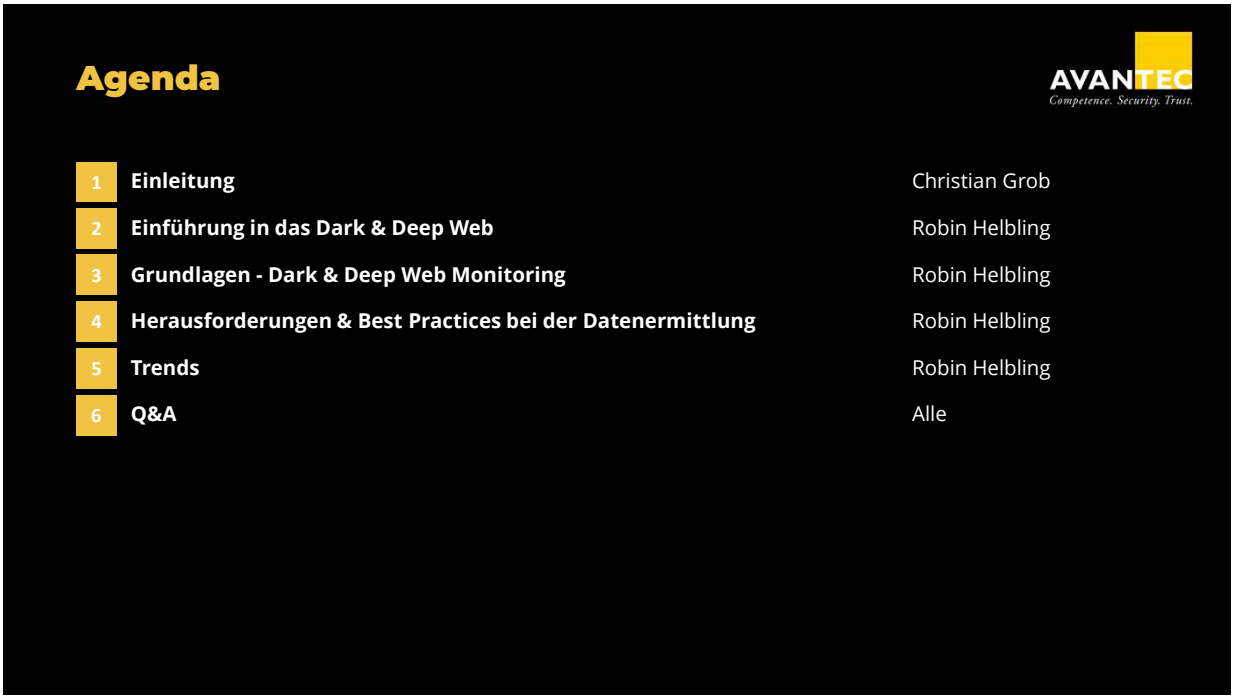
Dark Web Monitoring Webinar
13. & 19. März 2024



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

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

Webinar

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

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

Managed Security Analytics
- 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

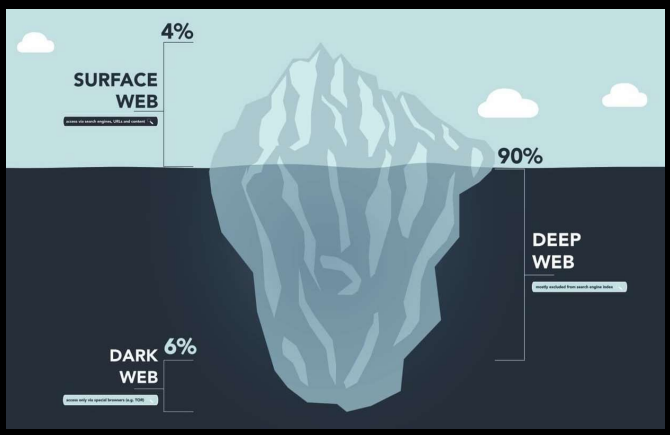
Threat Intelligence
- Bereitstellung hochwertiger Threat Intelligence
- Unternehmensspezifische Threat Landscape
- Betrieb einer MISP Instanz inkl. Bereitstellung von Feeds - Indicators of Compromise (IOC)

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, GNUnet, ZeroNet, dn42, eD2k etc.)



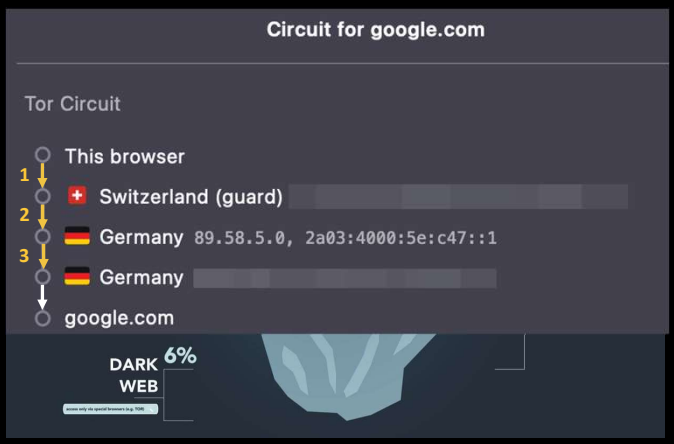
AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Einführung in das Dark & Deep Web

Definition of the "World Wide Webs"

- 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, GNUnet, ZeroNet, dn42, eD2k etc.)



Einführung in das Dark & Deep Web

Facts & Figures of TOR

- 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.)

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Einführung in das Dark & Deep Web

Facts & Figures of TOR

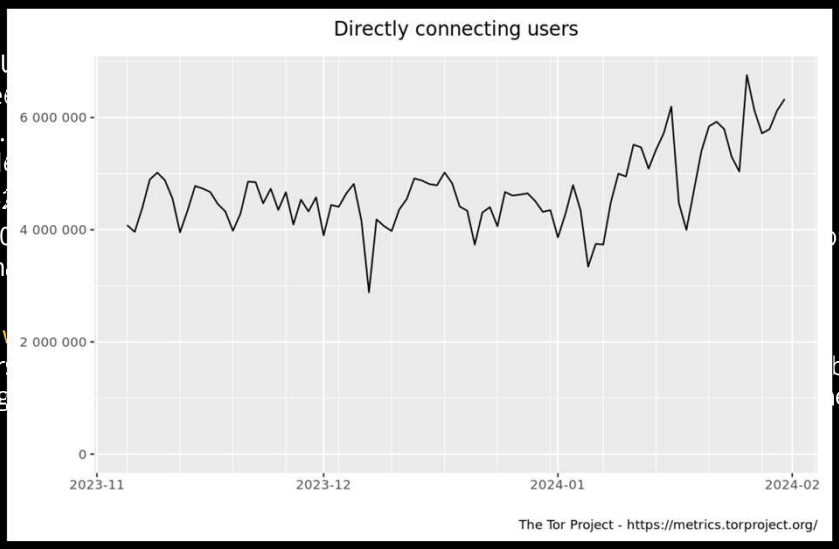
AVANTEC
Competence. Security. Trust.

- 1995 U
  → Ide
- Ab ca.
  → Jed
- 2008-2
- Seit 20
  Daten

onymen

- Nach v
  → Ver
  → Zug

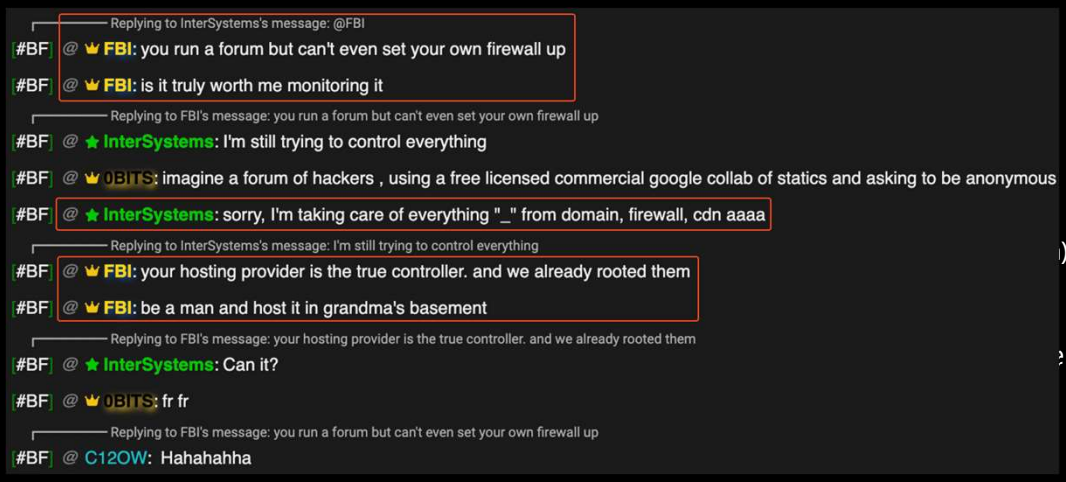
berwachung
es uvm.)



Einführung in das Dark & Deep Web

Abuse of Dark Web

AVANTEC
Competence. Security. Trust.



)

en

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Einführung in das Dark & Deep Web

Showcase: Abuse of Dark Web

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

- Viele Cybersicherheitsvorfälle beginnen oder enden im Dark Web

Cyber Kill Chain

AVANTEC
Competence. Security. Trust.

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

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

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

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

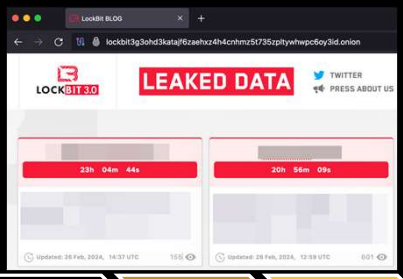
AVANTEC
Competence. Security. Trust.

- 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



REC → WEA → DEL → EXP → INS → C&C → ACT

Cyber Kill Chain

Einführung in das Dark & Deep Web

Dark Web and Attack Phases alignment

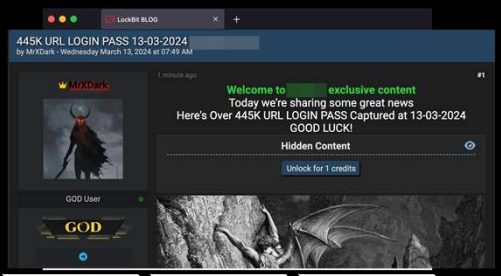
AVANTEC
Competence. Security. Trust.

- 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



REC → WEA → DEL → EXP → INS → C&C → ACT

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[redacted]",
            "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.

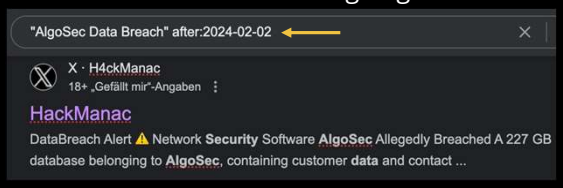
Dark Web Monitoring Webinar
13. & 19. März 2024

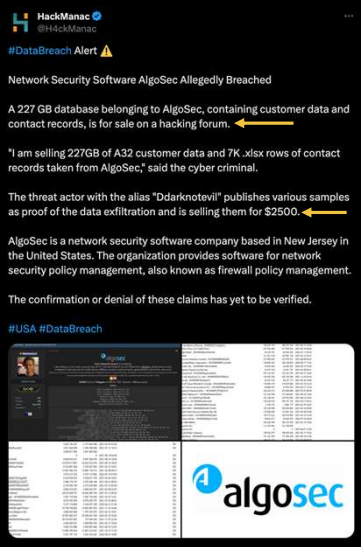
Grundlagen - Dark & Deep Web Monitoring

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



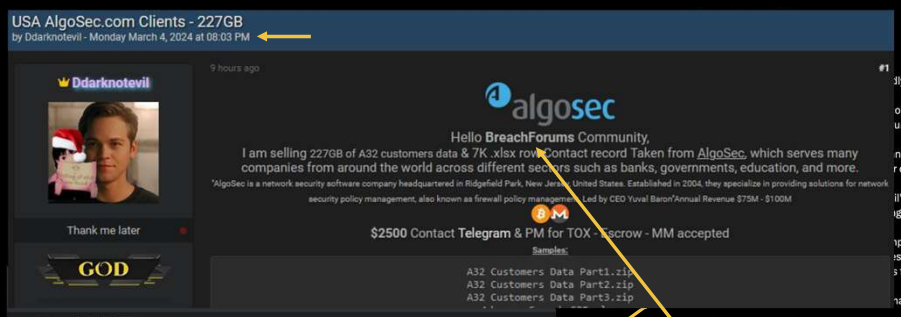


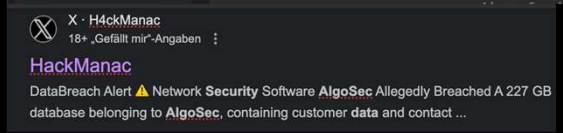
Grundlagen - Dark & Deep Web Monitoring

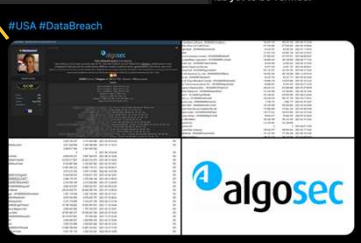
Showcase: Data Leak Detection (Supply Chain)

AVANTEC
Competence. Security. Trust.

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





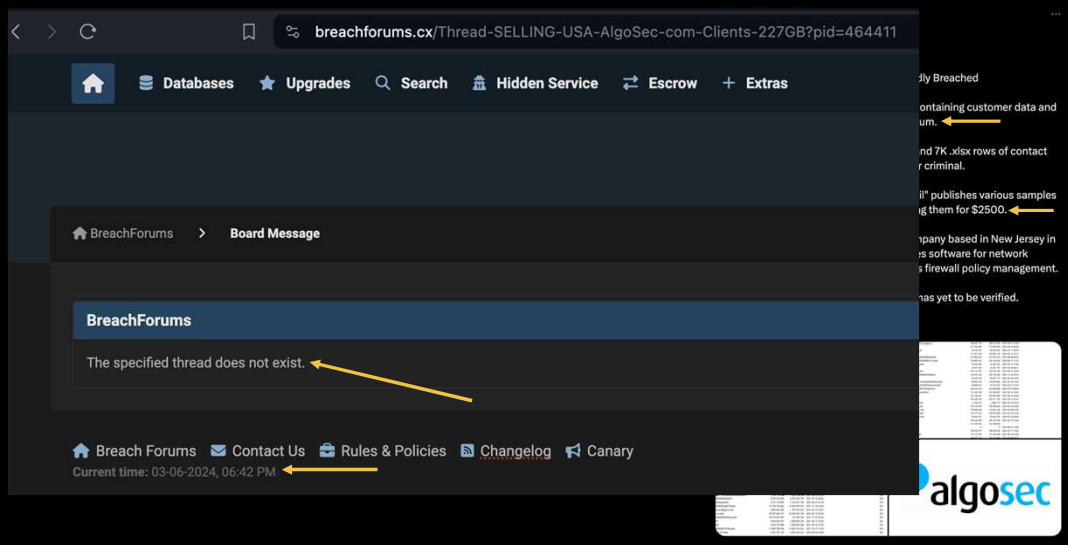


AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Data Leak Detection (Supply Chain)



Grundlagen - Dark & Deep Web Monitoring

Showcase: Data Leak Detection (Supply Chain)

- 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.

AVANTEC
Competence. Security. Trust.

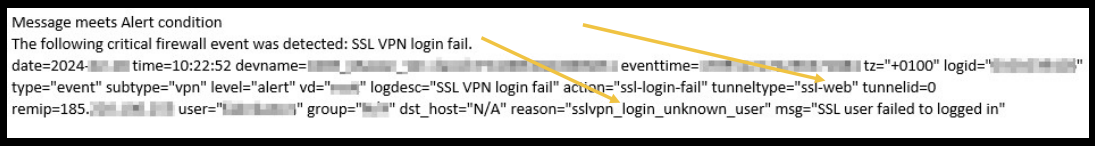
Dark Web Monitoring Webinar
13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

AVANTEC
Competence. Security. Trust.

- **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.

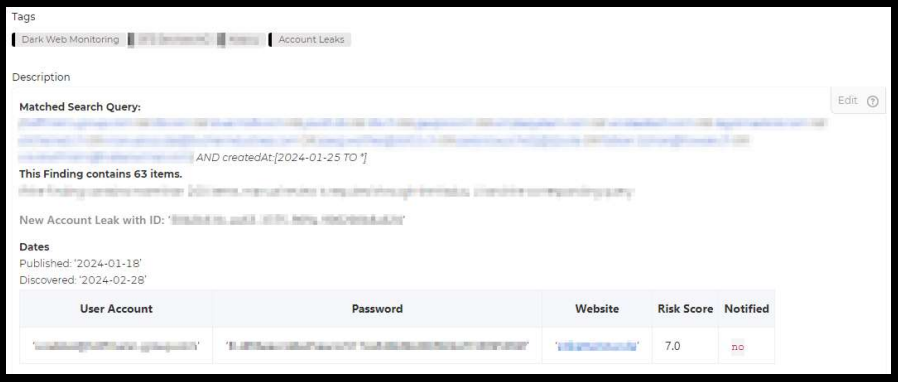


- Zu diesem Zeitpunkt war nicht klar, ob der Angreifer im Besitz von gültigen Passwörter/Cookies ist, jedoch der falsche «Entry Point» erwischt hat. Dies galt es schnellstmöglich zu klären, um geeignete Response Massnahmen einzuleiten.

Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

AVANTEC
Competence. Security. Trust.



- 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

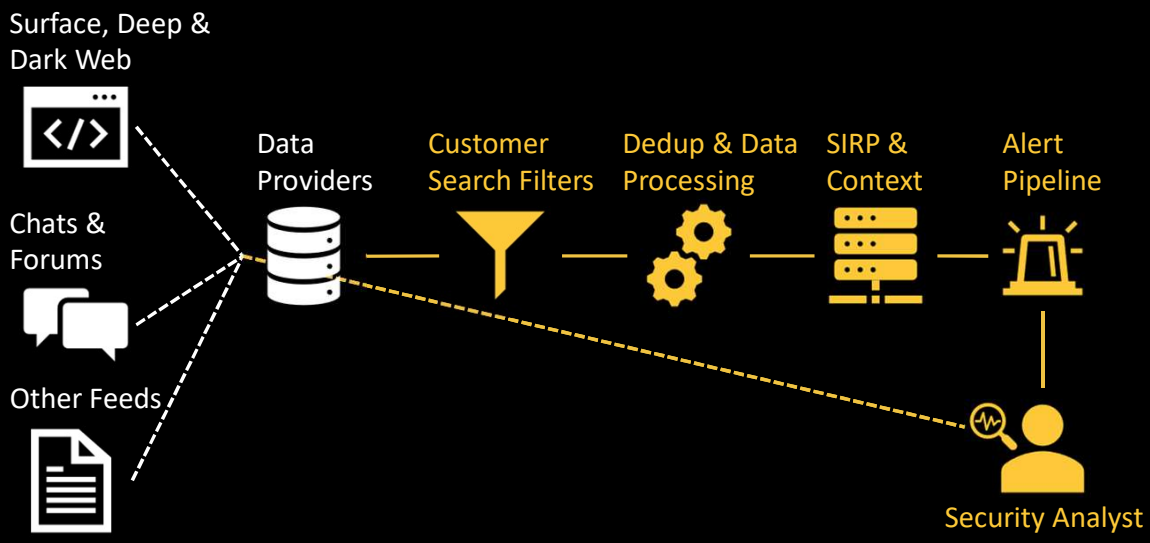
Grundlagen - Dark & Deep Web Monitoring

Showcase: Threat Intelligence Source

- 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



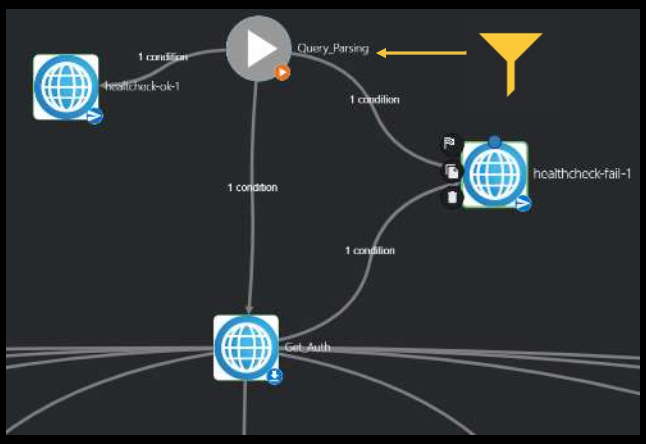
AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Grundlagen - Dark & Deep Web Monitoring

Our approach to monitor the Dark Web

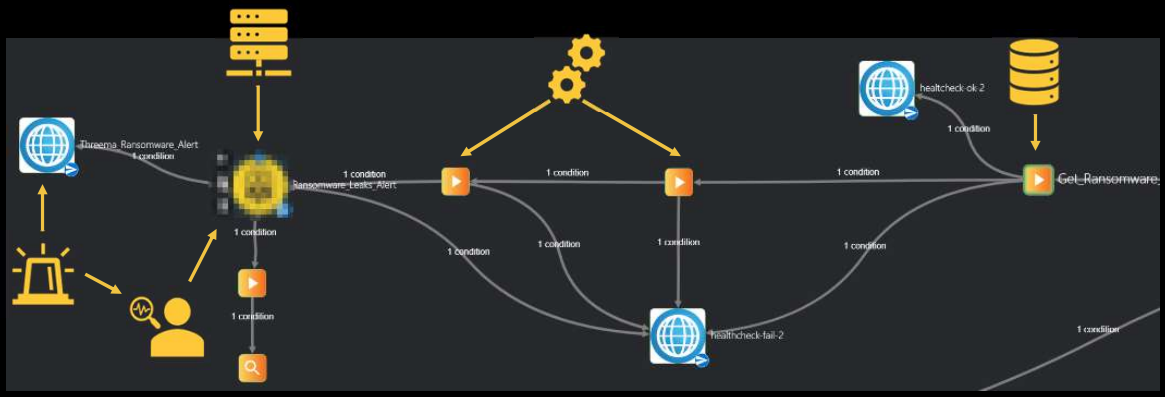
AVANTEC
Competence. Security. Trust.



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

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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»

AVANTEC
Competence. Security. Trust.

Dark Web Monitoring Webinar
13. & 19. März 2024

Trends

Latest Dark Web Trends

AVANTEC
Competence. Security. Trust.

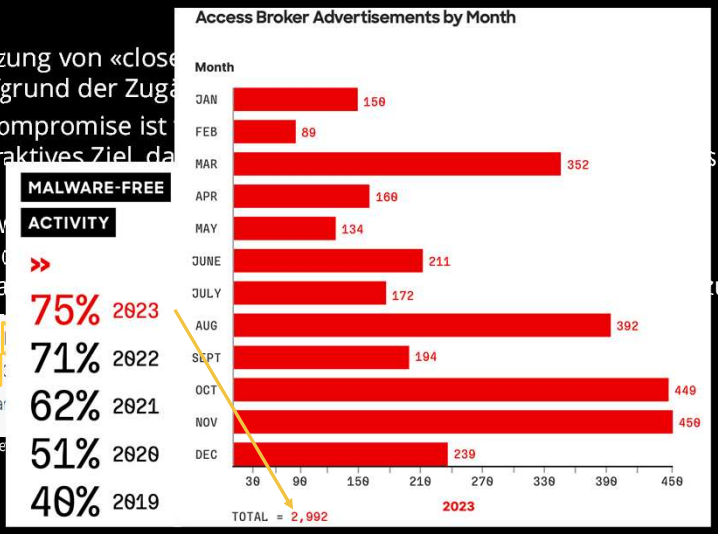
- Vermehrte Nutzung von «close
  Motivation: Aufgrund der Zug
- Supply Chain Compromise ist
  Motivation: Attraktives Ziel, da
  Kundschaft
- InfoStealer Malw
  Motivation: Vali
  für Cyber Opera

sbereite

ung

Notably, posts offering
2022 to 1,200 in 2023.
freely posted on the da

Source: «Dark web marke



Source: «Global Threat Report 2024, CrowdStrike»

Trends

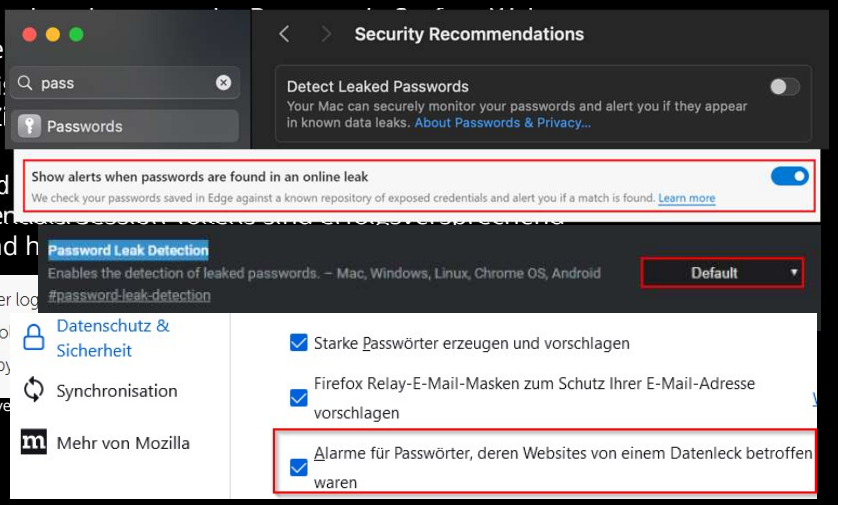
Latest Dark Web Trends

AVANTEC
Competence. Security. Trust.

- Vermehrte Nutzung von
  Motivation: Aufgrund de
- Supply Chain Compromi
  Motivation: Attraktives Z
  Kundschaft
- InfoStealer Malware wird
  Motivation: Valide Creden
  für Cyber Operations und h

Notably, posts offering Redline stealer log
2022 to 1,200 in 2023. Overall, the vo
freely posted on the dark web, rose by

Source: «Dark web market trends: last ye



AVANTEC
Competence. Security. Trust.

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

AVANTEC
Competence. Security. Trust.