

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241128



## 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>21</b>
5.0.1 Gehackt via Nachbar... oder die Palo Alto. . . . .	21
<b>6 Cyberangriffe: (Nov)</b>	<b>22</b>
<b>7 Ransomware-Erpressungen: (Nov)</b>	<b>23</b>
<b>8 Quellen</b>	<b>42</b>
8.1 Quellenverzeichnis . . . . .	42
<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

#### ***Palo Alto Globalprotect: Schadcode-Lücke durch unzureichende Zertifikatsprüfung***

Eine Sicherheitslücke in Palo Alto Networks Globalprotect-VPN-App ermöglicht Angreifern, Rechner vollständig zu kompromittieren.

- [Link](#)

—

#### ***Microsoft patcht teils kritische Lücken außer der Reihe***

Microsoft hat Sicherheitslecks in mehreren Produkten geschlossen. Einige Updates müssen Nutzer installieren.

- [Link](#)

—

#### ***Root-Sicherheitslücken in VMware Aria Operations geschlossen***

VMwares IT-Verwaltungsplattform Aria Operations ist verwundbar. Admins sollten die Sicherheitspatches in Bälde installieren.

- [Link](#)

—

#### ***HPE Insight Remote Support: Monitoring-Software ermöglicht Codeschmuggel***

In der kostenlosen Monitoring-Software HPE Insight Remote Support ermöglichen teils kritische Sicherheitslücken das Einschleusen von Schadcode.

- [Link](#)

—

#### ***Angreifer attackieren SSL-VPN-Gateways von Array Networks***

Es gibt derzeit Attacken auf eine kritische Sicherheitslücke in den VPN-Produkten Array Networks AG und vxAG.

- [Link](#)

—

#### ***Trellix: Update dichtet Sicherheitslücken in Enterprise Security Manager ab***

In Trellix Enterprise Security Manager bessert der Hersteller mehrere Sicherheitslücken aus. Admins sollten das Update zeitnah installieren.

- [Link](#)

—

#### ***Dell Wyse Management Suite: Angreifer können Sicherheitsmechanismen umgehen***

Dells Entwickler haben in der Clientverwaltungssoftware WMS mehrere Schwachstellen geschlossen.

- [Link](#)

—

**Wordpress-Plug-in Anti-Spam by Cleantalk gefährdet 200.000 Seiten**

Im Wordpress-Plug-in Anti-Spam by Cleantalk klaffen gleich zwei Sicherheitslücken, durch die nicht authentifizierte Angreifer Instanzen kompromittieren können.

- [Link](#)

---

**Mehrere Softwareschwachstellen gefährden Qnap NAS**

Angreifer können Netzwerkspeicher von Qnap unter anderem über Schwachstellen im Betriebssystem und Photo Station attackieren.

- [Link](#)

---

**Neue Wireshark-Version schließt zwei Absturz-Lücken**

Angreifer konnten bisherige Versionen des Netzwerkanalysertools Wireshark abstürzen lassen. Aktuelle Updates bringen zudem RTCP-Analysen zurück.

- [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	0.955020000	0.994630000	<a href="#">Link</a>
CVE-2023-6895	0.936280000	0.992180000	<a href="#">Link</a>
CVE-2023-6553	0.952340000	0.994230000	<a href="#">Link</a>
CVE-2023-6019	0.935090000	0.992040000	<a href="#">Link</a>
CVE-2023-6018	0.916750000	0.990340000	<a href="#">Link</a>
CVE-2023-52251	0.947690000	0.993530000	<a href="#">Link</a>
CVE-2023-4966	0.971030000	0.998320000	<a href="#">Link</a>
CVE-2023-49103	0.948250000	0.993620000	<a href="#">Link</a>
CVE-2023-48795	0.962880000	0.995970000	<a href="#">Link</a>
CVE-2023-47246	0.962620000	0.995910000	<a href="#">Link</a>
CVE-2023-46805	0.959100000	0.995320000	<a href="#">Link</a>
CVE-2023-46747	0.972680000	0.998930000	<a href="#">Link</a>
CVE-2023-46604	0.969640000	0.997800000	<a href="#">Link</a>
CVE-2023-4542	0.941060000	0.992710000	<a href="#">Link</a>
CVE-2023-43208	0.974210000	0.999550000	<a href="#">Link</a>
CVE-2023-43177	0.959840000	0.995440000	<a href="#">Link</a>
CVE-2023-42793	0.970830000	0.998250000	<a href="#">Link</a>
CVE-2023-41265	0.912600000	0.990100000	<a href="#">Link</a>
CVE-2023-39143	0.920260000	0.990630000	<a href="#">Link</a>
CVE-2023-38205	0.953810000	0.994430000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996410000	<a href="#">Link</a>
CVE-2023-38146	0.906640000	0.989660000	<a href="#">Link</a>
CVE-2023-38035	0.974360000	0.999600000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967890000	0.997340000	<a href="#">Link</a>
CVE-2023-3519	0.965540000	0.996640000	<a href="#">Link</a>
CVE-2023-35082	0.963840000	0.996210000	<a href="#">Link</a>
CVE-2023-35078	0.967840000	0.997330000	<a href="#">Link</a>
CVE-2023-34993	0.972760000	0.998960000	<a href="#">Link</a>
CVE-2023-34634	0.926130000	0.991080000	<a href="#">Link</a>
CVE-2023-34362	0.970200000	0.998040000	<a href="#">Link</a>
CVE-2023-34039	0.929610000	0.991470000	<a href="#">Link</a>
CVE-2023-3368	0.937890000	0.992340000	<a href="#">Link</a>
CVE-2023-33246	0.973040000	0.999030000	<a href="#">Link</a>
CVE-2023-32315	0.973370000	0.999170000	<a href="#">Link</a>
CVE-2023-32235	0.914280000	0.990210000	<a href="#">Link</a>
CVE-2023-30625	0.950240000	0.993890000	<a href="#">Link</a>
CVE-2023-30013	0.968110000	0.997390000	<a href="#">Link</a>
CVE-2023-29300	0.968250000	0.997440000	<a href="#">Link</a>
CVE-2023-29298	0.969330000	0.997720000	<a href="#">Link</a>
CVE-2023-28432	0.906870000	0.989670000	<a href="#">Link</a>
CVE-2023-28343	0.966250000	0.996810000	<a href="#">Link</a>
CVE-2023-28121	0.929810000	0.991490000	<a href="#">Link</a>
CVE-2023-27524	0.970320000	0.998070000	<a href="#">Link</a>
CVE-2023-27372	0.973870000	0.999380000	<a href="#">Link</a>
CVE-2023-27350	0.968620000	0.997510000	<a href="#">Link</a>
CVE-2023-26469	0.957610000	0.995080000	<a href="#">Link</a>
CVE-2023-26360	0.962010000	0.995810000	<a href="#">Link</a>
CVE-2023-26035	0.969120000	0.997650000	<a href="#">Link</a>
CVE-2023-25717	0.949440000	0.993770000	<a href="#">Link</a>
CVE-2023-25194	0.967670000	0.997290000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963800000	0.996190000	<a href="#">Link</a>
CVE-2023-24489	0.972870000	0.998990000	<a href="#">Link</a>
CVE-2023-23752	0.948310000	0.993630000	<a href="#">Link</a>
CVE-2023-23397	0.902750000	0.989400000	<a href="#">Link</a>
CVE-2023-23333	0.963300000	0.996080000	<a href="#">Link</a>
CVE-2023-22527	0.969680000	0.997830000	<a href="#">Link</a>
CVE-2023-22518	0.963120000	0.996040000	<a href="#">Link</a>
CVE-2023-22515	0.973360000	0.999160000	<a href="#">Link</a>
CVE-2023-21839	0.933960000	0.991920000	<a href="#">Link</a>
CVE-2023-21554	0.951950000	0.994130000	<a href="#">Link</a>
CVE-2023-20887	0.968860000	0.997580000	<a href="#">Link</a>
CVE-2023-1698	0.911050000	0.990010000	<a href="#">Link</a>
CVE-2023-1671	0.962610000	0.995900000	<a href="#">Link</a>
CVE-2023-0669	0.972180000	0.998740000	<a href="#">Link</a>

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

Wed, 27 Nov 2024

#### **[NEU] [hoch] Zabbix: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um einen Denial of Service Angriff durchzuführen, Sicherheitsvorkehrungen zu umgehen oder seine Rechte zu erweitern.

- [Link](#)

—

Wed, 27 Nov 2024

#### **[NEU] [hoch] GitLab: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Sicherheitsvorkehrungen zu umgehen, erhöhte Berechtigungen zu erlangen, einen Denial-of-Service-Zustand herbeizuführen und vertrauliche Informationen offenzulegen.

- [Link](#)



—  
Wed, 27 Nov 2024

**[NEU] [hoch] Synology DiskStation Manager: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Synology DiskStation Manager ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder seine Rechte zu erweitern.

- [Link](#)

—

Wed, 27 Nov 2024

**[NEU] [hoch] Mozilla Firefox 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, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Cross-Site-Scripting- oder Spoofing-Angriffe durchzuführen.

- [Link](#)

—

Wed, 27 Nov 2024

**[UPDATE] [hoch] docker: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Wed, 27 Nov 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- [Link](#)

—

Wed, 27 Nov 2024

**[UPDATE] [hoch] PostgreSQL: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.

- [Link](#)

—

Wed, 27 Nov 2024

**[UPDATE] [hoch] PHP: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen Spoofing-Angriff durchzuführen.

- [Link](#)

---

Tue, 26 Nov 2024

**[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

---

Tue, 26 Nov 2024

**[UPDATE] [hoch] Intel Prozessor (Xeon): Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Prozessor ausnutzen, um einen Denial of Service Angriff durchzuführen und sich erhöhte Rechte zu verschaffen.

- [Link](#)

---

Tue, 26 Nov 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux (perl-App-cpanminus): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Tue, 26 Nov 2024

**[NEU] [hoch] Netgate pfSense: Mehrere Schwachstellen**

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Netgate pfSense ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen seine Rechte zu erweitern oder Informationen offenzulegen.

- [Link](#)

---

Tue, 26 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Tue, 26 Nov 2024

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Tue, 26 Nov 2024

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Tue, 26 Nov 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 26 Nov 2024

**[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen**

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Tue, 26 Nov 2024

**[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Denial of Service und Codeausführung**

Ein entfernter Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Zustand herbeizuführen und potenziell um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 26 Nov 2024

**[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Offenlegung von Informationen**

Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Tue, 26 Nov 2024

**[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Offenlegung von Informationen**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/27/2024	[Fedora 40 : mingw-glib2 (2024-1e29ad7d25)]	critical
11/27/2024	[RHEL 9 : perl-App-cpanminus (RHSA-2024:10218)]	critical
11/27/2024	[RHEL 8 : perl-App-cpanminus:1.7044 (RHSA-2024:10219)]	critical
11/27/2024	[RHEL 7 : Red Hat JBoss Enterprise Application Platform 7.3.11 Security update (Important) (RHSA-2024:10207)]	critical
11/27/2024	[RHEL 7 : Red Hat JBoss Enterprise Application Platform 7.1.8 on RHEL 7 (RHSA-2024:10208)]	critical
11/27/2024	[FreeBSD : keycloak – Multiple security fixes (7d7a28cd-7f5a-450a-852f-c49aaab3fa7e)]	critical
11/27/2024	[Debian dla-3968 : netatalk - security update]	critical
11/26/2024	[Ubuntu 24.04 LTS / 24.10 : GitHub CLI vulnerability (USN-7130-1)]	critical
11/26/2024	[Debian dsa-5819 : libapache2-mod-php8.2 - security update]	critical
11/26/2024	[Korenix JetNet Arbitrary Unauthenticated TFTP Actions (CVE-2020-12504)]	critical
11/26/2024	[Korenix JetNet Backdoor Accounts (CVE-2020-12501)]	critical
11/26/2024	[Korenix JetNet Unauthenticated Device Administration (CVE-2020-12500)]	critical
11/27/2024	[Fedora 40 : mingw-libsoup (2024-8c3476dd24)]	high

Datum	Schwachstelle	Bewertung
11/27/2024	[Fedora 41 : qbittorrent (2024-1c74fc369b)]	high
11/27/2024	[Ubuntu 22.04 LTS / 24.04 LTS / 24.10 : libsoup3 vulnerabilities (USN-7127-1)]	high
11/27/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : libsoup vulnerabilities (USN-7126-1)]	high
11/27/2024	[RHEL 9 : Red Hat build of MicroShift 4.16.24 (RHSA-2024:10149)]	high
11/27/2024	[Photon OS 4.0: Linux PHSA-2024-4.0-0714]	high
11/27/2024	[Photon OS 4.0: Apache PHSA-2024-4.0-0711]	high
11/27/2024	[Atlassian Confluence 7.19.x < 7.19.26 / 7.20.x < 8.5.12 / 8.6.x < 8.9.4 / 9.0.x < 9.0.1 (CONFSERVER-98481)]	high
11/27/2024	[Veeam Backup and Replication 10.x < 12.2.0.334 Authentication Bypass (November 2024) (KB4682)]	high
11/27/2024	[RHEL 9 : pam (RHSA-2024:10232)]	high
11/27/2024	[Oracle Linux 9 : kernel (ELSA-2024-10274)]	high
11/27/2024	[FreeBSD : Gitlab – vulnerabilities (2263ea04-ac81-11ef-998c-2cf05da270f3)]	high
11/27/2024	[Debian dsa-5821 : thunderbird - security update]	high
11/27/2024	[Debian dsa-5820 : firefox-esr - security update]	high
11/27/2024	[Mitsubishi Electric MELSEC iQ-F Series Improper Validation of Specified Type of Input (CVE-2024-8403)]	high
11/26/2024	[Korenix JetNet Cross-Site Request Forgery (CVE-2020-12502)]	high
11/26/2024	[Korenix JetNet Authenticated Command Injection (CVE-2020-12503)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Wed, 27 Nov 2024

#### ***ABB Cylon Aspect 3.08.01 vstatConfigurationDownload.php Configuration Download***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vulnerability. This can be exploited to download the CSV DB that contains the configuration mappings information via the VMobileImportExportServlet by directly calling the vstatConfigurationDownload.php script.

- [Link](#)

—

” “Wed, 27 Nov 2024

#### ***Akuvox Smart Intercom/Doorphone ServicesHTTPAPI Improper Access Control***

The Akuvox Smart Intercom/Doorphone suffers from an insecure service API access control. The vulnerability in ServicesHTTPAPI endpoint allows users with “User” privileges to modify API access settings and configurations. This improper access control permits privilege escalation, enabling unauthorized access to administrative functionalities. Exploitation of this issue could compromise system integrity and lead to unauthorized system modifications.

- [Link](#)

—

” “Fri, 22 Nov 2024

#### ***CUPS IPP Attributes LAN Remote Code Execution***

This Metasploit module exploits vulnerabilities in OpenPrinting CUPS, which is running by default on most Linux distributions. The vulnerabilities allow an attacker on the LAN to advertise a malicious printer that triggers remote code execution when a victim sends a print job to the malicious printer. Successful exploitation requires user interaction, but no CUPS services need to be reachable via accessible ports. Code execution occurs in the context of the lp user. Affected versions are cups-browsed less than or equal to 2.0.1, libcupsfilters versions 2.1b1 and below, libppd versions 2.1b1 and below, and cups-filters versions 2.0.1 and below.

- [Link](#)

—

” “Fri, 22 Nov 2024

#### ***ProjectSend R1605 Unauthenticated Remote Code Execution***

This Metasploit module exploits an improper authorization vulnerability in ProjectSend versions r1295 through r1605. The vulnerability allows an unauthenticated attacker to obtain remote code execution by enabling user registration, disabling the whitelist of allowed file extensions, and uploading a malicious PHP file to the server.

- [Link](#)

—

” “Fri, 22 Nov 2024

***needrestart Local Privilege Escalation***

Qualys discovered that needrestart suffers from multiple local privilege escalation vulnerabilities that allow for root access from an unprivileged user.

- [Link](#)

—

” “Fri, 22 Nov 2024

***fronsetia 1.1 Cross Site Scripting***

fronsetia version 1.1 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 22 Nov 2024

***fronsetia 1.1 XML Injection***

fronsetia version 1.1 suffers from an XML external entity injection vulnerability.

- [Link](#)

—

” “Fri, 22 Nov 2024

***PowerVR psProcessHandleBase Reuse***

PowerVR has an issue where PVRSRVAcquireProcessHandleBase() can cause psProcessHandleBase reuse when PIDs are reused.

- [Link](#)

—

” “Fri, 22 Nov 2024

***Linux 6.6 Race Condition***

A security-relevant race between mremap() and THP code has been discovered. Reaching the buggy code typically requires the ability to create unprivileged namespaces. The bug leads to installing physical address 0 as a page table, which is likely exploitable in several ways: For example, triggering the bug in multiple processes can probably lead to unintended page table sharing, which probably can lead to stale TLB entries pointing to freed pages.

- [Link](#)

—

” “Fri, 22 Nov 2024

***Korenix JetPort 5601 1.2 Path Traversal***

Korenix JetPort 5601 version 1.2 suffers from a path traversal vulnerability.

- [Link](#)

—

” “Fri, 22 Nov 2024

***SEH utnserver Pro 20.1.22 Cross Site Scripting***

SEH utnservyer Pro version 20.1.22 suffers from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 21 Nov 2024

***Ivanti EPM Agent Portal Command Execution***

This Metasploit module leverages an unauthenticated remote command execution vulnerability in Ivanti’s EPM Agent Portal where an RPC client can invoke a method which will run an attacker-specified string on the remote target as NT AUTHORITY\SYSTEM. This vulnerability is present in versions prior to EPM 2021.1 Su4 and EPM 2022 Su2.

- [Link](#)

—

” “Thu, 21 Nov 2024

***Judge0 Sandbox Escape***

Judge0 does not account for symlinks placed inside the sandbox directory, which can be leveraged by an attacker to write to arbitrary files and gain code execution outside of the sandbox.

- [Link](#)

—

” “Tue, 19 Nov 2024

***WordPress Really Simple Security Authentication Bypass***

WordPress Really Simple Security plugin versions prior to 9.1.2 proof of concept authentication bypass exploit.

- [Link](#)

—

” “Tue, 19 Nov 2024

***Palo Alto PAN-OS Authentication Bypass / Remote Command Execution***

Proof of concept code to exploit an authentication bypass in Palo Alto’s PAN-OS that is coupled with remote command execution.

- [Link](#)

—

” “Mon, 18 Nov 2024

***Pyload Remote Code Execution***

CVE-2024-28397 is a sandbox escape in js2py versions 0.74 and below. js2py is a popular python package that can evaluate javascript code inside a python interpreter. The vulnerability allows for an attacker to obtain a reference to a python object in the js2py environment enabling them to escape the sandbox, bypass pyimport restrictions and execute arbitrary commands on the host. At the time of this writing no patch has been released and version 0.74 is the latest version of js2py



which was released Nov 6, 2022. CVE-2024-39205 is a remote code execution vulnerability in Pyload versions 0.5.0b3.dev85 and below. It is an open-source download manager designed to automate file downloads from various online sources. Pyload is vulnerable because it exposes the vulnerable js2py functionality mentioned above on the /flash/addcrypted2 API endpoint. This endpoint was designed to only accept connections from localhost but by manipulating the HOST header we can bypass this restriction in order to access the API to achieve unauthenticated remote code execution.

- [Link](#)

—

” “Mon, 18 Nov 2024

#### ***SOPlanning 1.52.01 Remote Code Execution***

SOPlanning version 1.52.01 authenticated remote code execution exploit.

- [Link](#)

—

” “Thu, 14 Nov 2024

#### ***Siemens Energy Omnivise T3000 8.2 SP3 Privilege Escalation / File Download***

Siemens Energy Omnivise T3000 version 8.2 SP3 suffers from local privilege escalation, cleartext storage of passwords in configuration and log files, file system access allowing for arbitrary file download, and IP whitelist bypass.

- [Link](#)

—

” “Thu, 14 Nov 2024

#### ***TX Text Control .NET Server For ASP.NET Arbitrary File Read / Write***

TX Text Control .NET Server For ASP.NET has an issue where it was possible to change the configured system path for reading and writing files in the underlying operating system with privileges of the user running a web application.

- [Link](#)

—

” “Thu, 14 Nov 2024

#### ***GravCMS 1.10.7 Arbitrary YAML Write / Update***

Proof of concept remote code execution exploit for GravCMS 1.10.7 that leverages an arbitrary YAML write / update.

- [Link](#)

—

” “Thu, 14 Nov 2024

#### ***PHP-CGI Argument Injection Remote Code Execution***

Proof of concept remote code execution exploit for PHP-CGI that affects versions 8.1 before 8.1.29, 8.2 before 8.2.20, and 8.3 before 8.3.8.

- [Link](#)

—  
” “Wed, 13 Nov 2024

#### ***Palo Alto Expedition 1.2.91 Remote Code Execution***

This Metasploit module lets you obtain remote code execution in Palo Alto Expedition versions 1.2.91 and below. The first vulnerability, CVE-2024-5910, allows to reset the password of the admin user, and the second vulnerability, CVE-2024-9464, is an authenticated OS command injection. In a default installation, commands will get executed in the context of www-data. When credentials are provided, this module will only exploit the second vulnerability. If no credentials are provided, the module will first try to reset the admin password and then perform the OS command injection.

- [Link](#)

—

” “Mon, 11 Nov 2024

#### ***HASOMED Elefant / Elefant Software Updater Data Exposure / Privilege Escalation***

HASOMED Elefant versions prior to 24.04.00 and Elefant Software Updater versions prior to 1.4.2.1811 suffer from having an unprotected exposed firebird database, unprotected FHIR API, multiple local privilege escalation, and hardcoded service password vulnerabilities.

- [Link](#)

—

” “Mon, 11 Nov 2024

#### ***WSO2 4.0.0 / 4.1.0 / 4.2.0 Shell Upload***

WSO2 versions 4.0.0, 4.1.0, and 4.2.0 are susceptible to remote code execution via an arbitrary file upload vulnerability.

- [Link](#)

—

” “Thu, 07 Nov 2024

#### ***WordPress Meetup 0.1 Authentication Bypass***

WordPress Meetup plugin versions 0.1 and below suffer from an authentication bypass vulnerability.

- [Link](#)

—

”

## **4.2 0-Days der letzten 5 Tage**

“Wed, 27 Nov 2024

#### ***ZDI-24-1630: (0Day) Fuji Electric Monitouch V-SFT X1 File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1629: (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1628: (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Stack-Based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1627: (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1626: (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1625: (0Day) Fuji Electric Tellus Lite V-Simulator 5 V8 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1624: (0Day) Fuji Electric Monitouch V-SFT X1 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1623: (0Day) Fuji Electric Monitouch V-SFT V8 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

**ZDI-24-1622: (0Day) Fuji Electric Monitouch V-SFT V9C File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1621: (0Day) Fuji Electric Monitouch V-SFT V8 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1620: (0Day) Fuji Electric Monitouch V-SFT V10 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1619: (0Day) Fuji Electric Monitouch V-SFT V9C File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1618: (0Day) Fuji Electric Monitouch V-SFT V8 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1617: (0Day) Fuji Electric Monitouch V-SFT V8C File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1616: (0Day) Fuji Electric Monitouch V-SFT V10 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1615: (0Day) Fuji Electric Monitouch V-SFT V10 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 27 Nov 2024

***ZDI-24-1614: (0Day) Fuji Electric Monitouch V-SFT V10 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—  
”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Gehackt via Nachbar... oder die Palo Alto.



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-27	Hoboken	[USA]	<a href="#">Link</a>
2024-11-25	Arrowe Park Hospital	[GBR]	<a href="#">Link</a>
2024-11-25	Hofer Ärztezentrum	[DEU]	<a href="#">Link</a>
2024-11-21	Blue Yonder	[USA]	<a href="#">Link</a>
2024-11-19	University of Algarve (UAlg)	[PRT]	<a href="#">Link</a>
2024-11-19	Minneapolis Park and Recreation Board (MPRB)	[USA]	<a href="#">Link</a>
2024-11-19	DGME du Costa Rica	[CRI]	<a href="#">Link</a>
2024-11-18	Chambre d'agriculture de la Lozère	[FRA]	<a href="#">Link</a>
2024-11-18	INPS Servizi	[ITA]	<a href="#">Link</a>
2024-11-18	Arrondissement de Montréal-Nord	[CAN]	<a href="#">Link</a>
2024-11-18	Le Safed	[FRA]	<a href="#">Link</a>
2024-11-17	Bergen auf Rügen	[DEU]	<a href="#">Link</a>
2024-11-17	International Game Technology (IGT)	[USA]	<a href="#">Link</a>
2024-11-17	SOFITEX	[BFA]	<a href="#">Link</a>
2024-11-14	Vossko	[DEU]	<a href="#">Link</a>
2024-11-13	Alberta Innovates	[CAN]	<a href="#">Link</a>
2024-11-13	Cégep de Sorel-Tracy	[CAN]	<a href="#">Link</a>
2024-11-13	Aschaffenburg	[DEU]	<a href="#">Link</a>
2024-11-13	Département de la Réunion	[REU]	<a href="#">Link</a>
2024-11-09	Sheboygan	[USA]	<a href="#">Link</a>
2024-11-09	Berufsförderungswerk Oberhausen	[DEU]	<a href="#">Link</a>
2024-11-09	Southern Oregon Veterinary Specialty Center (SOVSC)	[USA]	<a href="#">Link</a>
2024-11-07	Département des Hautes-Pyrénées	[FRA]	<a href="#">Link</a>
2024-11-07	Ahold Delhaize	[USA]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-11-05	Lojas Marisa	[BRA]	<a href="#">Link</a>
2024-11-05	Wexford County	[USA]	<a href="#">Link</a>
2024-11-05	Ridgewood Schools	[USA]	<a href="#">Link</a>
2024-11-04	Avis de Torino	[ITA]	<a href="#">Link</a>
2024-11-03	Washington state courts	[USA]	<a href="#">Link</a>
2024-11-03	La Sauvegarde	[FRA]	<a href="#">Link</a>
2024-11-03	Micon Office National	[AUS]	<a href="#">Link</a>
2024-11-02	Memorial Hospital and Manor	[USA]	<a href="#">Link</a>
2024-11-02	Kumla kommun	[SWE]	<a href="#">Link</a>
2024-11-01	South East Technological University (SETU)	[IRL]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-28	[cloudofgoods.com]	killsec	<a href="#">Link</a>
2024-11-28	[gehnaindia.com]	killsec	<a href="#">Link</a>
2024-11-28	[gajicermat.com]	killsec	<a href="#">Link</a>
2024-11-27	[corenroll.com]	ransomhub	<a href="#">Link</a>
2024-11-27	[ahn.org]	lockbit3	<a href="#">Link</a>
2024-11-27	[Contrack Facilities Management]	raworld	<a href="#">Link</a>
2024-11-27	[Ventana Micro Systems]	raworld	<a href="#">Link</a>
2024-11-27	[times-supermarket.com]	ransomhub	<a href="#">Link</a>
2024-11-27	[alleghenycontract.com]	ransomhub	<a href="#">Link</a>
2024-11-27	[tappi.org]	ransomhub	<a href="#">Link</a>
2024-11-27	[Grandview School District]	blacksuit	<a href="#">Link</a>
2024-11-27	[www.polleninformation.at]	apt73	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-27	[R Pac Central America S.A. de C.V.]	hunters	<a href="#">Link</a>
2024-11-27	[habeshacement.com]	lockbit3	<a href="#">Link</a>
2024-11-27	[Gruber Tool & Die (grubertool.com)]	fog	<a href="#">Link</a>
2024-11-08	[NUUO]	argonauts	<a href="#">Link</a>
2024-11-27	[wheelerassoc.com]	ransomhub	<a href="#">Link</a>
2024-11-27	[gronercrm.com.br]	ransomhub	<a href="#">Link</a>
2024-11-27	[Signal Health Washington (signalhealthwa.com)]	fog	<a href="#">Link</a>
2024-11-19	[bolognafc.it]	ransomhub	<a href="#">Link</a>
2024-11-26	[www.bent-tree.com]	ransomhub	<a href="#">Link</a>
2024-11-27	[facilcreditos.co]	ransomhub	<a href="#">Link</a>
2024-11-27	[osmedica.com.ar]	ransomhub	<a href="#">Link</a>
2024-11-27	[Vermilion Parish School System]	rhysida	<a href="#">Link</a>
2024-11-25	[formpipe.com]	incransom	<a href="#">Link</a>
2024-11-26	[SILKNET COMPANY]	medusalocker	<a href="#">Link</a>
2024-11-22	[Wisconsin Lifting Specialists]	lynx	<a href="#">Link</a>
2024-11-26	[www.sella.eng.br]	apt73	<a href="#">Link</a>
2024-11-26	[Pioneer Urban Land & Infrastructure (pioneerurban.in)]	fog	<a href="#">Link</a>
2024-11-26	[Pinnacle Plastic Products (pinnacleplastproducts.com)]	fog	<a href="#">Link</a>
2024-11-26	[Complete Recycling Services (completerecyclingservices.com)]	fog	<a href="#">Link</a>
2024-11-25	[GMG]	lynx	<a href="#">Link</a>
2024-11-26	[Marketing Incentives (leinsterappointments.ie)]	fog	<a href="#">Link</a>
2024-11-26	[Metroline (metrolinedirect.com)]	fog	<a href="#">Link</a>
2024-11-26	[reliv.la]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-26	[walkingtree.org]	ransomhub	<a href="#">Link</a>
2024-11-26	[SCM GROUP]	lynx	<a href="#">Link</a>
2024-11-26	[TWRU CPAs & Financial Advisors]	bianlian	<a href="#">Link</a>
2024-11-22	[cal-tool.com]	ransomhub	<a href="#">Link</a>
2024-11-26	[OfficeZilla.com]	ransomhub	<a href="#">Link</a>
2024-11-26	[waltersgardens.com]	killsec	<a href="#">Link</a>
2024-11-25	[CNHW Landscape Design, Ltd]	spacebears	<a href="#">Link</a>
2024-11-26	[tacomaengineers.com]	kairos	<a href="#">Link</a>
2024-11-26	[mdmcusa.com]	safepay	<a href="#">Link</a>
2024-11-26	[goformz.com]	killsec	<a href="#">Link</a>
2024-11-26	[empowersettlementservices.com]	killsec	<a href="#">Link</a>
2024-11-26	[mydelux.com.my]	killsec	<a href="#">Link</a>
2024-11-25	[karberinsulation.com]	ransomhub	<a href="#">Link</a>
2024-11-25	[Kela Health]	medusa	<a href="#">Link</a>
2024-11-25	[Fancy Foods]	medusa	<a href="#">Link</a>
2024-11-25	[glts.net]	abyss	<a href="#">Link</a>
2024-11-25	[coppelltx.gov]	ransomhub	<a href="#">Link</a>
2024-11-25	[isd109.org]	ransomhub	<a href="#">Link</a>
2024-11-25	[parkleigh.com]	ransomhub	<a href="#">Link</a>
2024-11-25	[dienesusa.com]	ransomhub	<a href="#">Link</a>
2024-11-25	[yunker.com]	ransomhub	<a href="#">Link</a>
2024-11-25	[minneapolisparcs.org]	ransomhub	<a href="#">Link</a>
2024-11-25	[maynard.k12.ma.us]	ransomhub	<a href="#">Link</a>
2024-11-25	[www.netromsoftware.ro]	apt73	<a href="#">Link</a>
2024-11-25	[www.itlindia.com]	ransomhub	<a href="#">Link</a>
2024-11-01	[INFiLED]	ransomhouse	<a href="#">Link</a>
2024-11-25	[Everything Breaks]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-25	[Keable & Brown]	lynx	<a href="#">Link</a>
2024-11-25	[TOC]	lynx	<a href="#">Link</a>
2024-11-25	[Perfection Plus Services Inc]	medusa	<a href="#">Link</a>
2024-11-25	[JN attorney]	hunters	<a href="#">Link</a>
2024-11-25	[Orshan, Spann & Fernandez-Mesa]	hunters	<a href="#">Link</a>
2024-11-23	[borohradek]	incransom	<a href="#">Link</a>
2024-11-23	[atfservices.com.au]	incransom	<a href="#">Link</a>
2024-11-23	[aclaser.com.au]	incransom	<a href="#">Link</a>
2024-11-24	[Nicholsons Solicitors]	incransom	<a href="#">Link</a>
2024-11-25	[Hadwins Volkswagen]	incransom	<a href="#">Link</a>
2024-11-23	[BeClever]	lynx	<a href="#">Link</a>
2024-11-23	[Extra]	lynx	<a href="#">Link</a>
2024-11-24	[Hypertype]	lynx	<a href="#">Link</a>
2024-11-25	[Ithbar]	killsec	<a href="#">Link</a>
2024-11-25	[Dardoc]	killsec	<a href="#">Link</a>
2024-11-25	[inv[...]nator]	killsec	<a href="#">Link</a>
2024-11-25	[RiverRestHome]	killsec	<a href="#">Link</a>
2024-11-25	[Ace Laboratories Limited]	hunters	<a href="#">Link</a>
2024-11-24	[titlenine.com]	safepay	<a href="#">Link</a>
2024-11-24	[Concord Orthopaedics]	everest	<a href="#">Link</a>
2024-11-24	[STIIIZY]	everest	<a href="#">Link</a>
2024-11-24	[Pastor Real Estate]	incransom	<a href="#">Link</a>
2024-11-24	[Sa.SS Datentechnik]	incransom	<a href="#">Link</a>
2024-11-24	[co.cullman.al.us]	blacksuit	<a href="#">Link</a>
2024-11-24	[Silicom]	handala	<a href="#">Link</a>
2024-11-24	[Nationwide Legal]	killsec	<a href="#">Link</a>
2024-11-24	[Eassy Life]	killsec	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-24	[Efi Sales]	killsec	<a href="#">Link</a>
2024-11-23	[Vogue Homes]	killsec	<a href="#">Link</a>
2024-11-23	[Service Avicole JGL]	incransom	<a href="#">Link</a>
2024-11-23	[Darlington EMS]	incransom	<a href="#">Link</a>
2024-11-23	[Schuck-Gruppe]	incransom	<a href="#">Link</a>
2024-11-18	[www.protectasecurity.pe]	apt73	<a href="#">Link</a>
2024-11-20	[rao.hr]	apt73	<a href="#">Link</a>
2024-11-23	[gureco.pl]	apt73	<a href="#">Link</a>
2024-11-23	[lgpunjab.gov.in]	apt73	<a href="#">Link</a>
2024-11-23	[Gulf Energy Maritime]	raworld	<a href="#">Link</a>
2024-11-23	[IPE Engwicht]	incransom	<a href="#">Link</a>
2024-11-23	[Jones & Mayer]	hunters	<a href="#">Link</a>
2024-11-23	[Aeris Energy]	hunters	<a href="#">Link</a>
2024-11-23	[Alna-Bioscience]	incransom	<a href="#">Link</a>
2024-11-22	[Trinity Petroleum Management, LLC]	bianlian	<a href="#">Link</a>
2024-11-22	[blr.com]	ransomhub	<a href="#">Link</a>
2024-11-22	[madison-home.com]	lockbit3	<a href="#">Link</a>
2024-11-22	[sheboyganwi.gov]	chort	<a href="#">Link</a>
2024-11-14	[Suneva Medical]	lynx	<a href="#">Link</a>
2024-11-22	[LBCO Contracting LTD]	qilin	<a href="#">Link</a>
2024-11-22	[Calvert Home Mortgage Investment]	qilin	<a href="#">Link</a>
2024-11-22	[Zimmerman & Frachtman PA Law Firm]	qilin	<a href="#">Link</a>
2024-11-22	[ABC Group]	killsec	<a href="#">Link</a>
2024-11-21	[Hronopoulos]	qilin	<a href="#">Link</a>
2024-11-21	[curenta.com]	ransomhub	<a href="#">Link</a>
2024-11-21	[LenelS2]	play	<a href="#">Link</a>
2024-11-21	[Goldsmith & Hull]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-21	[Brueck Golosow Kim & Associates]	incransom	<a href="#">Link</a>
2024-11-21	[United Bakery Equipment]	incransom	<a href="#">Link</a>
2024-11-21	[MGEMAL]	arcusmedia	<a href="#">Link</a>
2024-11-21	[Symantric IT]	arcusmedia	<a href="#">Link</a>
2024-11-14	[Suneva Medical(sunevamedical.com)]	lynx	<a href="#">Link</a>
2024-11-21	[ViralPitch]	killsec	<a href="#">Link</a>
2024-11-21	[Zimmerei Buder]	incransom	<a href="#">Link</a>
2024-11-21	[www.cobeldarou.com]	ransomhub	<a href="#">Link</a>
2024-11-16	[www.damcapital.in]	ransomhub	<a href="#">Link</a>
2024-11-21	[Hogan Mfg (hoganmfg.com)]	fog	<a href="#">Link</a>
2024-11-21	[Fifteenfortyseven Critical Systems Realty (1547realty.com)]	fog	<a href="#">Link</a>
2024-11-21	[Kellerhals Ferguson Kroblin PLLC]	bianlian	<a href="#">Link</a>
2024-11-21	[Silverback Exploration]	bianlian	<a href="#">Link</a>
2024-11-21	[DMF Lighting]	qilin	<a href="#">Link</a>
2024-11-21	[Stalcorp Metal Forming LLC]	qilin	<a href="#">Link</a>
2024-11-21	[SSV Blockchain Network]	handala	<a href="#">Link</a>
2024-11-20	[PK Mulyo]	arcusmedia	<a href="#">Link</a>
2024-11-20	[Barneek Safety Consultancies]	arcusmedia	<a href="#">Link</a>
2024-11-20	[Trust Seeds]	arcusmedia	<a href="#">Link</a>
2024-11-20	[HM Environmental Services]	arcusmedia	<a href="#">Link</a>
2024-11-20	[IT Networks]	arcusmedia	<a href="#">Link</a>
2024-11-20	[www.microlise.com]	safepay	<a href="#">Link</a>
2024-11-04	[Groupe PPA- Mahe]	qilin	<a href="#">Link</a>
2024-11-07	[Berman Law Group]	qilin	<a href="#">Link</a>
2024-11-07	[Prime Group US]	qilin	<a href="#">Link</a>
2024-11-11	[www.ekirkpatrick.com]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-14	[LaMear & Rapert, LLC - Accounting Firm]	qilin	<a href="#">Link</a>
2024-11-19	[Alpha Care Medical Group]	qilin	<a href="#">Link</a>
2024-11-20	[Privat Spitex]	qilin	<a href="#">Link</a>
2024-11-20	[James H Maloy]	akira	<a href="#">Link</a>
2024-11-20	[Automation Tool & Die]	akira	<a href="#">Link</a>
2024-11-20	[Tampa State Bank]	akira	<a href="#">Link</a>
2024-11-20	[Ship Services]	akira	<a href="#">Link</a>
2024-11-19	[Volo Internet Tech]	akira	<a href="#">Link</a>
2024-11-19	[Furniture Mart USA]	akira	<a href="#">Link</a>
2024-11-04	[PBS AEROSPACE]	incransom	<a href="#">Link</a>
2024-11-20	[RDS Electric]	medusa	<a href="#">Link</a>
2024-11-20	[Bishop Ireton High School]	rhysida	<a href="#">Link</a>
2024-11-20	[scalar.co.il]	ransomhub	<a href="#">Link</a>
2024-11-20	[CK Power Public Manufacturing]	hunters	<a href="#">Link</a>
2024-11-20	[inthinking.net]	darkvault	<a href="#">Link</a>
2024-11-20	[Amherstburg Family Health]	bianlian	<a href="#">Link</a>
2024-11-19	[polaraire.com]	ransomhub	<a href="#">Link</a>
2024-11-14	[Département de La Réunion]	termite	<a href="#">Link</a>
2024-11-20	[Oxford Auto Insurance]	monti	<a href="#">Link</a>
2024-11-20	[Camim]	killsec	<a href="#">Link</a>
2024-11-20	[LiquiTech]	killsec	<a href="#">Link</a>
2024-11-19	[onnicar.it]	safepay	<a href="#">Link</a>
2024-11-19	[BusinessTraining.be]	safepay	<a href="#">Link</a>
2024-11-19	[ccseniorservices]	safepay	<a href="#">Link</a>
2024-11-19	[Safex.us]	safepay	<a href="#">Link</a>
2024-11-19	[westwood]	safepay	<a href="#">Link</a>
2024-11-19	[Indesign, LLC]	interlock	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-19	[Henderson Stamping & Production]	play	<a href="#">Link</a>
2024-11-19	[Diamond Brand Gear]	play	<a href="#">Link</a>
2024-11-19	[Dairy Farmers of Canada]	play	<a href="#">Link</a>
2024-11-19	[Miller & Smith]	play	<a href="#">Link</a>
2024-11-19	[Hive Power Engineering]	play	<a href="#">Link</a>
2024-11-19	[CMD]	play	<a href="#">Link</a>
2024-11-19	[IVC Technologies]	play	<a href="#">Link</a>
2024-11-19	[Birdair]	play	<a href="#">Link</a>
2024-11-19	[Vox Printing]	play	<a href="#">Link</a>
2024-11-19	[Burkburnett Independent School District]	fog	<a href="#">Link</a>
2024-11-19	[Valley Planing Mill (valleyplaning.com)]	fog	<a href="#">Link</a>
2024-11-19	[IndicaOnline]	everest	<a href="#">Link</a>
2024-11-19	[arabot.io]	darkvault	<a href="#">Link</a>
2024-11-19	[Performance Health & Fitness]	hunters	<a href="#">Link</a>
2024-11-19	[techguard.in]	darkvault	<a href="#">Link</a>
2024-11-18	[wulffco.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[smawins.net]	ransomhub	<a href="#">Link</a>
2024-11-19	[chsplumbing.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[tempaircompany.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[Anderson Miller LTD]	monti	<a href="#">Link</a>
2024-11-19	[Premier Tax Services]	monti	<a href="#">Link</a>
2024-11-19	[KVF]	monti	<a href="#">Link</a>
2024-11-19	[Southern Oregon Veterinary Specialty Center]	monti	<a href="#">Link</a>
2024-11-19	[rembe.de]	blackbasta	<a href="#">Link</a>
2024-11-19	[brylesresearch.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[hartmannbund.de]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-19	[citywestcommercials.co.uk]	ransomhub	<a href="#">Link</a>
2024-11-07	[thinkecs.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[San Francisco Ballet]	meow	<a href="#">Link</a>
2024-11-19	[gfemlaw.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[instinctpetfood.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[eatonmetal.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[continentalserves.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[wachter.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[jonti-craft.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[isaitaly.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[rockportmortgage.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[kmcglobal.com]	blackbasta	<a href="#">Link</a>
2024-11-19	[rauch.de]	blackbasta	<a href="#">Link</a>
2024-11-19	[interborosd.org]	ransomhub	<a href="#">Link</a>
2024-11-19	[Thebike.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[3ccaresystems.com]	ransomhub	<a href="#">Link</a>
2024-11-19	[Equentis Wealth]	killsec	<a href="#">Link</a>
2024-11-19	[Terra Energy]	killsec	<a href="#">Link</a>
2024-11-19	[Find Great People1]	akira	<a href="#">Link</a>
2024-11-06	[www.depewgillen.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[Fleet Equipment Center, Inc.]	ElDorado	<a href="#">Link</a>
2024-11-18	[ATD-American]	ElDorado	<a href="#">Link</a>
2024-11-18	[K-State College of Veterinary Medicine]	ElDorado	<a href="#">Link</a>
2024-11-18	[UCC Retrievals, Inc.]	ElDorado	<a href="#">Link</a>
2024-11-18	[TBM Consulting Group, Inc.]	ElDorado	<a href="#">Link</a>
2024-11-18	[Premier Packaging]	ElDorado	<a href="#">Link</a>
2024-11-18	[LINDOSTAR]	ElDorado	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-18	[Gough Construction]	ElDorado	<a href="#">Link</a>
2024-11-18	[Programs Improving Public Safety]	ElDorado	<a href="#">Link</a>
2024-11-18	[Palm Facility Services]	ElDorado	<a href="#">Link</a>
2024-11-18	[Kennedy Funding]	ElDorado	<a href="#">Link</a>
2024-11-18	[BUROTEC S.A.]	ElDorado	<a href="#">Link</a>
2024-11-18	[A & L Auto Recyclers]	ElDorado	<a href="#">Link</a>
2024-11-18	[Alliance Industries, LLC.]	ElDorado	<a href="#">Link</a>
2024-11-18	[CelPlan Technologies, Inc.]	ElDorado	<a href="#">Link</a>
2024-11-18	[Panzer Solutions LLC Business Services]	ElDorado	<a href="#">Link</a>
2024-11-18	[The Recycler Core]	ElDorado	<a href="#">Link</a>
2024-11-18	[Thunderbird Country Club]	ElDorado	<a href="#">Link</a>
2024-11-18	[Istituto di Istruzione Superiore “Giulio Natta”]	ElDorado	<a href="#">Link</a>
2024-11-18	[ANKERSKA PLOVIDBA d.d.]	ElDorado	<a href="#">Link</a>
2024-11-18	[Adams Homes]	ElDorado	<a href="#">Link</a>
2024-11-18	[A-1 Mobile Lock & Key]	ElDorado	<a href="#">Link</a>
2024-11-18	[CURVC Corp]	ElDorado	<a href="#">Link</a>
2024-11-18	[Pensacola]	ElDorado	<a href="#">Link</a>
2024-11-18	[Think Simple]	ElDorado	<a href="#">Link</a>
2024-11-18	[Patrick Sanders and Company, P.C.]	ElDorado	<a href="#">Link</a>
2024-11-18	[Mullen Wylie, LLC]	ElDorado	<a href="#">Link</a>
2024-11-18	[Cmc Construction Material]	ElDorado	<a href="#">Link</a>
2024-11-18	[Cucina Tagliani]	ElDorado	<a href="#">Link</a>
2024-11-18	[Data Campos Sistemas]	ElDorado	<a href="#">Link</a>
2024-11-18	[GC Custom Metal Fabricationsoon]	ElDorado	<a href="#">Link</a>
2024-11-18	[Business Systems House FZ-LLC]	ElDorado	<a href="#">Link</a>
2024-11-18	[Aberdeen]	ElDorado	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-18	[Compr LTD Aruba]	ElDorado	<a href="#">Link</a>
2024-11-18	[Minuteman Press]	ElDorado	<a href="#">Link</a>
2024-11-18	[Keizer's Collision CSN & Automotive]	ElDorado	<a href="#">Link</a>
2024-11-18	[The Municipal Administration of Barranquitas and its Department of Finance]	ElDorado	<a href="#">Link</a>
2024-11-18	[The PHOENIX]	ElDorado	<a href="#">Link</a>
2024-11-18	[PC AfterHours]	ElDorado	<a href="#">Link</a>
2024-11-18	[Bells Tax Service]	ElDorado	<a href="#">Link</a>
2024-11-18	[Tiendas Carrion & Fernandez]	ElDorado	<a href="#">Link</a>
2024-11-01	[LA LUCKY Brand]	ElDorado	<a href="#">Link</a>
2024-11-18	[SUSTA S.r.l.]	dragonforce	<a href="#">Link</a>
2024-11-18	[Maxeon]	medusa	<a href="#">Link</a>
2024-11-18	[eastgateauto.com]	blacksuit	<a href="#">Link</a>
2024-11-18	[kciaviation.com]	blacksuit	<a href="#">Link</a>
2024-11-16	[totaldevelopmentsolutions.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[jergenspiping.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[sealevelinc.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[Jornstax.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[waive.com.au]	ransomhub	<a href="#">Link</a>
2024-11-18	[allconstructiongroupwv.com]	ransomhub	<a href="#">Link</a>
2024-11-18	[Waters Truck and Tractor (waterstruck.com)]	fog	<a href="#">Link</a>
2024-11-18	[Dorner Law & Title Services]	hunters	<a href="#">Link</a>
2024-11-18	[Maxus Group]	akira	<a href="#">Link</a>
2024-11-18	[Bulbrite Industries]	akira	<a href="#">Link</a>
2024-11-18	[HUTTER ACUSTIX]	akira	<a href="#">Link</a>
2024-11-18	[Followup CRM]	killsec	<a href="#">Link</a>
2024-11-17	[Mantinga]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-14	[Apple Electric Ltd]	medusa	<a href="#">Link</a>
2024-11-15	[LEGO Construction Co]	medusa	<a href="#">Link</a>
2024-11-15	[Logistical Software Ltd]	medusa	<a href="#">Link</a>
2024-11-15	[Manens-Tifs SpA]	medusa	<a href="#">Link</a>
2024-11-14	[Conseil scolaire Viamonde]	termite	<a href="#">Link</a>
2024-11-13	[Lebenshilfe Heinsberg]	termite	<a href="#">Link</a>
2024-11-12	[Oman Oil]	termite	<a href="#">Link</a>
2024-11-12	[Nifast]	termite	<a href="#">Link</a>
2024-11-16	[uatf.edu.bo]	stormous	<a href="#">Link</a>
2024-11-15	[Nunziaplast Srl]	dragonforce	<a href="#">Link</a>
2024-11-15	[Grupo Trisan]	lynx	<a href="#">Link</a>
2024-11-17	[Buddy Loan]	killsec	<a href="#">Link</a>
2024-11-17	[hetrhedens.nl]	blacksuit	<a href="#">Link</a>
2024-11-17	[texanscan.org]	chort	<a href="#">Link</a>
2024-11-17	[edwardsburgschoolsfoundation.org]	chort	<a href="#">Link</a>
2024-11-17	[Tri-TechElectronics.com]	chort	<a href="#">Link</a>
2024-11-17	[bartow.k12.ga.us]	chort	<a href="#">Link</a>
2024-11-17	[paaf.gov.kw]	chort	<a href="#">Link</a>
2024-11-17	[hartwick.edu]	chort	<a href="#">Link</a>
2024-11-17	[The Egyptian Tax Authority (ETA)]	moneymessage	<a href="#">Link</a>
2024-11-17	[Dragon Capital]	killsec	<a href="#">Link</a>
2024-11-15	[kapurinc.com]	blacksuit	<a href="#">Link</a>
2024-11-16	[American Addiction Centers]	rhysida	<a href="#">Link</a>
2024-11-15	[Grupo_Trisan]	lynx	<a href="#">Link</a>
2024-11-15	[klarenbeek-transport.nl]	blacksuit	<a href="#">Link</a>
2024-11-15	[kenmore.com]	blacksuit	<a href="#">Link</a>
2024-11-15	[www.gob.mx]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-15	[jhs.co.uk]	ransomhub	<a href="#">Link</a>
2024-11-15	[potteau.com]	ransomhub	<a href="#">Link</a>
2024-11-15	[A&O IT Group]	hunters	<a href="#">Link</a>
2024-11-15	[Vector Transport (vectortransport.com)]	fog	<a href="#">Link</a>
2024-11-15	[Bio-Clima Service Srl]	everest	<a href="#">Link</a>
2024-11-15	[Total Patient Care LLC]	everest	<a href="#">Link</a>
2024-11-15	[A Sensitive Touch Home Health;Alphastar Home Health Care;Heart of Texas Home Healthcare Se]	everest	<a href="#">Link</a>
2024-11-15	[PHARMATIS-SAS]	incransom	<a href="#">Link</a>
2024-11-13	[fortinainvestments.com]	ransomhub	<a href="#">Link</a>
2024-11-15	[BluMed Health]	killsec	<a href="#">Link</a>
2024-11-14	[Datron WorldCommunications]	akira	<a href="#">Link</a>
2024-11-14	[Xtrim TVCable]	akira	<a href="#">Link</a>
2024-11-14	[SKS Bottle &Packaging]	akira	<a href="#">Link</a>
2024-11-14	[REV Engineering]	akira	<a href="#">Link</a>
2024-11-14	[Bergeron LLC]	akira	<a href="#">Link</a>
2024-11-14	[mk Technology Group]	akira	<a href="#">Link</a>
2024-11-14	[Saint Andrews Bureau]	akira	<a href="#">Link</a>
2024-11-14	[Ascend Packaging Systems]	akira	<a href="#">Link</a>
2024-11-14	[Tedkomp AB]	akira	<a href="#">Link</a>
2024-11-14	[Pemberton Fabricators, Inc (Sexual Harassment videos inside)]	akira	<a href="#">Link</a>
2024-11-14	[Burmeister &Wain Scandinavian Contractor]	akira	<a href="#">Link</a>
2024-11-14	[Optical Cable Corporation]	akira	<a href="#">Link</a>
2024-11-14	[Ultimus]	akira	<a href="#">Link</a>
2024-11-14	[Tennis Canada]	akira	<a href="#">Link</a>
2024-11-14	[Don's MobileGlass]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-14	[Zyloware]	meow	<a href="#">Link</a>
2024-11-14	[Pine Belt Cars]	meow	<a href="#">Link</a>
2024-11-14	[DieTech North America]	meow	<a href="#">Link</a>
2024-11-14	[Cottles Asphalt Maintenance Inc]	meow	<a href="#">Link</a>
2024-11-14	[Herron Todd White]	meow	<a href="#">Link</a>
2024-11-14	[J.S.T. Espana]	meow	<a href="#">Link</a>
2024-11-14	[Karl Malone Toyota]	meow	<a href="#">Link</a>
2024-11-14	[OMara Ag Equipment]	meow	<a href="#">Link</a>
2024-11-14	[Pincu Barkan, Law Office and Notary]	everest	<a href="#">Link</a>
2024-11-14	[ADT Freight Services Australia Pty Lt]	sarcoma	<a href="#">Link</a>
2024-11-14	[Kumla Kommun]	hunters	<a href="#">Link</a>
2024-11-14	[CP Construplan]	sarcoma	<a href="#">Link</a>
2024-11-13	[Dumont Printing]	akira	<a href="#">Link</a>
2024-11-13	[Berexco LLC]	akira	<a href="#">Link</a>
2024-11-13	[Intercomp]	akira	<a href="#">Link</a>
2024-11-12	[DynamicSystems]	medusa	<a href="#">Link</a>
2024-11-14	[Popular Life Insurance]	sarcoma	<a href="#">Link</a>
2024-11-14	[Micon National]	sarcoma	<a href="#">Link</a>
2024-11-14	[Kelowna Springs]	sarcoma	<a href="#">Link</a>
2024-11-13	[stalyhill-inf.tameside.sch.uk]	blacksuit	<a href="#">Link</a>
2024-11-13	[AXEON 360]	ciphbit	<a href="#">Link</a>
2024-11-13	[COOPERATIVA TELEFONICA DE CALAFATE LTD.]	BrainCipher	<a href="#">Link</a>
2024-11-13	[G-One Auto Parts de México S.A. de C.V.]	BrainCipher	<a href="#">Link</a>
2024-11-13	[Schmack]	hunters	<a href="#">Link</a>
2024-11-13	[Sercomm]	hunters	<a href="#">Link</a>
2024-11-13	[midstatesindustrial.com]	threeam	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-13	[nanolive.ch 2.0]	apt73	<a href="#">Link</a>
2024-11-05	[formosacpa.com.tw]	kairos	<a href="#">Link</a>
2024-11-05	[askyouraccountant.com]	kairos	<a href="#">Link</a>
2024-11-13	[kansasrmc.com]	kairos	<a href="#">Link</a>
2024-11-13	[Value Dental Center]	everest	<a href="#">Link</a>
2024-11-13	[Artistic Family Dental]	everest	<a href="#">Link</a>
2024-11-13	[Asaro Dental Aesthetics]	everest	<a href="#">Link</a>
2024-11-13	[Axpr Valve Science]	killsec	<a href="#">Link</a>
2024-11-12	[American Associated Pharmacies]	embargo	<a href="#">Link</a>
2024-11-12	[Giggle Finance]	killsec	<a href="#">Link</a>
2024-11-12	[Orange County Pathology Medical Group]	raworld	<a href="#">Link</a>
2024-11-12	[SK Gas]	raworld	<a href="#">Link</a>
2024-11-03	[Medigroup.ca]	ransomhub	<a href="#">Link</a>
2024-11-12	[Hillandale Farms]	akira	<a href="#">Link</a>
2024-11-12	[jst.es]	blacksuit	<a href="#">Link</a>
2024-11-12	[jarrellimc.com]	blacksuit	<a href="#">Link</a>
2024-11-06	[Banco de Fomento Internacional]	lynx	<a href="#">Link</a>
2024-11-11	[TaxPros of Clermont]	lynx	<a href="#">Link</a>
2024-11-11	[National Institute of Administration]	killsec	<a href="#">Link</a>
2024-11-07	[DSZ]	lynx	<a href="#">Link</a>
2024-11-07	[Future Metals]	lynx	<a href="#">Link</a>
2024-11-07	[Plowman Craven]	lynx	<a href="#">Link</a>
2024-11-11	[Supply Technologies]	blacksuit	<a href="#">Link</a>
2024-11-11	[Maxxis International]	blacksuit	<a href="#">Link</a>
2024-11-11	[potteau.be]	ransomhub	<a href="#">Link</a>
2024-11-11	[Followmont TransportPty Ltd]	akira	<a href="#">Link</a>
2024-11-11	[dezinecorp.com]	blacksuit	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-11	[Amourgis & Associates]	hunters	<a href="#">Link</a>
2024-11-11	[Dietzgen Corporation]	hunters	<a href="#">Link</a>
2024-11-01	[nynewspapers.com]	ransomhub	<a href="#">Link</a>
2024-11-11	[comarchs.com]	ransomhub	<a href="#">Link</a>
2024-11-11	[tolbertlegal.com]	ransomhub	<a href="#">Link</a>
2024-11-10	[OxyHealth]	killsec	<a href="#">Link</a>
2024-11-10	[Immuno Laboratories, Inc]	bianlian	<a href="#">Link</a>
2024-11-05	[bitquail.com]	ransomhub	<a href="#">Link</a>
2024-11-09	[ATSG, Inc]	bianlian	<a href="#">Link</a>
2024-11-09	[Mizuno (USA)]	bianlian	<a href="#">Link</a>
2024-11-09	[Palmisano & Goodman, P.A.]	bianlian	<a href="#">Link</a>
2024-11-09	[Finger Beton Unternehmensgruppe]	meow	<a href="#">Link</a>
2024-11-09	[Karman Inc]	meow	<a href="#">Link</a>
2024-11-09	[Siltech (siltechcorp.local)]	lynx	<a href="#">Link</a>
2024-11-09	[emefarmario.com.br]	apt73	<a href="#">Link</a>
2024-11-09	[Granite School District]	rhysida	<a href="#">Link</a>
2024-11-09	[WimCoCorp]	lynx	<a href="#">Link</a>
2024-11-09	[NEBRASKALAND]	lynx	<a href="#">Link</a>
2024-11-08	[MENZIES CNAC (Jardine Aviation Services, Agility)]	spacebears	<a href="#">Link</a>
2024-11-08	[bartleycorp.com]	ransomhub	<a href="#">Link</a>
2024-11-08	[interlabel.be]	ransomhub	<a href="#">Link</a>
2024-11-07	[del-electric.com]	ransomhub	<a href="#">Link</a>
2024-11-08	[liftkits4less.com]	apt73	<a href="#">Link</a>
2024-11-08	[www.lamaisonducitron.com]	apt73	<a href="#">Link</a>
2024-11-08	[www.baldinger-ag.ch]	apt73	<a href="#">Link</a>
2024-11-07	[Marisa S.A]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-08	[www.assurified.com]	apt73	<a href="#">Link</a>
2024-11-08	[www.botiga.com.uy]	apt73	<a href="#">Link</a>
2024-11-08	[Healthcare Management Systems]	bianlian	<a href="#">Link</a>
2024-11-08	[MedElite Group]	everest	<a href="#">Link</a>
2024-11-07	[nelconinc.biz]	ransomhub	<a href="#">Link</a>
2024-11-07	[www.bluco.com]	ransomhub	<a href="#">Link</a>
2024-11-07	[naj.ae]	darkvault	<a href="#">Link</a>
2024-11-07	[Equator Worldwide]	meow	<a href="#">Link</a>
2024-11-07	[Lexco]	meow	<a href="#">Link</a>
2024-11-07	[europe-qualité]	incransom	<a href="#">Link</a>
2024-11-07	[Winnebago Public School Foundation]	interlock	<a href="#">Link</a>
2024-11-05	[Alliance Technical Group]	medusa	<a href="#">Link</a>
2024-11-06	[Jomar Electrical Contractors]	medusa	<a href="#">Link</a>
2024-11-06	[Howell Electric Inc]	medusa	<a href="#">Link</a>
2024-11-06	[www.msdl.ca]	ransomhub	<a href="#">Link</a>
2024-11-07	[Postcard Mania]	play	<a href="#">Link</a>
2024-11-07	[New Law]	hunters	<a href="#">Link</a>
2024-11-06	[klinkamkurpark]	helldown	<a href="#">Link</a>
2024-11-06	[AMERICANVENTURE]	helldown	<a href="#">Link</a>
2024-11-06	[CSIKBS]	helldown	<a href="#">Link</a>
2024-11-06	[SANJACINTOCOUNY]	helldown	<a href="#">Link</a>
2024-11-06	[brandenburgerplumbing.com]	ransomhub	<a href="#">Link</a>
2024-11-06	[arcoexc.com]	ransomhub	<a href="#">Link</a>
2024-11-06	[Lincoln University]	meow	<a href="#">Link</a>
2024-11-06	[Cape Cod Regional Technical High School (capetech.us)]	fog	<a href="#">Link</a>
2024-11-06	[GSR Andrade Architects (gsr-andrade.com)]	fog	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-05	[metroelectric.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[sector5.ro]	ransomhub	<a href="#">Link</a>
2024-11-05	[Paragon Plastics]	play	<a href="#">Link</a>
2024-11-05	[Delfin Design & Manufacturing]	play	<a href="#">Link</a>
2024-11-05	[Smitty's Supply]	play	<a href="#">Link</a>
2024-11-05	[S & W Kitchens]	play	<a href="#">Link</a>
2024-11-05	[Dome Construction]	play	<a href="#">Link</a>
2024-11-06	[Interoute agency]	lynx	<a href="#">Link</a>
2024-11-06	[LmayInteroute agency]	lynx	<a href="#">Link</a>
2024-11-05	[pacificglazing.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[nwhealthporter.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[wexfordcounty.org]	embargo	<a href="#">Link</a>
2024-11-05	[ebrso]	qilin	<a href="#">Link</a>
2024-11-05	[Model Die & Mold]	lynx	<a href="#">Link</a>
2024-11-04	[mh-m.org]	embargo	<a href="#">Link</a>
2024-11-05	[Falco Sult]	bianlian	<a href="#">Link</a>
2024-11-05	[apoyoconsultoria.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[Webb Institute]	incransom	<a href="#">Link</a>
2024-11-05	[Fylde Coast Academy Trust]	rhysida	<a href="#">Link</a>
2024-11-04	[sundt.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[Memorial Hospital & Manor]	embargo	<a href="#">Link</a>
2024-11-02	[Scolari]	dragonforce	<a href="#">Link</a>
2024-11-05	[McMillan Electric Company]	medusa	<a href="#">Link</a>
2024-11-04	[maxdata.com.br]	ransomhub	<a href="#">Link</a>
2024-11-04	[goodline.com.au]	ransomhub	<a href="#">Link</a>
2024-11-04	[kenanasugarcompany.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[www.schweiker.de]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-04	[www.drbutlerandassociates.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[www.mssupply.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[fullfordelectric.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[College of Business - Tanzania]	hellcat	<a href="#">Link</a>
2024-11-04	[Ministry of Education - Jordan]	hellcat	<a href="#">Link</a>
2024-11-04	[Schneider Electric - France]	hellcat	<a href="#">Link</a>
2024-11-04	[International University of Sarajevo]	medusa	<a href="#">Link</a>
2024-11-04	[Whitaker Construction Group]	medusa	<a href="#">Link</a>
2024-11-04	[csucontracting.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[redphoenixconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-03	[krigerconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-03	[caseconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-03	[lambertstonecommercial.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[Doctor 24x7]	killsec	<a href="#">Link</a>
2024-11-03	[Hemubo]	hunters	<a href="#">Link</a>
2024-11-03	[Elad municipality]	handala	<a href="#">Link</a>
2024-11-03	[Russell Law Firm, LLC]	bianlian	<a href="#">Link</a>
2024-11-03	[L & B Transport, L.L.C.]	bianlian	<a href="#">Link</a>
2024-11-03	[guardianhc]	stormous	<a href="#">Link</a>
2024-11-02	[bravodigitaltrader.co.uk]	ransomhub	<a href="#">Link</a>
2024-11-02	[SVP Worldwide]	blacksuit	<a href="#">Link</a>
2024-11-02	[Sumitomo]	killsec	<a href="#">Link</a>
2024-11-01	[DieTech North America]	qilin	<a href="#">Link</a>
2024-11-01	[www.fatboysfleetandauto.com]	ransomhub	<a href="#">Link</a>
2024-11-01	[lighthouseelectric.com]	ransomhub	<a href="#">Link</a>
2024-11-01	[JS McCarthy Printers]	play	<a href="#">Link</a>
2024-11-01	[CGR Technologies]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-01	[United Sleep Diagnostics]	medusa	<a href="#">Link</a>
2024-11-01	[eap.gr]	ransomhub	<a href="#">Link</a>
2024-11-01	[vikurverk.is]	lockbit3	<a href="#">Link</a>
2024-11-01	[mirandaproduce.com.ve]	lockbit3	<a href="#">Link</a>
2024-11-01	[Cerp Bretagne Nord]	hunters	<a href="#">Link</a>
2024-11-01	[Hope Valley Recovery]	rhysida	<a href="#">Link</a>
2024-11-01	[lsst.ac]	cactus	<a href="#">Link</a>
2024-11-01	[MCNA Dental]	everest	<a href="#">Link</a>
2024-11-01	[Arctrade]	everest	<a href="#">Link</a>

## 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.