

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240525



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>13</b>
4.1 Exploits der letzten 5 Tage . . . . .	13
4.2 0-Days der letzten 5 Tage . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>22</b>
5.0.1 Déjà-vu: BreachForum <i>schon wieder</i> offline, zweiter Admin verhaftet . . . . .	22
<b>6 Cyberangriffe: (Mai)</b>	<b>23</b>
<b>7 Ransomware-Erpressungen: (Mai)</b>	<b>24</b>
<b>8 Quellen</b>	<b>41</b>
8.1 Quellenverzeichnis . . . . .	41
<b>9 Impressum</b>	<b>43</b>

## 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Windows Server 2019: Aktualisiertes Sicherheitsupdate behebt Installationsfehler***

Das Sicherheitsupdate für Windows Server 2019 schlug mit den Fehlernummern 0x800f0982 und 0x80004005 fehl. Ein aktualisiertes Update ist verfügbar.

- [Link](#)

---

#### ***GitLab: Accountübernahme nach 1-Klick-Attacke möglich***

Mehrere Sicherheitslücken in GitLab gefährden Systeme. Gegen mögliche Attacken gerüstete Versionen stehen zum Download bereit.

- [Link](#)

---

#### ***Google Chrome: Vierte bereits missbrauchte Zero-Day-Lücke in zwei Wochen***

Google schließt eine Zero-Day-Lücke im Chrome-Webbrowser, die bereits angegriffen wird. Die vierte in zwei Wochen.

- [Link](#)

---

#### ***Workaround vonnöten: Kritische Lücken bedrohen Ivanti Endpoint Manager***

Gegen mögliche Schadcode-Attacken gerüstete Ivanti-EPM-Versionen lassen noch auf sich warten. Bislang gibt es nur einen Hot Patch für eine Version.

- [Link](#)

---

#### ***Sicherheitsupdates VMware: Schadcode kann aus VM ausbüchsen***

Admins sollten zeitnah mehrere Sicherheitspatches für diverse VMware-Produkte installieren.

- [Link](#)

---

#### ***Cisco: Root-Zugriff durch SQL-Injection-Lücke in Firepower möglich***

Cisco warnt vor Sicherheitslücken in ASA- und Firepower-Appliances. Angreifer können mit SQL-Injection Firepower-Geräte kompromittieren.

- [Link](#)

---

#### ***Patchday: Atlassian rüstet Data Center gegen Schadcode-Attacken***

Admins sollten aus Sicherheitsgründen unter anderem Jira Data Center and Server und Service Management auf den aktuellen Stand bringen.

- [Link](#)

---

***DoS-Lücke in Loggingtool Fluent Bit mit 13 Milliarden Downloads geschlossen***

Sicherheitsforscher warnen vor einer kritischen Sicherheitslücke in Fluent Bit. Das Loggingtool kommt unter anderem bei vielen Cloudanbietern zum Einsatz.

- [Link](#)

—

***Kritische Lücke gewährt Angreifern Zugriff auf Veeam Backup Enterprise Manager***

In einer aktuellen Version von Veeam Backup & Replication haben die Entwickler mehrere Schwachstellen geschlossen.

- [Link](#)

—

***Sicherheitsupdate: DoS-Lücken in Netzwerkanalysetool Wireshark geschlossen***

In der aktuellen Version von Wireshark haben die Entwickler drei Sicherheitslücken geschlossen und mehrere Bugs gefixt.

- [Link](#)

—

### 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

#### 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-7028	0.959520000	0.994640000	<a href="#">Link</a>
CVE-2023-6553	0.909510000	0.988380000	<a href="#">Link</a>
CVE-2023-5360	0.965120000	0.995960000	<a href="#">Link</a>
CVE-2023-4966	0.967100000	0.996510000	<a href="#">Link</a>
CVE-2023-48795	0.959940000	0.994740000	<a href="#">Link</a>
CVE-2023-47246	0.946220000	0.992390000	<a href="#">Link</a>
CVE-2023-46805	0.965580000	0.996130000	<a href="#">Link</a>
CVE-2023-46747	0.971160000	0.997900000	<a href="#">Link</a>
CVE-2023-46604	0.922790000	0.989480000	<a href="#">Link</a>
CVE-2023-4542	0.909770000	0.988400000	<a href="#">Link</a>
CVE-2023-43208	0.963060000	0.995390000	<a href="#">Link</a>
CVE-2023-43177	0.964020000	0.995670000	<a href="#">Link</a>
CVE-2023-42793	0.970940000	0.997770000	<a href="#">Link</a>
CVE-2023-41265	0.914120000	0.988730000	<a href="#">Link</a>
CVE-2023-39143	0.953670000	0.993600000	<a href="#">Link</a>
CVE-2023-38646	0.913020000	0.988650000	<a href="#">Link</a>
CVE-2023-38205	0.922000000	0.989360000	<a href="#">Link</a>
CVE-2023-38203	0.970370000	0.997550000	<a href="#">Link</a>
CVE-2023-38146	0.905210000	0.988050000	<a href="#">Link</a>
CVE-2023-38035	0.975060000	0.999830000	<a href="#">Link</a>
CVE-2023-36845	0.966630000	0.996360000	<a href="#">Link</a>
CVE-2023-3519	0.911860000	0.988590000	<a href="#">Link</a>
CVE-2023-35082	0.967320000	0.996600000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996890000	<a href="#">Link</a>
CVE-2023-34993	0.966440000	0.996310000	<a href="#">Link</a>
CVE-2023-34960	0.933140000	0.990670000	<a href="#">Link</a>
CVE-2023-34634	0.918830000	0.989120000	<a href="#">Link</a>
CVE-2023-34362	0.959160000	0.994570000	<a href="#">Link</a>
CVE-2023-34039	0.935790000	0.990950000	<a href="#">Link</a>
CVE-2023-3368	0.932830000	0.990630000	<a href="#">Link</a>
CVE-2023-33246	0.972850000	0.998620000	<a href="#">Link</a>
CVE-2023-32315	0.974090000	0.999270000	<a href="#">Link</a>
CVE-2023-32235	0.914550000	0.988760000	<a href="#">Link</a>
CVE-2023-30625	0.948870000	0.992860000	<a href="#">Link</a>
CVE-2023-30013	0.963050000	0.995390000	<a href="#">Link</a>
CVE-2023-29300	0.969500000	0.997240000	<a href="#">Link</a>
CVE-2023-29298	0.948030000	0.992690000	<a href="#">Link</a>
CVE-2023-28771	0.914030000	0.988730000	<a href="#">Link</a>
CVE-2023-28432	0.938730000	0.991300000	<a href="#">Link</a>
CVE-2023-28121	0.941330000	0.991620000	<a href="#">Link</a>
CVE-2023-27524	0.970950000	0.997770000	<a href="#">Link</a>
CVE-2023-27372	0.973760000	0.999050000	<a href="#">Link</a>
CVE-2023-27350	0.971070000	0.997830000	<a href="#">Link</a>
CVE-2023-26469	0.942400000	0.991750000	<a href="#">Link</a>
CVE-2023-26360	0.962980000	0.995370000	<a href="#">Link</a>
CVE-2023-26035	0.969280000	0.997180000	<a href="#">Link</a>
CVE-2023-25717	0.956860000	0.994140000	<a href="#">Link</a>
CVE-2023-25194	0.967170000	0.996530000	<a href="#">Link</a>
CVE-2023-2479	0.965320000	0.996050000	<a href="#">Link</a>
CVE-2023-24489	0.974200000	0.999330000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.932080000	0.990530000	<a href="#">Link</a>
CVE-2023-23397	0.922480000	0.989430000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995450000	<a href="#">Link</a>
CVE-2023-22527	0.974590000	0.999550000	<a href="#">Link</a>
CVE-2023-22518	0.962670000	0.995280000	<a href="#">Link</a>
CVE-2023-22515	0.973130000	0.998750000	<a href="#">Link</a>
CVE-2023-21839	0.959090000	0.994540000	<a href="#">Link</a>
CVE-2023-21554	0.959390000	0.994630000	<a href="#">Link</a>
CVE-2023-20887	0.963500000	0.995520000	<a href="#">Link</a>
CVE-2023-1698	0.907920000	0.988280000	<a href="#">Link</a>
CVE-2023-1671	0.969090000	0.997110000	<a href="#">Link</a>
CVE-2023-0669	0.969690000	0.997290000	<a href="#">Link</a>

### 3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 24 May 2024

#### **[UPDATE] [hoch] Node.js: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 24 May 2024

#### **[UPDATE] [hoch] ILIAS: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in ILIAS ausnutzen, um beliebigen Code auszuführen oder einen Cross-Site Scripting (XSS) Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024



**[UPDATE] [hoch] zlib: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in zlib ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Red Hat JBoss A-MQ: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss A-MQ ausnutzen,

um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Podman: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Podman ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Google Chrome/Microsoft Edge: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome/Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio und Microsoft .NET Framework ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 24 May 2024

**[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- [Link](#)

—

Fri, 24 May 2024

**[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/25/2024	[openSUSE 15 Security Update : qt6-networkauth (openSUSE-SU-2024:0138-1)]	critical
5/24/2024	[TensorFlow < 2.9.3 Multiple Vulnerabilities]	critical
5/24/2024	[Debian dsa-5697 : chromium - security update]	critical
5/25/2024	[Fedora 40 : crosswords / libipuz (2024-e4717532c4)]	high
5/25/2024	[Fedora 39 : perl-Email-MIME (2024-38fb541a75)]	high
5/25/2024	[Fedora 40 : perl-Email-MIME (2024-032e16360b)]	high
5/25/2024	[Fedora 40 : mingw-libxml2 (2024-9ffc6cc7bf)]	high
5/25/2024	[Fedora 39 : dotnet7.0 (2024-3136a71490)]	high
5/25/2024	[Fedora 39 : crosswords / libipuz (2024-4d785e16a2)]	high
5/25/2024	[Fedora 39 : mingw-libxml2 (2024-4862425658)]	high
5/25/2024	[SUSE SLES15 Security Update : libfastjson (SUSE-SU-2024:1775-1)]	high
5/25/2024	[SUSE SLES15 Security Update : python3 (SUSE-SU-2024:1774-1)]	high
5/25/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ucode-intel (SUSE-SU-2024:1771-1)]	high
5/24/2024	[Oracle Linux 9 : tomcat (ELSA-2024-3307)]	high

Datum	Schwachstelle	Bewertung
5/24/2024	[MongoDB 5.0.x < 5.0.25 / 6.0.x < 6.0.14 / 7.0.x < 7.0.6 Improper Input Validation (SERVER-85263)]	high
5/24/2024	[Ivanti Connect Secure 9.x / 22.x XSS Vulnerability]	high
5/24/2024	[Ivanti Policy Secure 22.x XSS Vulnerability]	high
5/24/2024	[Foxit PDF Editor < 2024.2.2 Vulnerability]	high
5/24/2024	[Foxit PDF Reader < 2024.2.2 Vulnerability]	high
5/24/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0137-1)]	high
5/24/2024	[Jenkins plugins Multiple Vulnerabilities (2024-05-24)]	high
5/24/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2024:1770-1)]	high
5/24/2024	[SUSE SLES15 / openSUSE 15 Security Update : python-sqlparse (SUSE-SU-2024:1767-1)]	high
5/24/2024	[Oracle Linux 7 : libreoffice (ELSA-2024-3304)]	high
5/24/2024	[Atlassian Confluence 5.2 < 7.19.22 / 7.20.x < 8.5.9 / 8.6.x < 8.9.1 RCE (CONFSERVER-95832)]	high
5/24/2024	[F5 Networks BIG-IP : Apache HTTPD vulnerability (K000139764)]	high
5/24/2024	[F5 Networks BIG-IP : Libexpat vulnerability (K000139525)]	high
5/23/2024	[RHEL 8 : gdk-pixbuf2 (RHSA-2024:3341)]	high
5/23/2024	[RHEL 8 : xorg-x11-server-Xwayland (RHSA-2024:3343)]	high
5/23/2024	[RHEL 8 : glibc (RHSA-2024:3344)]	high
5/23/2024	[RHEL 8 / 9 : OpenShift Container Platform 4.13.42 (RHSA-2024:2877)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 24 May 2024

#### **Jcow Social Network Cross Site Scripting**

Jcow Social Networking versions 14.2 up to 16.2.1 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 24 May 2024

#### **4BRO Insecure Direct Object Reference / API Information Exposure**

4BRO versions prior to 2024-04-17 suffer from insecure direct object reference and API information disclosure vulnerabilities.

- [Link](#)

—

” “Fri, 24 May 2024

#### **Debezium UI 2.5 Credential Disclosure**

Debezium UI version 2.5 suffers from a credential disclosure vulnerability.

- [Link](#)

—

” “Thu, 23 May 2024

#### **FleetCart 4.1.1 Information Disclosure**

FleetCart version 4.1.1 suffers from an information leakage vulnerability.

- [Link](#)

—

” “Wed, 22 May 2024

#### **NorthStar C2 Cross Site Scripting / Code Execution**

NorthStar C2, prior to commit 7674a44 on March 11 2024, contains a vulnerability where the logs page is vulnerable to a stored cross site scripting issue. An unauthenticated user can simulate an agent registration to cause the cross site scripting attack and take over a users session. With this access, it is then possible to run a new payload on all of the NorthStar C2 compromised hosts (agents), and kill the original agent. Successfully tested against NorthStar C2 commit e7fdce148b6a81516e8aa5e5e037acd082611f73 running on Ubuntu 22.04. The agent was running on Windows 10 19045.

- [Link](#)

—

” “Wed, 22 May 2024

***AVideo WWBNIndex Plugin Unauthenticated Remote Code Execution***

This Metasploit module exploits an unauthenticated remote code execution vulnerability in the WWBNIndex plugin of the AVideo platform. The vulnerability exists within the submitIndex.php file, where user-supplied input is passed directly to the require() function without proper sanitization. By exploiting this, an attacker can leverage the PHP filter chaining technique to execute arbitrary PHP code on the server. This allows for the execution of commands and control over the affected system. The exploit is particularly dangerous because it does not require authentication, making it possible for any remote attacker to exploit this vulnerability.

- [Link](#)

—

” “Wed, 22 May 2024

***Chat Bot 1.0 SQL Injection***

Chat Bot version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 21 May 2024

***CHAOS 5.0.8 Cross Site Scripting / Remote Command Execution***

CHAOS version 5.0.8 is a free and open-source Remote Administration Tool that allows generated binaries to control remote operating systems. The web application contains a remote command execution vulnerability which can be triggered by an authenticated user when generating a new executable. The web application also contains a cross site scripting vulnerability within the view of a returned command being executed on an agent.

- [Link](#)

—

” “Tue, 21 May 2024

***Joomla 4.2.8 Information Disclosure***

Joomla versions 4.2.8 and below remote unauthenticated information disclosure exploit.

- [Link](#)

—

” “Tue, 21 May 2024

***Nethserver 7 / 8 Cross Site Scripting***

The NethServer module installed as WebTop, produced by Sonicle, is affected by a stored cross site scripting vulnerability due to insufficient input sanitization and output escaping which allows an attacker to store a malicious payload as to execute arbitrary web scripts or HTML. Versions 7 and 8 are affected.

- [Link](#)

—

” “Tue, 21 May 2024

**PowerVR DevmemIntChangeSparse2() Dangling Page Table Entry**

PowerVR suffers from a wrong order of operations in DevmemIntChangeSparse2() that leads to a temporarily dangling page table entry.

- [Link](#)

—

” “Tue, 21 May 2024

\*\*\*PowerVR \_UnrefAndMaybeDestroy() Use-After-Free\*\*\*

PowerVR suffers from a use-after-free vulnerability in \_UnrefAndMaybeDestroy().

- [Link](#)

—

” “Tue, 21 May 2024

**Arm Mali r45p0 Broken State Use-After-Free**

Arm Mali versions since r45p0 suffer from a broken KBASE\_USER\_BUF\_STATE\_\* state machine for userspace mappings that can lead to a use-after-free condition.

- [Link](#)

—

” “Mon, 20 May 2024

**Tenant Limited 1.0 SQL Injection**

Tenant Limited version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 20 May 2024

**WordPress XStore Theme 9.3.8 SQL Injection**

WordPress XStore theme version 9.3.8 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 20 May 2024

**Apache OFBiz 18.12.12 Directory Traversal**

Apache OFBiz versions 18.12.12 and below suffer from a directory traversal vulnerability.

- [Link](#)

—

” “Mon, 20 May 2024

**Backdrop CMS 1.27.1 Remote Command Execution**

Backdrop CMS version 1.27.1 suffers from a remote command execution vulnerability.

- [Link](#)

—

” “Mon, 20 May 2024

**PopojiCMS 2.0.1 Remote Command Execution**



PopojiCMS version 2.0.1 remote command execution exploit that requires an administrative login. This vulnerability was originally reported by tmrswrr in November of 2023.

- [Link](#)

—

” “Mon, 20 May 2024

***Rocket LMS 1.9 Cross Site Scripting***

Rocket LMS version 1.9 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 16 May 2024

***GhostRace: Exploiting And Mitigating Speculative Race Conditions***

This archive is a GhostRace proof of concept exploit exemplifying the concept of a speculative race condition in a step-by-step single-threaded fashion. Coccinelle scripts are used to scan the Linux kernel version 5.15.83 for Speculative Concurrent Use-After-Free (SCUAF) gadgets.

- [Link](#)

—

” “Wed, 15 May 2024

***Cacti 1.2.26 Remote Code Execution***

Cacti versions 1.2.26 and below suffer from a remote code execution execution vulnerability in import.php.

- [Link](#)

—

” “Wed, 15 May 2024

***SAP Cloud Connector 2.16.1 Missing Validation***

SAP Cloud Connector versions 2.15.0 through 2.16.1 were found to happily accept self-signed TLS certificates between SCC and SAP BTP.

- [Link](#)

—

” “Wed, 15 May 2024

***Zope 5.9 Command Injection***

Zope version 5.9 suffers from a command injection vulnerability in /utilities/mkwsgiinstance.py.

- [Link](#)

—

” “Tue, 14 May 2024

***CrushFTP Directory Traversal***

CrushFTP versions prior to 11.1.0 suffers from a directory traversal vulnerability.

- [Link](#)

—

” “Tue, 14 May 2024

***TrojanSpy.Win64.EMOTET.A MVID-2024-0684 Code Execution***

TrojanSpy.Win64.EMOTET.A malware suffers from a code execution vulnerability.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Fri, 24 May 2024

***ZDI-24-515: NETGEAR ProSAFE Network Management System UploadServlet Unrestricted File Upload Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-514: Ivanti Endpoint Manager GetVulnerabilitiesDataTable SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-513: Ivanti Endpoint Manager GetLogFileRulesNameUniqueSQL SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-512: Ivanti Endpoint Manager GetLogFileRulesSQL SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-511: Ivanti Endpoint Manager GetRulesetsSQL SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-510: Ivanti Endpoint Manager GetDBPatchProducts SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-509: Ivanti Endpoint Manager GetDBPatches SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-508: Ivanti Endpoint Manager RecordBrokenApp SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-507: Ivanti Endpoint Manager RecordGoodApp SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-506: Ivanti Endpoint Manager GetDBVulnerabilities SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-505: Ivanti Endpoint Manager RecordGoodApp SQL Injection Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 24 May 2024

***ZDI-24-504: Ivanti Avalanche FileStoreConfig Unrestricted File Upload Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 23 May 2024

***ZDI-24-503: (Pwn2Own) TP-Link Omada ER605 Reliance on Security Through Obscurity Vulnerability***

- [Link](#)

—

” “Thu, 23 May 2024

***ZDI-24-502: (Pwn2Own) TP-Link Omada ER605 Buffer Overflow Remote Code Execution Vulnerability***

**lity**

- [Link](#)

—

” “Thu, 23 May 2024

**ZDI-24-501: (Pwn2Own) TP-Link Omada ER605 Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 23 May 2024

**ZDI-24-500: (Pwn2Own) TP-Link Omada ER605 Comexe DDNS Response Handling Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 23 May 2024

**ZDI-24-499: (Pwn2Own) TP-Link Omada ER605 PPTP VPN username Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-498: NETGEAR ProSAFE Network Management System UploadServlet Unrestricted File Upload Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-497: NETGEAR ProSAFE Network Management System Tomcat Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-496: NETGEAR ProSAFE Network Management System Default Credentials Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-495: (Pwn2Own) Microsoft Windows CLFS Integer Underflow Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-494: VMware Workstation SVGA Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-493: Adobe Acrobat Reader DC JPEG2000 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-492: Adobe Acrobat Pro DC AcroForm Annotation Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-491: WithSecure Elements Endpoint Protection Link Following Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-490: LAquis SCADA LGX Report Processing AddComboFile Path Traversal Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-489: LAquis SCADA LGX Report File Open Path Traversal Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-488: LAquis SCADA LGX Report TextFile Open Path Traversal Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

**ZDI-24-487: LAquis SCADA LGX Report STRING READFROMFILE Path Traversal Information Disclosure Vulnerability**

- [Link](#)

—

” “Wed, 22 May 2024

***ZDI-24-486: LAquis SCADA LGX Report STRING WRITETOFILE Path Traversal Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 22 May 2024

***ZDI-24-485: LAquis SCADA LGX Report TextFile OpenWithoutMemory Path Traversal Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 22 May 2024

***ZDI-24-484: LAquis SCADA LGX Report Table Save Path Traversal Remote Code Execution Vulnerability***

- [Link](#)

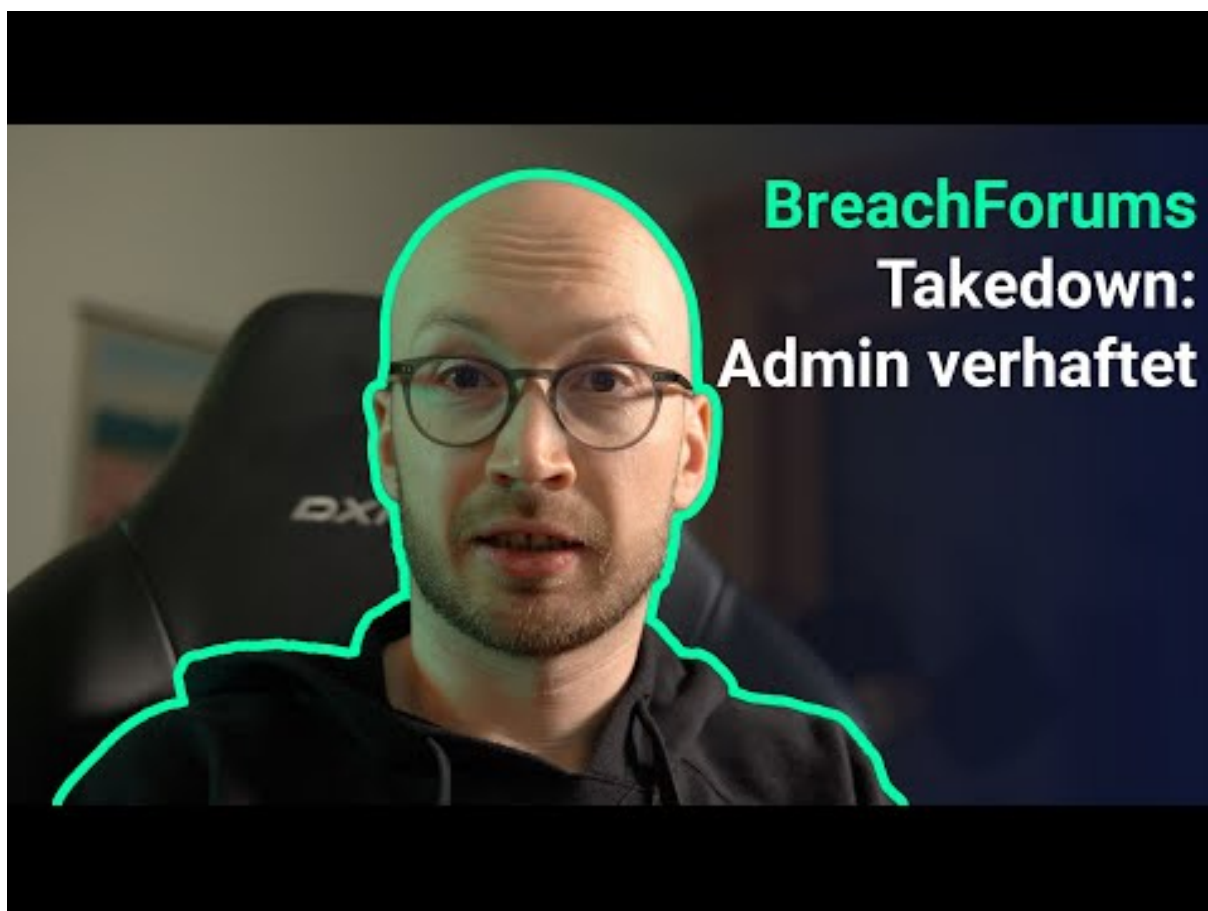
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Déjà-vu: BreachForum schon wieder offline, zweiter Admin verhaftet



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2024-05-22	Jumbo Group	[SGP]	<a href="#">Link</a>
2024-05-21	Le Cup (Centre Unique de Programmation)	[ITA]	<a href="#">Link</a>
2024-05-21	Top-Medien	[CHE]	<a href="#">Link</a>
2024-05-20	Hong Kong Institute of Contemporary Culture Lee Shau Kee School of Creativity	[HKG]	<a href="#">Link</a>
2024-05-17	AddComm	[NLD]	<a href="#">Link</a>
2024-05-16	American Radio Relay League (ARRL)	[USA]	<a href="#">Link</a>
2024-05-15	MediSecure	[AUS]	<a href="#">Link</a>
2024-05-15	Rockford Public Schools	[USA]	<a href="#">Link</a>
2024-05-15	Ranzijn	[NLD]	<a href="#">Link</a>
2024-05-15	Le Collège Ahuntsic	[CAN]	<a href="#">Link</a>
2024-05-15	Central Contra Costa Transit Authority (County Connection)	[USA]	<a href="#">Link</a>
2024-05-13	Universidad Complutense de Madrid	[ESP]	<a href="#">Link</a>
2024-05-13	L'aéroport et l'école de commerce de Pau	[FRA]	<a href="#">Link</a>
2024-05-13	First Nations Health Authority (FNHA)	[CAN]	<a href="#">Link</a>
2024-05-12	Christie's	[CHE]	<a href="#">Link</a>
2024-05-12	Travelite Holdings Ltd.	[SGP]	<a href="#">Link</a>
2024-05-12	Union Township School District	[USA]	<a href="#">Link</a>
2024-05-11	Wehrle-Werk AG	[DEU]	<a href="#">Link</a>
2024-05-08	Ascension Health	[USA]	<a href="#">Link</a>
2024-05-06	DocGo	[USA]	<a href="#">Link</a>
2024-05-06	Key Tronic Corporation	[USA]	<a href="#">Link</a>
2024-05-06	Trego County Lemke Memorial Hospital	[USA]	<a href="#">Link</a>
2024-05-05	Wichita	[USA]	<a href="#">Link</a>
2024-05-05	Université de Sienne	[ITA]	<a href="#">Link</a>



Datum	Opfer	Land	Information
2024-05-05	Concord Public Schools et Concord-Carlisle Regional School District	[USA]	<a href="#">Link</a>
2024-05-04	Regional Cancer Center (RCC)	[IND]	<a href="#">Link</a>
2024-05-03	Eucatex (EUCA4)	[BRA]	<a href="#">Link</a>
2024-05-03	Cégep de Lanaudière	[CAN]	<a href="#">Link</a>
2024-05-03	Coradix-Magnescan	[FRA]	<a href="#">Link</a>
2024-05-02	Umeå universitet	[SWE]	<a href="#">Link</a>
2024-05-02	Ewing Marion Kauffman School	[USA]	<a href="#">Link</a>
2024-05-01	Brandywine Realty Trust	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-25	[\$150.000]	blacksuit	<a href="#">Link</a>
2024-05-24	[bnsgroup.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-24	[Ipsotek LTD]	blacksuit	<a href="#">Link</a>
2024-05-24	[Vannguard Utility Partners]	akira	<a href="#">Link</a>
2024-05-24	[workscapes.com]	lockbit3	<a href="#">Link</a>
2024-05-24	[EMPIRECOMFORT.COM]	clap	<a href="#">Link</a>
2024-05-24	[kns.com]	lockbit3	<a href="#">Link</a>
2024-05-24	[colfax.k12.wi.us - \$150.000]	blacksuit	<a href="#">Link</a>
2024-05-24	[Sichuan Dowell Science and Technology Company Inc]	blacksuit	<a href="#">Link</a>
2024-05-24	[hiawathahomes]	blacksuit	<a href="#">Link</a>
2024-05-23	[valleylandtitleco.com]	lockbit3	<a href="#">Link</a>
2024-05-22	[umbrellaproperties.com PART2]	dispossessor	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-23	[brightwayconsultants.co.uk]	apt73	<a href="#">Link</a>
2024-05-23	[Nutec Group]	bianlian	<a href="#">Link</a>
2024-05-04	[United Urology Group]	ransomhouse	<a href="#">Link</a>
2024-05-23	[Hands TheFamilyHelpNetwork.ca]	incransom	<a href="#">Link</a>
2024-05-23	[iseta.fr (institut des Sciences de l'Environnement et des Territoires d'Annecy)]	ransomhub	<a href="#">Link</a>
2024-05-22	[ICC]	rhysida	<a href="#">Link</a>
2024-05-22	[Newman Ferrara]	akira	<a href="#">Link</a>
2024-05-22	[IZOMAT Praha]	akira	<a href="#">Link</a>
2024-05-22	[GRANVILLE FOOD CARE LIMITED]	akira	<a href="#">Link</a>
2024-05-22	[Richland City Hall]	incransom	<a href="#">Link</a>
2024-05-22	[Midwest Covenant Home]	incransom	<a href="#">Link</a>
2024-05-22	[First Nations Health Authority (fnha.local)]	incransom	<a href="#">Link</a>
2024-05-22	[Golden Acre]	qilin	<a href="#">Link</a>
2024-05-22	[Ryder Scott Co.]	play	<a href="#">Link</a>
2024-05-22	[Tri-state General Contractors]	play	<a href="#">Link</a>
2024-05-22	[Starostwo Powiatowe w Świebodzinie]	play	<a href="#">Link</a>
2024-05-22	[Aspire Tax]	play	<a href="#">Link</a>
2024-05-22	[The Louis G Freeman]	play	<a href="#">Link</a>
2024-05-22	[Experis Technology Group]	play	<a href="#">Link</a>
2024-05-22	[Anchorage Daily News]	play	<a href="#">Link</a>
2024-05-22	[RDI-USA]	play	<a href="#">Link</a>
2024-05-22	[Ardenbrook]	play	<a href="#">Link</a>
2024-05-22	[Visa Lighting]	play	<a href="#">Link</a>
2024-05-22	[Semicore Equipment]	play	<a href="#">Link</a>
2024-05-22	[Levin Porter Associates]	play	<a href="#">Link</a>
2024-05-22	[Critchfield & Johnston]	bianlian	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-21	[shamrocktradingcorp.com]	embargo	<a href="#">Link</a>
2024-05-21	[londondrugs.com]	lockbit3	<a href="#">Link</a>
2024-05-21	[schmittyyandsons.com]	lockbit3	<a href="#">Link</a>
2024-05-21	[ThrottleUp ]	ransomhub	<a href="#">Link</a>
2024-05-21	[ramfoam.com]	lockbit3	<a href="#">Link</a>
2024-05-21	[ALO diamonds]	8base	<a href="#">Link</a>
2024-05-21	[Brittany Horne ]	ransomhub	<a href="#">Link</a>
2024-05-20	[Aztec Services Group]	medusa	<a href="#">Link</a>
2024-05-20	[International Modern Hospital]	medusa	<a href="#">Link</a>
2024-05-20	[Heras ]	medusa	<a href="#">Link</a>
2024-05-21	[levian.com]	blackbasta	<a href="#">Link</a>
2024-05-21	[lactanet.ca]	blackbasta	<a href="#">Link</a>
2024-05-21	[mfgroup.it]	blackbasta	<a href="#">Link</a>
2024-05-21	[grupocadarso.com]	blackbasta	<a href="#">Link</a>
2024-05-21	[atlasoil.com]	blackbasta	<a href="#">Link</a>
2024-05-21	[trugreen.com]	blackbasta	<a href="#">Link</a>
2024-05-20	[Matadero de Gijón - Biogas energy plant - mataderodegijon.es]	ransomhub	<a href="#">Link</a>
2024-05-20	[American Clinical Solutions(acslabtest.com)]	ransomhub	<a href="#">Link</a>
2024-05-20	[ORIUX: Experts in Mobility ]	ransomhub	<a href="#">Link</a>
2024-05-20	[Jess-link Products]	hunters	<a href="#">Link</a>
2024-05-20	[MAH Machine]	bianlian	<a href="#">Link</a>
2024-05-20	[Marigin]	akira	<a href="#">Link</a>
2024-05-20	[GE Aerospace]	meow	<a href="#">Link</a>
2024-05-20	[Crooker]	8base	<a href="#">Link</a>
2024-05-20	[Embellir]	8base	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-20	[LEMKEN]	8base	<a href="#">Link</a>
2024-05-20	[California Highway Patrol (SVEL237.org)]	incransom	<a href="#">Link</a>
2024-05-20	[qualityplumbingassociates.com]	lockbit3	<a href="#">Link</a>
2024-05-18	[Regional Obstetrical Consultants]	incransom	<a href="#">Link</a>
2024-05-20	[Specialty Market Managers]	incransom	<a href="#">Link</a>
2024-05-20	[Sterling Transportation Services (sts.local)]	incransom	<a href="#">Link</a>
2024-05-20	[Continuing Healthcare Solutions (chs.local)]	incransom	<a href="#">Link</a>
2024-05-20	[schuettemetals.com]	cactus	<a href="#">Link</a>
2024-05-07	[allied-mechanical-services-inc]	incransom	<a href="#">Link</a>
2024-05-16	[Patriot Machine, Updated data leak.]	donutleaks	<a href="#">Link</a>
2024-05-18	[carcajou.fr]	lockbit3	<a href="#">Link</a>
2024-05-18	[equinoxinc.org]	lockbit3	<a href="#">Link</a>
2024-05-18	[unisi.it]	lockbit3	<a href="#">Link</a>
2024-05-18	[Widdop & Co.]	rhysida	<a href="#">Link</a>
2024-05-18	[Colégio Nova Dimensão]	arcusmedia	<a href="#">Link</a>
2024-05-18	[catiglass.com \$100.000]	blacksuit	<a href="#">Link</a>
2024-05-18	[Bluebonnet Nutrition]	bianlian	<a href="#">Link</a>
2024-05-18	[Center for Digestive Health]	bianlian	<a href="#">Link</a>
2024-05-18	[drmsusa.com]	incransom	<a href="#">Link</a>
2024-05-17	[WEICON]	medusa	<a href="#">Link</a>
2024-05-17	[County Connection]	medusa	<a href="#">Link</a>
2024-05-17	[Elm Grove]	medusa	<a href="#">Link</a>
2024-05-17	[Comwave ]	medusa	<a href="#">Link</a>
2024-05-17	[Mesopolys]	spacebears	<a href="#">Link</a>
2024-05-14	[Pittsburgh's Trusted Orthopaedic Surgeons]	donutleaks	<a href="#">Link</a>
2024-05-17	[Sullairargentina.com]	redransomware	<a href="#">Link</a>
2024-05-15	[www.belcherpharma.com]	underground	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-17	[orga-soft.de]	embargo	<a href="#">Link</a>
2024-05-17	[Houston Waste Solutions ]	ransomhub	<a href="#">Link</a>
2024-05-17	[Shyang Shin Bao Ind. Co., Ltd. (hereinafter referred to as "SSB")]	qilin	<a href="#">Link</a>
2024-05-17	[Vision Mechanical]	blacksuit	<a href="#">Link</a>
2024-05-08	[aharvey.nf.ca]	incransom	<a href="#">Link</a>
2024-05-17	[PRIMARYSYS.COM]	clop	<a href="#">Link</a>
2024-05-17	[Formosa Plastics USA]	hunters	<a href="#">Link</a>
2024-05-16	[Dean Lumber & Supply]	dragonforce	<a href="#">Link</a>
2024-05-16	[WindCom]	dragonforce	<a href="#">Link</a>
2024-05-17	[For sale. Contact through admin. \$100.000]	blacksuit	<a href="#">Link</a>
2024-05-17	[agranibank.org]	killsec	<a href="#">Link</a>
2024-05-17	[laxmicapital.com.np]	killsec	<a href="#">Link</a>
2024-05-16	[pricemodern.com]	lockbit3	<a href="#">Link</a>
2024-05-16	[OKUANT - okuant.com]	ransomhub	<a href="#">Link</a>
2024-05-16	[valleyjoist.com]	lockbit3	<a href="#">Link</a>
2024-05-16	[fulcrum.pro]	cactus	<a href="#">Link</a>
2024-05-16	[Insurance Agency Marketing Services]	moneymessage	<a href="#">Link</a>
2024-05-15	[Neovia]	snatch	<a href="#">Link</a>
2024-05-16	[Baeckerei-raddatz.de]	cloak	<a href="#">Link</a>
2024-05-14	[Colonial Surety Company ]	medusa	<a href="#">Link</a>
2024-05-16	[kauffmanschool.org]	lockbit3	<a href="#">Link</a>
2024-05-16	[ema-eda.com]	lockbit3	<a href="#">Link</a>
2024-05-16	[twpunionschools.org]	lockbit3	<a href="#">Link</a>
2024-05-16	[Chuo System Service Co.,Ltd ]	ransomhub	<a href="#">Link</a>
2024-05-16	[East Shore Sound]	ransomhub	<a href="#">Link</a>
2024-05-16	[thermalsolutionsllc.com]	threeam	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-16	[escriba.com.br]	threeam	<a href="#">Link</a>
2024-05-16	[RIO TECHNOLOGY]	arcusmedia	<a href="#">Link</a>
2024-05-16	[Egyptian Sudanese]	arcusmedia	<a href="#">Link</a>
2024-05-15	[Consulting Radiologists]	qilin	<a href="#">Link</a>
2024-05-15	[FIAB SpA]	qilin	<a href="#">Link</a>
2024-05-15	[project sold]	monti	<a href="#">Link</a>
2024-05-14	[Malone]	dragonforce	<a href="#">Link</a>
2024-05-14	[Hardings Transport]	dragonforce	<a href="#">Link</a>
2024-05-14	[Connelly Security Systems]	dragonforce	<a href="#">Link</a>
2024-05-14	[Motor Munich]	dragonforce	<a href="#">Link</a>
2024-05-15	[epsd.org]	lockbit3	<a href="#">Link</a>
2024-05-15	[district70.org]	lockbit3	<a href="#">Link</a>
2024-05-15	[keuka.edu]	lockbit3	<a href="#">Link</a>
2024-05-15	[allcare-med.com]	lockbit3	<a href="#">Link</a>
2024-05-15	[Coplosa]	8base	<a href="#">Link</a>
2024-05-15	[Surrey Place Healthcare & Rehabilitation]	rhapsida	<a href="#">Link</a>
2024-05-15	[daubertchemical.com]	lockbit3	<a href="#">Link</a>
2024-05-08	[BRAZIL GOV]	arcusmedia	<a href="#">Link</a>
2024-05-11	[Braz Assessoria Contábil]	arcusmedia	<a href="#">Link</a>
2024-05-11	[Thibabem Atacadista]	arcusmedia	<a href="#">Link</a>
2024-05-11	[FILSCAP]	arcusmedia	<a href="#">Link</a>
2024-05-11	[Cusat]	arcusmedia	<a href="#">Link</a>
2024-05-11	[Frigrífico Boa Carne]	arcusmedia	<a href="#">Link</a>
2024-05-11	[GOLD RH S.A.S]	arcusmedia	<a href="#">Link</a>
2024-05-11	[Grupo SASMET]	arcusmedia	<a href="#">Link</a>
2024-05-15	[City of Neodesha]	ransomhub	<a href="#">Link</a>
2024-05-08	[gravetye-manor]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-15	[Wealth Depot LLC]	everest	<a href="#">Link</a>
2024-05-14	[morrisgroupint.com]	lockbit3	<a href="#">Link</a>
2024-05-14	[pierfoundry.com]	blacksuit	<a href="#">Link</a>
2024-05-14	[Fiskars Group]	akira	<a href="#">Link</a>
2024-05-14	[Bruno generators (Italian manufacturing)]	akira	<a href="#">Link</a>
2024-05-14	[GMJ & Co, Chartered Accountants]	bianlian	<a href="#">Link</a>
2024-05-14	[Rocky Mountain Sales ]	ransomhub	<a href="#">Link</a>
2024-05-14	[Talley Group]	incransom	<a href="#">Link</a>
2024-05-14	[acla.de]	lockbit3	<a href="#">Link</a>
2024-05-14	[Watt Carmichael]	dragonforce	<a href="#">Link</a>
2024-05-14	[500gb/www.confins.com.br/10kk/BR/Come to chat or we will attack you again.]	ransomhub	<a href="#">Link</a>
2024-05-14	[eucatex.com.br]	ransomhub	<a href="#">Link</a>
2024-05-14	[LPDB KUMKM LPDB.ID/LPDB.GO.ID]	ransomhub	<a href="#">Link</a>
2024-05-13	[Accurate Lock and Hardware]	dragonforce	<a href="#">Link</a>
2024-05-13	[Monocon International Refractory]	dragonforce	<a href="#">Link</a>
2024-05-13	[Persyn]	dragonforce	<a href="#">Link</a>
2024-05-13	[Aero Tec Laboratories]	hunters	<a href="#">Link</a>
2024-05-13	[Altipal]	dragonforce	<a href="#">Link</a>
2024-05-13	[Municipalité La Guadeloupe]	qilin	<a href="#">Link</a>
2024-05-13	[Eden Project Ltd]	incransom	<a href="#">Link</a>
2024-05-13	[Helapet Ltd]	incransom	<a href="#">Link</a>
2024-05-13	[oseranbahn.com]	lockbit3	<a href="#">Link</a>
2024-05-13	[jmjcorporation.com]	lockbit3	<a href="#">Link</a>
2024-05-13	[countyins.com]	lockbit3	<a href="#">Link</a>
2024-05-13	[utc-silverstone.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-13	[hesperiausd.org]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-13	[Eden Project]	incransom	<a href="#">Link</a>
2024-05-13	[umbrellaproperties.com]	dispossessor	<a href="#">Link</a>
2024-05-13	[Treasury of Cote d'Ivoire]	hunters	<a href="#">Link</a>
2024-05-13	[scanda.com.mx]	cactus	<a href="#">Link</a>
2024-05-13	[acfin.cl]	cactus	<a href="#">Link</a>
2024-05-13	[New Boston Dental Care]	8base	<a href="#">Link</a>
2024-05-13	[Service public de Wallonie]	8base	<a href="#">Link</a>
2024-05-13	[Cushman Contracting Corporation]	8base	<a href="#">Link</a>
2024-05-13	[Costa Edutainment SpA]	8base	<a href="#">Link</a>
2024-05-13	[Sigmund Espeland AS]	8base	<a href="#">Link</a>
2024-05-13	[Brovedani Group]	8base	<a href="#">Link</a>
2024-05-13	[Fic Expertise]	8base	<a href="#">Link</a>
2024-05-13	[W.I.S. Sicherheit]	8base	<a href="#">Link</a>
2024-05-12	[Brick Court Chambers]	medusa	<a href="#">Link</a>
2024-05-03	[Seaman's Mechanical]	incransom	<a href="#">Link</a>
2024-05-06	[Deeside Timberframe]	incransom	<a href="#">Link</a>
2024-05-12	[McSweeney / Langevin]	qilin	<a href="#">Link</a>
2024-05-11	[NITEK International LLC]	medusa	<a href="#">Link</a>
2024-05-11	[National Metalwares, L.P]	medusa	<a href="#">Link</a>
2024-05-12	[Romeo Pitaro Injury & Litigation Lawyers]	bianlian	<a href="#">Link</a>
2024-05-11	[NHS (press update)]	incransom	<a href="#">Link</a>
2024-05-11	[Jackson County]	blacksuit	<a href="#">Link</a>
2024-05-11	[For sale. Contact through admin.]	blacksuit	<a href="#">Link</a>
2024-05-10	[21stcenturyvitamins.com]	lockbit3	<a href="#">Link</a>
2024-05-10	[Montgomery County Board of Developmental Disabilities Services]	blacksuit	<a href="#">Link</a>
2024-05-10	[LiveHelpNow]	play	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-10	[NK Parts Industries]	play	<a href="#">Link</a>
2024-05-10	[Badger Tag & Label]	play	<a href="#">Link</a>
2024-05-10	[Haumiller Engineering]	play	<a href="#">Link</a>
2024-05-10	[Barid soft]	stormous	<a href="#">Link</a>
2024-05-10	[Pella]	hunters	<a href="#">Link</a>
2024-05-10	[Reading Electric]	akira	<a href="#">Link</a>
2024-05-10	[Kuhn Rechtsanwlte GmbH]	monti	<a href="#">Link</a>
2024-05-10	[colonialsd.org]	lockbit3	<a href="#">Link</a>
2024-05-09	[wisconsinindustrialcoatings.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[amsoft.cl]	lockbit3	<a href="#">Link</a>
2024-05-09	[cultivarnet.com.br]	lockbit3	<a href="#">Link</a>
2024-05-09	[ecotruck.com.br]	lockbit3	<a href="#">Link</a>
2024-05-09	[iaconnecticut.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[incegroup.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[contest.omg]	lockbit3	<a href="#">Link</a>
2024-05-05	[Banco central argentina]	zerotolerance	<a href="#">Link</a>
2024-05-09	[Administração do Porto de São Francisco do Sul (APSFS)]	ransomhub	<a href="#">Link</a>
2024-05-09	[lavalpoincon.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ccimp.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ufresources.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[cloudminds.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[calvia.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[manusa.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[habeco.com.vn]	lockbit3	<a href="#">Link</a>
2024-05-09	[rehub.ie]	lockbit3	<a href="#">Link</a>
2024-05-09	[torrepacheco.es]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[ccofva.com]	lockbit3	Link
2024-05-09	[dagma.com.ar]	lockbit3	Link
2024-05-09	[Edlong]	qilin	Link
2024-05-09	[dpkv.cz]	lockbit3	Link
2024-05-09	[hetero.com]	lockbit3	Link
2024-05-09	[vikrantsprings.com]	lockbit3	Link
2024-05-09	[doublehorse.in]	lockbit3	Link
2024-05-09	[iitm.ac.in]	lockbit3	Link
2024-05-09	[cttxpress.com]	lockbit3	Link
2024-05-09	[garage-cretot.fr]	lockbit3	Link
2024-05-09	[hotel-ostella.com]	lockbit3	Link
2024-05-09	[vm3fincas.es]	lockbit3	Link
2024-05-09	[thaiagri.com]	lockbit3	Link
2024-05-09	[tegaindustries.com]	lockbit3	Link
2024-05-09	[kioti.com]	lockbit3	Link
2024-05-09	[taylorcrane.com]	lockbit3	Link
2024-05-09	[grc-c.co.il]	lockbit3	Link
2024-05-09	[mogaisrael.com]	lockbit3	Link
2024-05-09	[ultragasmexico.com]	lockbit3	Link
2024-05-09	[eif.org.na]	lockbit3	Link
2024-05-09	[auburnpikapp.org]	lockbit3	Link
2024-05-09	[acla-werke.com]	lockbit3	Link
2024-05-09	[college-stemarie-elven.org]	lockbit3	Link
2024-05-09	[snk.sk]	lockbit3	Link
2024-05-09	[mutualclubunion.com.ar]	lockbit3	Link
2024-05-09	[rfca.com]	lockbit3	Link
2024-05-09	[hpo.pe]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[spu.ac.th]	lockbit3	<a href="#">Link</a>
2024-05-09	[livia.in]	lockbit3	<a href="#">Link</a>
2024-05-09	[cinealbeniz.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[truehomesusa.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[uniter.net]	lockbit3	<a href="#">Link</a>
2024-05-09	[itss.com.tr]	lockbit3	<a href="#">Link</a>
2024-05-09	[elements-ing.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[heartlandhealthcenter.org]	lockbit3	<a href="#">Link</a>
2024-05-09	[dsglobaltech.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[alian.mx]	lockbit3	<a href="#">Link</a>
2024-05-09	[evw.k12.mn.us]	lockbit3	<a href="#">Link</a>
2024-05-09	[mpeprevencion.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[binder.de]	lockbit3	<a href="#">Link</a>
2024-05-09	[interfashion.it]	lockbit3	<a href="#">Link</a>
2024-05-09	[vstar.in]	lockbit3	<a href="#">Link</a>
2024-05-09	[brfibra.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[museu-goeldi.br]	lockbit3	<a href="#">Link</a>
2024-05-09	[doxim.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[essinc.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[sislocar.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[depenning.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[asafoot.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[frankmiller.com]	blacksuit	<a href="#">Link</a>
2024-05-09	[vitema.vi.gov]	lockbit3	<a href="#">Link</a>
2024-05-09	[snapethorpeprimary.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[agencavisystems.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[salmonesaysen.cl]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[kowessex.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[totto.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[randi-group.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[grupopm.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ondozabal.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[orsiniimballaggi.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[vinatiorganics.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[peninsulacrane.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[brockington.leics.sch.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[cargotrinidad.com]	lockbit3	<a href="#">Link</a>
2024-05-02	[Pinnacle Orthopaedics]	incransom	<a href="#">Link</a>
2024-05-09	[Protected: HIDE NAME]	medusalocker	<a href="#">Link</a>
2024-05-09	[Zuber Gardner CPAs]	everest	<a href="#">Link</a>
2024-05-09	[Corr & Corr]	everest	<a href="#">Link</a>
2024-05-08	[rexmoore.com]	embargo	<a href="#">Link</a>
2024-05-08	[Northeast Orthopedics and Sports Medicine]	dAn0n	<a href="#">Link</a>
2024-05-08	[Glenwood Management]	dAn0n	<a href="#">Link</a>
2024-05-08	[College Park Industries]	dAn0n	<a href="#">Link</a>
2024-05-08	[Holstein Association USA]	qilin	<a href="#">Link</a>
2024-05-08	[Unimed Vales do Taquari e Rio Pardo]	rhysida	<a href="#">Link</a>
2024-05-08	[Electric Mirror Inc]	incransom	<a href="#">Link</a>
2024-05-08	[Richelieu Foods]	hunters	<a href="#">Link</a>
2024-05-08	[Trade-Mark Industrial]	hunters	<a href="#">Link</a>
2024-05-08	[Dragon Tax and Management INC]	bianlian	<a href="#">Link</a>
2024-05-08	[Mewborn & DeSelms]	blacksuit	<a href="#">Link</a>
2024-05-07	[Merritt Properties, LLC]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-07	[Autobell Car Wash, Inc]	medusa	<a href="#">Link</a>
2024-05-08	[fortify.pro]	apt73	<a href="#">Link</a>
2024-05-06	[Electric Mirror]	incransom	<a href="#">Link</a>
2024-05-07	[Intuitae]	qilin	<a href="#">Link</a>
2024-05-07	[Tholen Building Technology Group]	qilin	<a href="#">Link</a>
2024-05-07	[williamsrdm.com]	qilin	<a href="#">Link</a>
2024-05-07	[inforius]	qilin	<a href="#">Link</a>
2024-05-07	[Kamo Jou Trading ]	ransomhub	<a href="#">Link</a>
2024-05-07	[wichita.gov]	lockbit3	<a href="#">Link</a>
2024-05-01	[City of Buckeye (buckeyeaz.gov)]	incransom	<a href="#">Link</a>
2024-05-07	[Hibser Yamauchi Architects]	hunters	<a href="#">Link</a>
2024-05-07	[Noritsu America Corp.]	hunters	<a href="#">Link</a>
2024-05-07	[Autohaus Ebert]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Elbers GmbH & Co. KG]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Jetson Specialty Marketing Services, Inc.]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Vega Reederei GmbH & Co. KG]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Max Wild GmbH]	metaencryptor	<a href="#">Link</a>
2024-05-07	[woldae.com]	abyss	<a href="#">Link</a>
2024-05-07	[Information Integration Experts]	dAn0n	<a href="#">Link</a>
2024-05-06	[One Toyota of Oakland ]	medusa	<a href="#">Link</a>
2024-05-07	[Chemring Group ]	medusa	<a href="#">Link</a>
2024-05-07	[lalengineering]	ransomhub	<a href="#">Link</a>
2024-05-07	[skanlog.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[ctc-corp.net]	lockbit3	<a href="#">Link</a>
2024-05-07	[uslinen.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[tu-ilmenau.de]	lockbit3	<a href="#">Link</a>
2024-05-07	[thede-culpepper.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-07	[kimmelcleaners.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[emainc.net]	lockbit3	<a href="#">Link</a>
2024-05-07	[southernspecialtysupply.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[lenmed.co.za]	lockbit3	<a href="#">Link</a>
2024-05-07	[churchill-linen.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[rollingfields.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[srg-plc.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[gorrias-mercedes-benz.fr]	lockbit3	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2 Leak]	flocker	<a href="#">Link</a>
2024-05-07	[Central Florida Equipment]	play	<a href="#">Link</a>
2024-05-07	[High Performance Services]	play	<a href="#">Link</a>
2024-05-07	[Mauritzon]	play	<a href="#">Link</a>
2024-05-07	[Somerville]	play	<a href="#">Link</a>
2024-05-07	[Donco Air]	play	<a href="#">Link</a>
2024-05-07	[Affordable Payroll & Bookkeeping Services]	play	<a href="#">Link</a>
2024-05-07	[Utica Mack]	play	<a href="#">Link</a>
2024-05-07	[KC Scout]	play	<a href="#">Link</a>
2024-05-07	[Sentry Data Management]	play	<a href="#">Link</a>
2024-05-07	[aletech.com.br]	darkvault	<a href="#">Link</a>
2024-05-07	[Young Consulting]	blacksuit	<a href="#">Link</a>
2024-05-06	[Thaayakam LTD ]	ransomhub	<a href="#">Link</a>
2024-05-06	[The Weinstein Firm]	qilin	<a href="#">Link</a>
2024-05-06	[Nikolaus & Hohenadel]	bianlian	<a href="#">Link</a>
2024-05-06	[NRS Healthcare ]	ransomhub	<a href="#">Link</a>
2024-05-06	[gammarenax.ch]	lockbit3	<a href="#">Link</a>
2024-05-06	[oraclinical.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-06	[acsistemas.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[cpashin.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[epr-groupe.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[isee.biz]	lockbit3	<a href="#">Link</a>
2024-05-06	[cdev.gc.ca]	lockbit3	<a href="#">Link</a>
2024-05-06	[netspectrum.ca]	lockbit3	<a href="#">Link</a>
2024-05-06	[qstartlabs.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[syntax-architektur.at]	lockbit3	<a href="#">Link</a>
2024-05-06	[carespring.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[grand-indonesia.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[remagroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[telekom.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[aev-iledefrance.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[elarabygroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[thebiglifegroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[sonoco.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[ville-bouchemaine.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[eskarabajo.mx]	darkvault	<a href="#">Link</a>
2024-05-06	[Rafael Viñoly Architects]	blacksuit	<a href="#">Link</a>
2024-05-06	[TRC Talent Solutions]	blacksuit	<a href="#">Link</a>
2024-05-06	[M2E Consulting Engineers]	akira	<a href="#">Link</a>
2024-05-06	[sunray.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[eviivo.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[kras.hr]	lockbit3	<a href="#">Link</a>
2024-05-06	[tdt.aero]	lockbit3	<a href="#">Link</a>
2024-05-06	[svenskakyrkan.se]	lockbit3	<a href="#">Link</a>
2024-05-06	[htcinc.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-06	[irc.be]	lockbit3	<a href="#">Link</a>
2024-05-06	[geotechenv.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[ishoppes.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[parat-techology.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[getcloudapp.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[yucatan.gob.mx]	lockbit3	<a href="#">Link</a>
2024-05-06	[arcus.pl]	lockbit3	<a href="#">Link</a>
2024-05-06	[Nestoil]	blacksuit	<a href="#">Link</a>
2024-05-06	[Patterson & Rothwell Ltd]	medusa	<a href="#">Link</a>
2024-05-06	[Boyden]	medusa	<a href="#">Link</a>
2024-05-06	[W.F. Whelan]	medusa	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2]	flocker	<a href="#">Link</a>
2024-05-05	[Seneca Nation Health System]	incransom	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmom, and Rutgers University Part 2]	flocker	<a href="#">Link</a>
2024-05-04	[COMPEXLEGAL.COM]	clop	<a href="#">Link</a>
2024-05-04	[ikfhomefinance.com]	darkvault	<a href="#">Link</a>
2024-05-04	[The Islamic Emirat of Afghanistan National Environmental Protection Agency ]	ransomhub	<a href="#">Link</a>
2024-05-04	[Accounting Professionals LLC. Price, Breazeale & Chastang]	everest	<a href="#">Link</a>
2024-05-04	[cmactrans.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[ids-michigan.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[provencherroy.ca]	blackbasta	<a href="#">Link</a>
2024-05-04	[swisspro.ch]	blackbasta	<a href="#">Link</a>
2024-05-04	[olsonsteel.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[teaspa.it]	blackbasta	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-04	[ayesa.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[synlab.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[active-pcb.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[gai-it.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[Macildowie Associates]	medusa	<a href="#">Link</a>
2024-05-03	[Dr Charles A Evans]	qilin	<a href="#">Link</a>
2024-05-03	[Universidad Nacional Autónoma de México ]	ransomhub	<a href="#">Link</a>
2024-05-03	[thelawrencegroup.com]	blackbasta	<a href="#">Link</a>
2024-05-02	[sharik]	stormous	<a href="#">Link</a>
2024-05-02	[tdra]	stormous	<a href="#">Link</a>
2024-05-02	[fanr.gov.ae]	stormous	<a href="#">Link</a>
2024-05-02	[Bayanat]	stormous	<a href="#">Link</a>
2024-05-02	[kidx]	stormous	<a href="#">Link</a>
2024-05-03	[MCS]	qilin	<a href="#">Link</a>
2024-05-03	[Tohlen Building Technology Group]	qilin	<a href="#">Link</a>
2024-05-03	[Stainless Foundry & Engineering]	play	<a href="#">Link</a>
2024-05-02	[Ayoub & associates CPA Firm]	everest	<a href="#">Link</a>
2024-05-02	[www.servicepower.com]	apt73	<a href="#">Link</a>
2024-05-02	[www.credio.eu]	apt73	<a href="#">Link</a>
2024-05-02	[Lopez Hnos]	rhapsida	<a href="#">Link</a>
2024-05-02	[GWF Frankenwein]	raworld	<a href="#">Link</a>
2024-05-02	[Reederei Jüngerhans]	raworld	<a href="#">Link</a>
2024-05-02	[extraco.ae]	ransomhub	<a href="#">Link</a>
2024-05-02	[watergate]	qilin	<a href="#">Link</a>
2024-05-02	[Imedi L]	akira	<a href="#">Link</a>
2024-05-01	[Azteca Tax Systems]	bianlian	<a href="#">Link</a>
2024-05-01	[Clinica de Salud del Valle de Salinas]	bianlian	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-01	[cochraneglobal.com]	underground	Link
2024-05-01	[UK government]	snatch	Link
2024-05-01	[hookerfurniture.com]	lockbit3	Link
2024-05-01	[alimmigration.com]	lockbit3	Link
2024-05-01	[anatomage.com]	lockbit3	Link
2024-05-01	[bluegrasstechnologies.net]	lockbit3	Link
2024-05-01	[PINNACLEENGR.COM]	clop	Link
2024-05-01	[MCKINLEYPACKAGING.COM]	clop	Link
2024-05-01	[PILOTPEN.COM]	clop	Link
2024-05-01	[colonial.edu]	lockbit3	Link
2024-05-01	[cordish.com]	lockbit3	Link
2024-05-01	[concorr.com]	lockbit3	Link
2024-05-01	[yupousa.com]	lockbit3	Link
2024-05-01	[peaseinc.com]	lockbit3	Link
2024-05-01	[bdcm.com]	blackbasta	Link
2024-05-01	[MORTON WILLIAMS]	everest	Link
2024-05-03	[melting-mind.de]	apt73	Link
2024-05-21	[netscout.com]	dispossessor	Link

## 8 Quellen

### 8.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>

- 7) Exploit - [packetstormsecurity.com](https://packetstormsecurity.com)
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

## 9 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.