alerts when passwords are found in an online leak
We check your passwords saved in Edge against a known repository of exposed credentials and alert you if a match is found. [Learn more](#)

Password Leak Detection
Enables the detection of leaked passwords. – Mac, Windows, Linux, Chrome OS, Android
#password-leak-detection

Datenschutz & Sicherheit

Synchronisation

Mehr von Mozilla

- Starke Passwörter erzeugen und vorschlagen
- Firefox Relay-E-Mail-Masken zum Schutz Ihrer E-Mail-Adresse vorschlagen
- Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren

Dark Web Monitoring Webinar

13. & 19. März 2024

Key-Takeaways



... und Mehrwert eines Dark Web Monitoring-Services

- 1** Einfacher und wirkungsvoller Schutz gegen opportunistische Cyberangriffe
 - Aktuelle Cyberbedrohungen erfordern einen proaktiven Schutz vor Identitätsmissbrauch
 - Vollständige Prävention gegen Identitätsdiebstahl praktisch unmöglich
- 2** Frühwarnsystem für geleakte Daten
 - Rechtzeitige Reaktion auf Datenlecks die Source Code, Geschäftsgeheimnisse oder ausgelagerte Informationen bei Lieferanten/Partnern betreffen
- 3** Security Incident Enrichment
 - Erweiterter Kontext für effiziente Triage aufgrund aktuellen Datenleaks oder Schwachstellen-Trends etc.
 - Schnellere Identifizierung des Patient 0

Q & A



Sind Ihre Firmendaten im Dark Web?

Kontinuierliche Überwachung des Dark und Deep Web auf Daten und Account Leaks sowie auffällige Erwähnungen in Untergrund-Foren

- ✓ Kontinuierliche Suche nach kompromittierten Accounts mit Bezug zum Kunden
- ✓ Kontinuierliche Suche nach gestohlenen Daten z.B. von Ransomware Gruppen
- ✓ Monitoring von Domains mit Bezug zum Kunden (Hinweis Phishing Kampagnen)
- ✓ Überwachung von Paste Sites, Onion Sites, Git etc.
- ✓ Spezifisches Monitoring von Kredit Karten
- ✓ Überwachung Ransomware Data Leak Sites (auch von Herstellern/Vendoren/Partnerfirmen)
- ✓ Alarmierung bei kritischen Feststellungen

