



Mehrwert hochwertiger Threat Intelligence bei der Vorbereitung oder Bewältigung von Cyberangriffen

Christian Grob

Head of Security Services
Mitglied der Geschäftsleitung

Agenda

- 1 **Bedrohungslage & Einleitung**
- 2 **Arten von Threat Intelligence**
- 3 **Bereiche und Fragestellungen**
- 4 **Stakeholder**
- 5 **Quellen & Marktübersicht**
- 6 **Threat Intelligence Lifecycle**
- 7 **Beispiele Threat Intelligence**
- 8 **AVANTEC Cyber Defense Services**
- 9 **Q&A**

Cyber Bedrohungslage



Knapp 50'000 Meldungen im 2023 beim Nationalen Zentrum für Cyber Sicherheit (NCSC) – im Vergleich zum Vorjahr +30%



Cyberkriminelle werden professioneller – 84 Minuten vergehen gemäss CrowdStrike vom Initial Access -> Lateral Movement



Das **Zeitfenster**, um Angriffe abzuwehren bevor diese einen grösseren Schaden anrichten, **wird immer kleiner**



Terabytes sensibler Daten von CH Unternehmen **im Dark Web** – Double Extortion beliebt bei Angreifer



Ungepatchete **Schwachstellen**, offene oder **falsch konfigurierte** extern erreichbare Dienste, **Supply-Chain Angriffe**



Mittelständische Unternehmen vermehrt im Visier, **fehlende Ressourcen** im Bereich Cyber Sicherheit führen zu Breaches

Angriffsfläche

Wachsende Angriffsfläche durch zunehmenden Einsatz & Komplexität der Technologie

Bedrohungen

Informationen über Bedrohungen müssen **schneller verarbeitet** werden

- um mit der **Geschwindigkeit** und Professionalisierung der **Angreifer mitzuhalten**
- und das Sicherheitsdispositiv **rechtzeitig** zu **adaptieren**

Definition

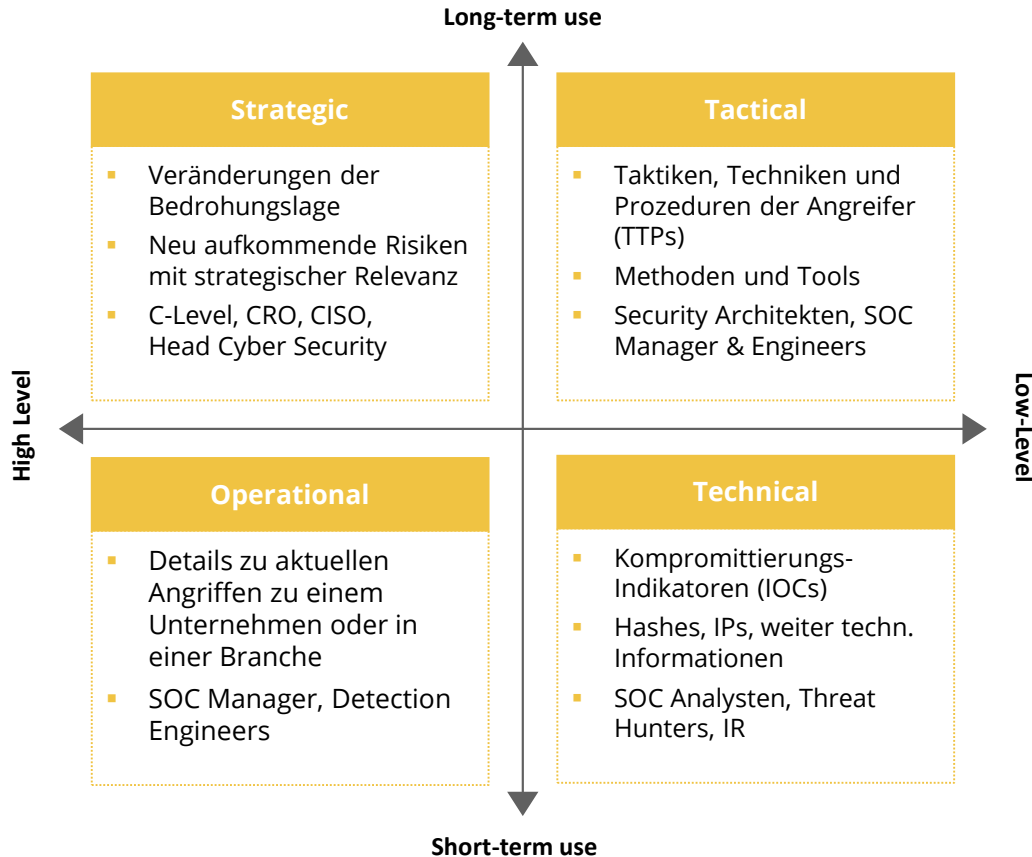
Threat Intelligence

- entsteht durch **Bewertung** vergangener, gegenwärtiger und potenzieller **Bedrohungen**
- unter **Berücksichtigung** des **Kontext** des jeweiligen Unternehmens
- um **möglichst viel Klarheit** für gute strategische, taktische und operative **Entscheidung & Investitionen** zu schaffen

Status Quo

Viele Unternehmen nutzen Threat Intelligence **“nur” am Rande** z.B. in Form von Feeds

Arten von Threat Intelligence



Threat Intelligence soll:

relevant sein

Berücksichtigung der **spezifischen Gegebenheiten** des Unternehmens & konkreten Geschäftsfeldes

zeitgerecht sein

Balance zwischen **Geschwindigkeit & Qualität** der bereitgestellten Information

vertrauenswürdig sein

Verlässliche und qualitativ **hochwertige Quellen** erhöhen den effektiven **Mehrwert**

Bereiche und Fragestellungen

Bereiche	Beispiel Fragestellungen
Branche (Industrie)	Welche Angriffe sind in unserer Branche wahrscheinlich? Von welchen Angriffen sind meine direkten Konkurrenten betroffen?
Geographisch	Welche Angriffe sind in unserer Land/Region wahrscheinlich? Welche Angreifer Gruppen sind besonders in unserem Land/Region aktiv?
Technologie	Gibt es Angriffe die speziell auf von uns eingesetzte Technologien abzielen? Werden spezifische Schwachstellen in eingesetzten Technologien ausgenutzt?
Geplante Angriffe	Gibt es Anzeichen für einen bevorstehenden Angriff auf unser Unternehmen? Bieten wir Angriffsfläche die für Angreifer ein leichtes Ziel darstellen könnte?
Kunden	Werden unsere Kunden angegriffen und könnte dies unserem Unternehmen schaden? Könnte ich meine Kunden frühzeitig über bevorstehende Angriffe informieren?
Geschäftspartner (3rd Parties)	Werden unsere Geschäftspartner angegriffen & könnte dies unserem Unternehmen schaden? Stellen gewisse Geschäftspartner ein erhöhtes Risiko dar?
Erfolgreiche Angriffe	Gibt es Indikatoren für einen bereits erfolgreich stattgefundenen Angriff? Sind Accounts teil eines Dumps oder werden Accounts im Dark Web verkauft?

Stakeholder & Art der Information



Beispiele für Art der Information

- Strategische Intelligence Reports (Trends, Ausblick, Einschätzung)
- Aktuelle Bedrohungslage (Threat Landscape, Angreifer Gruppen)
- Threat Models, TTPs, Tools
- Vulnerability Intelligence / Patch Priorisierung (Criticals, Zero Days)
- Indicators of Compromise (IOC) (Hashed, URLs, IPs)
- Auffälligkeiten im Dark Web (Accounts, Foren etc.)
- 3rd Party Risiken, Ratings, Auffälligkeiten, Leaks, Erpressungen
- Veränderungen in der externen Angriffsfläche
- Threat Hunting Kampagnen (Yara Rules etc.)
- Registration von verdächtigen Domains (Typosquatting)

Stakeholder

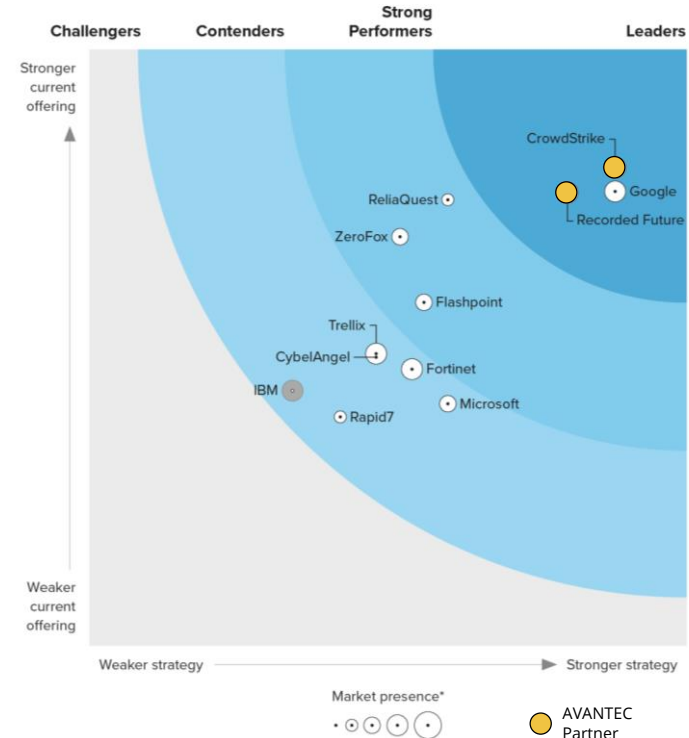
1	4	7	9	<input type="checkbox"/>
4	5	7	9	<input type="checkbox"/>
2	3	5	8	<input type="checkbox"/>
2	4	6	8	<input type="checkbox"/>
2	3	8	<input type="checkbox"/>	<input type="checkbox"/>
2	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	10	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Quellen & Marktübersicht

Gängige Informationsquellen

- **Intern**
 - Security Incident Daten
 - Security Analytics / SIEM / Logs
- **Interessensgruppen**
 - Industrie Gruppen, ISACs
 - Austausch mit Peers
- **Öffentlich**
 - Internet, News, Foren, Soziale Netzwerke
 - Freie Feeds, IP, Domain, URL Listen etc.
- **Regierungsnahe**
 - Nationale Gruppen, NCSC
 - Internationale Gruppen, Enisa, CISA
- **Kommerziell**
 - Threat Intelligence Anbieter/Services
 - Recorded Future, CrowdStrike etc.

Forrester Wave Q3 2023



Threat Intelligence Lifecycle

Feedback

Einholen von Stakeholder Feedback, kontinuierliche Anpassung & Verbesserung der Threat Intelligence

Integration in Prozesse

Integration der Threat Intelligence in die relevanten (Entscheidungs-) Prozesse, Einleitung von Massnahmen

Bereitstellung Intelligence

Aufbereitung in den Formaten die für die Stakeholder definiert wurden & Kommunikation auf den vereinbarten Kanälen



Anforderungen

Erarbeitung der Anforderungen, Definition der relevanten Bereiche, Fragestellungen, Stakeholder, Art der Information, Intervall, Format

Informationsbeschaffung

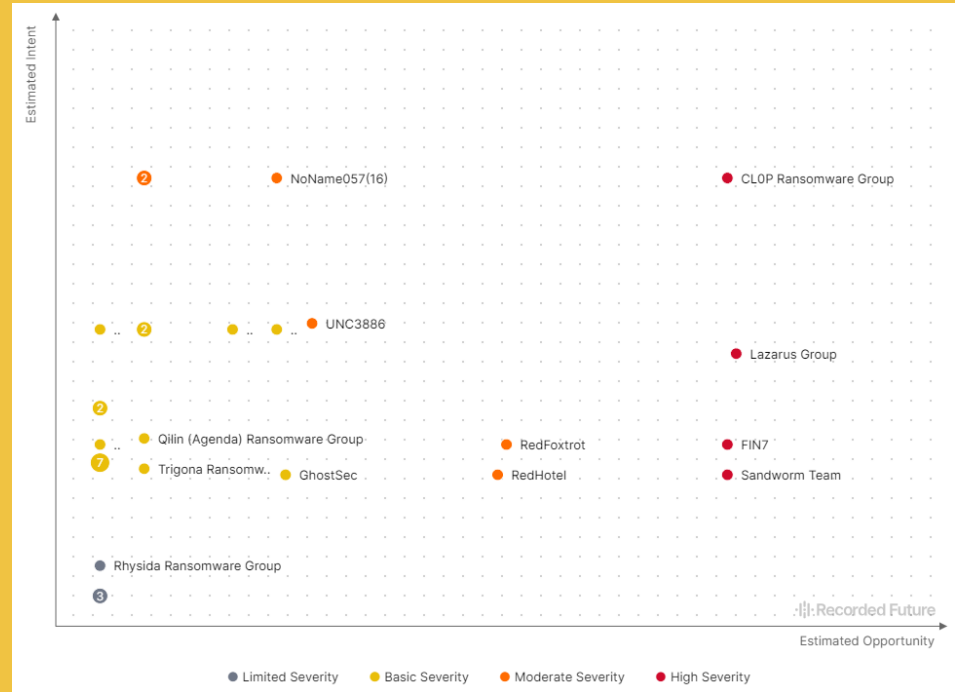
Auswahl der Quellen & Sammlung der benötigten Informationen für die Erfüllung der Anforderungen

Informationsverarbeitung

Verarbeitung & Analyse der Informationen zur Findung der Antworten auf die definierten Fragestellungen

Beispiel Threat Landscape

Welche Angreifergruppen sind in unserer Region & in der Finanzindustrie aktiv?

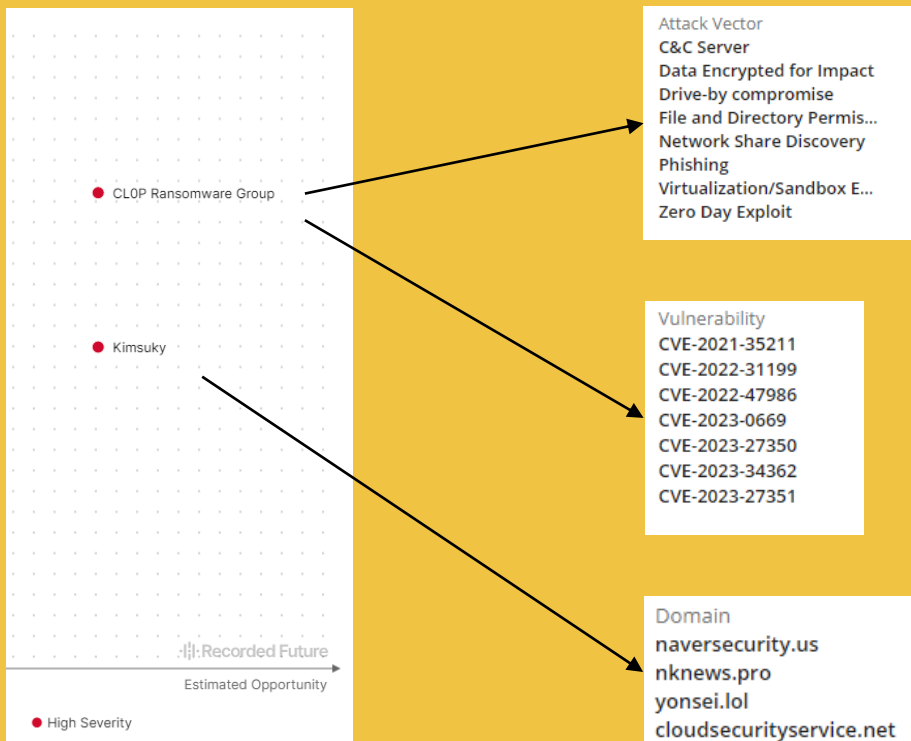


Beispiel Threat Landscape

Welche Angreifer
Gruppen sind in
unserer Region &
in der Fertigungs-
industrie aktiv?



Beispiel Threat Landscape



Welche
Angriffsvektoren
werden eingesetzt?

Werden spezifische
Schwachstellen
ausgenutzt?

Gibt es Indicators of
Compromise?

Technical Intelligence

Recorded Future

DOMAIN

xbox-ms-store-debug.com

Notes	2 Insikt Group Notes
References	1 000+
First Reference	Nov 21, 2020
Latest Reference	Jan 2, 2024
Recorded Future Community	Domain

MALICIOUS RISK SCORE

8 of 53 Risk Rules Triggered

Show recent events or cyber events

Recorded Future AI Insights

Narrative View

The domain **xbox-ms-store-debug.com** has been identified as a threat in multiple instances. It has been observed to be a malware site domain that leads to malicious content such as executables, drive-by infection sites, malicious scripts, viruses, trojans, or code. Additionally, it is suspected to be a **phishing URL/domain** that may be utilized in **phishing campaigns**. There have been reports of its association with the **SDBBot CC server** and the **TA505 group**. It has also been mentioned in relation to the **CLOP Ransomware Operation**. The domain has been detected exhibiting malicious behavior and has been flagged by **Bitdefender**. These observations highlight the potential cybersecurity risks associated with **xbox-ms-store-debug.com**.

Generated based on 8 Risk Rules | Analyst: Christian Grob

Share feedback?

TRIGGERED RISK RULES

Learn More

- Recently Detected Malware Operation** • 1 sighting on 1 source
External Sensor Data Analysis. **xbox-ms-store-debug.com** is observed to be a **malware site domain** that navigates to malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, or code.
- Recently Suspected Phishing Techniques** • 1 sighting on 1 source
External Sensor Data Analysis. **xbox-ms-store-debug.com** is suspected to be a **phishing URL/Domain** that may be used in phishing campaigns.
- Historically Detected Malware Operation** • 31 sightings on 2 sources
External Sensor Data Analysis, Bitdefender. **xbox-ms-store-debug.com** is observed to be a **malware site domain** that navigates to malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, or code.
- Historically Suspected Phishing Techniques** • 13 sightings on 1 source
External Sensor Data Analysis. **xbox-ms-store-debug.com** is suspected to be a **phishing URL/Domain** that may be used in phishing campaigns.
- Historically Reported by Insikt Group** • 2 sightings on 1 source
Insikt Group. 2 reports including An Overview of FIN11's CLOP Ransomware Operation. Most recent link (Jan 13, 2021): <https://app.recordedfuture.com/portal/analyst-note/doc:g7zMAY>
- Historically Reported as a Defanged DNS Name** • 2 sightings on 2 sources
@tbarabosch, @AdamTheAnalyst. Most recent tweet: Is the latest #SDBBot CC server xbox-ms-store-debug[.]com (89.40.206.124) really still up and running? It seems to respond correctly to #SDBBot traffic as of now. Be sure to block it! #TA505. Most recent link (Jan 12, 2021): <https://twitter.com/tbarabosch/status/1348973312089731072>
- Historically Suspected Malware Operation** • 1 sighting on 1 source
Bitdefender. Detected malicious behavior from an endpoint agent via global telemetry. Last observed on Apr 4, 2021.
- Historically Reported in Threat List** • Previous sightings on 1 source
Recorded Future Analyst Community Trending Indicators. Observed between Nov 18, 2023, and Nov 18, 2023.

SCREENSHOTS

URL <https://xbox-ms-store-debug.com/> Image Actions

```

"subject": [REDACTED],
"dumps": [
  {
    "name": "Stealer Malware Logs 2023-08-31",
    "description": "This credential data was derived from stealer malware logs.",
    "downloaded": "2023-09-18T16:44:43.666Z",
    "compromise": {
      "exfiltration_date": "2023-08-31T19:35:00.000Z",
      "os": "Windows 10 Enterprise 64 Bit",
      "os_username": [REDACTED],
      "malware_file": "C:\\FRST\\taskhostw.exe",
      "computer_name": "DESKTOP-6000BHN",
      "antivirus": [
        "Windows Defender"
      ]
    },
    "infrastructure": {
      "ip": [REDACTED]
    },
    "location": {
      "country": "AT"
    }
  }
],
"first_downloaded": "2023-09-18T16:44:43.663Z",
"latest_downloaded": "2023-09-18T16:44:43.666Z",
"exposed_secret": {
  "type": "clear",
  "hashes": [
    {
      "algorithm": "SHA1",
      "hash_prefix": "913c"
    },
    {
      "algorithm": "SHA256",
      "hash_prefix": "ddcf"
    },
    {
      "algorithm": "NTLM",
      "hash_prefix": "02d0"
    },
    {
      "algorithm": "MD5",
      "hash_prefix": "f4bc"
    }
  ]
}

```

Username

Infection details

Credential age

MD5, SHA1,
SHA256 and NTLM
Hashes

```

"details": {
  "properties": [
    "Letter",
    "Number",
    "UpperCase",
    "LowerCase",
    "AtLeast12Characters"
  ],
  "clear_text_hint": "DN"
},
"effectively_clear": true
},
"compromise": {
  "exfiltration_date": "2023-08-31T19:35:00.000Z"
},
"authorization_service": {
  "url": "https://secure.[REDACTED]/",
  "domain": [REDACTED],
  "fqdn": "secure[REDACTED]",
  "technology": [],
  "protocols": [
    "https"
  ]
}
},
"malware_family": {
  "name": "Dark Crystal RAT",
  "id": "ZEqKiv"
}

```

Password Properties

Login URL

Malware Family

```

"subject": ██████████
"dumps": [
  {
    "name": "Stealer Malware Logs 2023-06-11",
    "description": "This credential data was derived from stealer malware logs. These logs are
"downloaded": "2023-06-12T12:26:50.996Z",
    "compromise": {
      "exfiltration_date": "2023-06-11T13:44:33.000Z",
      "os": "Windows 10 Home Single Language [x64]",
      "os_username": ██████████,
      "malware_file": "C:\\Users\\████████\\AppData\\Local\\Programs\\NvNode\\Speech\\dwm.exe",
      "timezone": "UTC-06:00",
      "computer_name": ██████████
    },
    "infrastructure": {
      "ip": ██████████
    },
    "location": {
      "country": "MX"
    }
  },
  {
    "first_downloaded": "2023-06-12T12:26:50.996Z",
    "latest_downloaded": "2023-06-12T12:26:50.996Z",
    "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"
        }
      ]
    }
  }
]

```

Username

Infection details

Credential age

MD5, SHA1,
SHA256 and NTLM
Hashes

```

"details": {
  "properties": [
    "Letter",
    "Number",
    "UpperCase",
    "LowerCase",
    "AtLeast10Characters"
  ],
  "clear_text_hint": "Je"
},
"effectively_clear": true
},
"compromise": {
  "exfiltration_date": "2023-06-11T13:44:33.000Z"
},
"authorization_service": {
  "url": "https://\████████\vpn\tmlindex.html",
  "domain": "████████.com",
  "fqdn": "auth████████.com",
  "technology": [
    {
      "name": "Citrix NetScaler Access Gateway",
      "id": "Qtqzc7",
      "category": "CAfZv"
    },
    {
      "name": "VPN",
      "id": "CAfZv"
    }
  ]
},
"protocols": [
  "https"
],
"malware_family": {
  "name": "Vidar",
  "id": "YuDlEm"
},
"cookies": [
  {
    "dns": ██████████,
    "name": "_ga",
    "http": true,
    "expiration": "2024-06-07T17:32:58.000Z",
    "secure": true
  },
  {
    "dns": ██████████,
    "name": "_gid",
    "http": true,
    "expiration": "2023-05-05T17:32:58.000Z",
    "secure": true
  }
]

```

Password Properties

Login URL

Malware Family

Cookies

Vulnerability Intelligence

Recorded Future

VULNERABILITY in Microsoft Skype For Business Server

CVE-2023-41763

Notes 2 Inskit Group Notes
References 1 000+
First Reference Sep 1, 2023
Latest Reference Jan 11, 2024
Curated ★
Recorded Future Community Vulnerability

Used in List [CISA Known Exploited Vulnerabilities Catalog](#)

Affected Products 1 of 1
[Microsoft Skype For Business Server](#)
[Show All Versions](#)

89
CRITICAL RISK SCORE
5 of 23 Risk Rules Triggered

Show [recent events](#) or [cyber events](#)

Recorded Future AI Insights Narrative View

CVE-2023-41763 is a vulnerability that has been reported by Microsoft and has caught the attention of threat intelligence analysts. The vulnerability is related to Microsoft Skype for Business and involves **privilege escalation**. It has been included in the CISA Known Exploited Vulnerabilities Catalog, indicating that it has been actively exploited in the wild. As a vulnerability analyst responsible for patch management, it is highly recommended to prioritize patching this vulnerability as soon as possible. Failure to do so could potentially expose your company's assets to unauthorized access and compromise. It is crucial to follow the vendor's instructions for applying mitigations or consider discontinuing the use of the affected product if no mitigations are available.

Generated based on 5 Risk Rules | Analyst: Christian Grob Share feedback?

TRIGGERED RISK RULES

Learn More

Currently Triggered Risk Rules

Exploited in the Wild by Malware • 1 sighting on 1 source
CISA Known Exploited Vulnerabilities Catalog. Microsoft Skype for Business Privilege Escalation Vulnerability from vendor Microsoft. The recommended action is to apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Added Oct 10, 2023.
[Security Control Feeds: Exploits in the Wild](#) • [Learn More](#)

Vendor Severity: Medium • 1 sighting on 1 source
Recorded Future Vulnerability Analysis via National Vulnerability Database. CVSS v3.1 Score (5.3) calculated using Microsoft-reported CVSS Base Score (5.3) and Recorded Future Temporal Metrics. Base vector string: CVSS:3.1(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N. Temporal vector string: E:H/RLX/RCC. Most recent link (Oct 10, 2023): <https://nvd.nist.gov/vuln/detail/CVE-2023-41763>

Historically Linked to Malware • 233 sightings on 19 sources including
Malware Analysis News and Indicators Latest Posts, Codebook, Mastodon, Check Point Research, SOCRadar Cyber Intelligence. 9 related malware families including Shellbot, Denial of Service, Denial-of-Service, Offensive Security Tools (OST), DDOS Toolkit. Most recent tweet: Rapid reset: Ddos attacks rise: october 2023 patch tuesday has arrived (CVE-2023-36563, CVE-2023-41763, CVE-2023-44487) - First hackers news <https://t.co/hjeBMstPKA> <https://t.co/Kjn8Eqnh1Y>. Most recent link (Oct 13, 2023): https://twitter.com/Info_FHNews/statuses/1712709457107431521

Summary note for CVE-2023-41763 • Informational
Numerous sources confirmed exploitation in the wild. The intelligence was collected from social media. A threat actor created a PoC internally. The Admiralty score was A1.
Source: [Cyber Threat Cognitive Intelligence \(CTCI\)](#) [Expand Full Note](#)



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



Vulnerability 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 Intel Services



Threat Intelligence

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



Dark Web Monitoring

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

Kontakt

AVANTEC AG
Christian Grob
Head Security Services

+41 44 457 13 13
c.grob@avantec.ch



<https://www.linkedin.com/in/christian-grob-34529557>



<https://www.tec-bite.ch/author/christian-grob/>

