# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241125

# Inhaltsverzeichnis

# 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

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

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

- Link

—

***Sicherheitsupdates für Drupal: Schadcode-Attacken auf Webbrowser möglich***

Die Entwickler von Drupal haben in ihrem Content Management System mehrere Schwachstellen geschlossen.

- Link

—

***Angriffe auf Citrix-Sicherheitslücke beobachtet***

In der vergangenen Woche hat Citrix Sicherheitslücken im Session Recording geschlossen. Nun haben IT-Forscher Angriffe darauf beobachtet.

- Link

—

***PHP-Updates: 8.1.31, 8.2.26, 8.3.14 und 8.4.1 stopfen Sicherheitslecks***

Die PHP-Entwickler haben neue Pakete veröffentlicht. PHP 8.1.31, 8.2.26, 8.3.14 und 8.4.1 schließen Sicherheitslücken.

- Link

—

***Ubuntu-Server: Root-Lücke durch needrestart-Komponente***

IT-Sicherheitsforscher haben gleich fünf Root-Lücken in der needrestart-Komponente von Ubuntu-Servern entdeckt.

- Link

—

***7-Zip-Lücke ermöglicht Codeschmuggel mit manipulierten Archiven***

Mit manipulierten Archiven können Angreifer versuchen, 7-Zip-Nutzern Schadcode unterzujubeln. Ein Update steht bereit.

- Link

—

***Mehrere Sicherheitslücken in Zimbra 10.1.3 geschlossen***

Angreifer können die E-Mail- und Groupwarelösung Zimbra über mehrere Schwachstellen attackieren.

- Link

—

***Bitbucket, Confluence & Co.: Atlassian schließt DoS- und Schadcode-Lücken***

Atlassians Entwickler haben Sicherheitslücken in Bamboo, Bitbucket, Confluence, Crowd Data, Jira, Jira Service Management und Sourcetree geschlossen.

- Link

—

***Trend Micros Deep Security Agent ermöglicht Einschleusen von Schadcode***

Angreifer können Trend Micros Deep Security Agent Schadcode unterjubeln, etwa auch im lokalen Netz. Admins sollten zügig aktualisieren.

- Link

—

***Angreifer attackieren Oracle Agile PLM***

Oracle hat aufgrund von laufenden Attacken auf Oracle Agile Product Lifecycle Management ein Sicherheitsupdate außer der Reihe veröffentlicht.

- 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 | 0.994610000 | Link |
| CVE-2023-6895 | 0.936280000 | 0.992160000 | Link |
| CVE-2023-6553 | 0.951250000 | 0.994010000 | Link |
| CVE-2023-6019 | 0.935090000 | 0.992020000 | Link |
| CVE-2023-6018 | 0.916750000 | 0.990320000 | Link |
| CVE-2023-52251 | 0.947690000 | 0.993520000 | Link |
| CVE-2023-4966 | 0.971030000 | 0.998320000 | Link |
| CVE-2023-49103 | 0.951130000 | 0.994000000 | Link |
| CVE-2023-48795 | 0.962880000 | 0.995960000 | Link |
| CVE-2023-47246 | 0.962620000 | 0.995900000 | Link |
| CVE-2023-46805 | 0.959100000 | 0.995300000 | Link |
| CVE-2023-46747 | 0.972560000 | 0.998870000 | Link |
| CVE-2023-46604 | 0.969640000 | 0.997800000 | Link |
| CVE-2023-4542 | 0.941060000 | 0.992680000 | Link |
| CVE-2023-43208 | 0.974790000 | 0.999770000 | Link |
| CVE-2023-43177 | 0.959840000 | 0.995420000 | Link |
| CVE-2023-42793 | 0.970830000 | 0.998250000 | Link |
| CVE-2023-41265 | 0.912600000 | 0.990080000 | Link |
| CVE-2023-39143 | 0.920260000 | 0.990610000 | Link |
| CVE-2023-38205 | 0.953810000 | 0.994420000 | Link |
| CVE-2023-38203 | 0.964750000 | 0.996390000 | Link |
| CVE-2023-38146 | 0.906640000 | 0.989640000 | Link |
| CVE-2023-38035 | 0.974360000 | 0.999600000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-36845 | 0.967890000 | 0.997330000 | Link |
| CVE-2023-3519 | 0.965540000 | 0.996620000 | Link |
| CVE-2023-35082 | 0.963840000 | 0.996210000 | Link |
| CVE-2023-35078 | 0.967840000 | 0.997320000 | Link |
| CVE-2023-34993 | 0.972760000 | 0.998950000 | Link |
| CVE-2023-34634 | 0.926130000 | 0.991080000 | Link |
| CVE-2023-34362 | 0.969380000 | 0.997730000 | Link |
| CVE-2023-34039 | 0.929610000 | 0.991460000 | Link |
| CVE-2023-3368 | 0.937890000 | 0.992320000 | Link |
| CVE-2023-33246 | 0.973040000 | 0.999030000 | Link |
| CVE-2023-32315 | 0.973370000 | 0.999160000 | Link |
| CVE-2023-32235 | 0.910390000 | 0.989920000 | Link |
| CVE-2023-30625 | 0.954240000 | 0.994490000 | Link |
| CVE-2023-30013 | 0.966660000 | 0.996940000 | Link |
| CVE-2023-29300 | 0.967820000 | 0.997310000 | Link |
| CVE-2023-29298 | 0.968380000 | 0.997480000 | Link |
| CVE-2023-28432 | 0.906870000 | 0.989650000 | Link |
| CVE-2023-28343 | 0.966250000 | 0.996790000 | Link |
| CVE-2023-28121 | 0.929810000 | 0.991480000 | Link |
| CVE-2023-27524 | 0.970320000 | 0.998070000 | Link |
| CVE-2023-27372 | 0.973870000 | 0.999390000 | Link |
| CVE-2023-27350 | 0.969220000 | 0.997680000 | Link |
| CVE-2023-26469 | 0.957610000 | 0.995070000 | Link |
| CVE-2023-26360 | 0.962010000 | 0.995810000 | Link |
| CVE-2023-26035 | 0.969120000 | 0.997640000 | Link |
| CVE-2023-25717 | 0.949440000 | 0.993750000 | Link |
| CVE-2023-25194 | 0.967670000 | 0.997280000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-2479 | 0.963800000 | 0.996190000 | Link |
| CVE-2023-24489 | 0.972870000 | 0.998980000 | Link |
| CVE-2023-23752 | 0.948310000 | 0.993610000 | Link |
| CVE-2023-23397 | 0.902750000 | 0.989380000 | Link |
| CVE-2023-23333 | 0.963300000 | 0.996080000 | Link |
| CVE-2023-22527 | 0.969680000 | 0.997840000 | Link |
| CVE-2023-22518 | 0.963120000 | 0.996040000 | Link |
| CVE-2023-22515 | 0.973360000 | 0.999150000 | Link |
| CVE-2023-21839 | 0.933960000 | 0.991890000 | Link |
| CVE-2023-21554 | 0.951950000 | 0.994120000 | Link |
| CVE-2023-20887 | 0.968860000 | 0.997560000 | Link |
| CVE-2023-1698 | 0.911050000 | 0.990000000 | Link |
| CVE-2023-1671 | 0.962610000 | 0.995890000 | Link |
| CVE-2023-0669 | 0.971930000 | 0.998610000 | Link |

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

Fri, 22 Nov 2024

***[UPDATE] [kritisch] PaloAlto Networks PAN-OS: Mehrere Schwachstellen ermöglichen Privilegieneskalation***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PaloAlto Networks PAN-OS ausnutzen, um die Authentisierung zu umgehen und anschließend Root-Rechte zu erlangen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Oracle Communications: Mehrere Schwachstellen***

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Communications ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen***

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen***

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 22 Nov 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, 22 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Oracle Communications: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Communications ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- Link

—

Fri, 22 Nov 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, 22 Nov 2024

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

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen***

Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden

- Link

—

Fri, 22 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Mozilla Firefox: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Code auszuführen, um einen Denial of Service Zustand herbeizuführen und um Sicherheitsmechanismen zu umgehen, sowie den Benutzer zu täuschen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen***

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

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Red Hat Enterprise Linux (Advanced Cluster Management): Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Fri, 22 Nov 2024

***[UPDATE] [hoch] Red Hat Enterprise Linux (xerces-c): Schwachstelle ermöglicht Codeausführung, Offenlegung von Informationen oder DoS***

Ein entfernter, authentifizierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 22 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstelle in Red Hat OpenShift ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und beliebigen Code auszuführen.

- Link

—

Fri, 22 Nov 2024

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

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

- Link

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 11/24/2024 | [PHOENIX CONTACT Emalytics Controller ILC Incorrect Permission Assignment For Critical Resource (CVE-2020-8768)] | critical |
| 11/23/2024 | [Fedora 41 : dotnet9.0 (2024-aab6aded81)] | critical |
| 11/23/2024 | [Fedora 41 : php (2024-3891a08c9e)] | critical |
| 11/22/2024 | [Fedora 40 : trafficserver (2024-b3c4e8da81)] | critical |
| 11/22/2024 | [Fedora 39 : trafficserver (2024-589ea34c42)] | critical |
| 11/22/2024 | [Fedora 41 : trafficserver (2024-f4dc07db08)] | critical |
| 11/22/2024 | [Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : ZBar vulnerabilities (USN-7118-1)] | critical |
| 11/22/2024 | [Slackware Linux 15.0 / current php81 Multiple Vulnerabilities (SSA:2024-327-01)] | critical |
| 11/23/2024 | [CBL Mariner 2.0 Security Update: clamav (CVE-2024-20505)] | high |
| 11/23/2024 | [CBL Mariner 2.0 Security Update: reaper (CVE-2024-21538)] | high |
| 11/23/2024 | [CBL Mariner 2.0 Security Update: reaper (CVE-2020-28458)] | high |
| 11/22/2024 | [Oracle Linux 7 : xerces-c (ELSA-2024-8795)] | high |
| 11/22/2024 | [Oracle Linux 9 : osbuild-composer (ELSA-2024-9456)] | high |
| 11/22/2024 | [Oracle Linux 7 : squid (ELSA-2024-9738)] | high |

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 11/22/2024 | [Fedora 40 : microcode_ctl (2024-d20a106350)] | high |
| 11/22/2024 | [Fedora 39 : microcode_ctl (2024-7dfc167df4)] | high |
| 11/22/2024 | [Microsoft Edge (Chromium) < 131.0.2903.63 Multiple Vulnerabilities] | high |
| 11/22/2024 | [Photon OS 5.0: Linux PHSA-2024-5.0-0407] | high |
| 11/22/2024 | [7-Zip < 24.07 RCE (ZDI-24-1532)] | high |
| 11/22/2024 | [Rockwell Automation FactoryTalk Updater Client 4.20.00 RCE] | high |
| 11/22/2024 | [Rockwell Automation FactoryTalk Updater Agent < 4.20.00 Privilege Escalation] | high |
| 11/22/2024 | [Atlassian SourceTree 4.2.8 RCE] | high |
| 11/22/2024 | [Atlassian SourceTree 3.4.19 RCE] | high |
| 11/22/2024 | [Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel (Low Latency) vulnerabilities (USN-7120-3)] | high |
| 11/21/2024 | [CBL Mariner 2.0 Security Update: libsoup (CVE-2024-52532)] | high |
| 11/21/2024 | [CBL Mariner 2.0 Security Update: fluent-bit (CVE-2024-25431)] | high |
| 11/21/2024 | [CBL Mariner 2.0 Security Update: xorg-x11-server (CVE-2024-9632)] | high |

# 4 Aktiv ausgenutzte Sicherheitslücken

## 4.1 Exploits der letzten 5 Tage

“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***

WS02 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

—

” “Thu, 07 Nov 2024

***CyberPanel upgrademysqlstatus Arbitrary Command Execution***

Proof of concept remote command execution exploit for CyberPanel versions prior to 5b08cd6.

- Link

—

” “Thu, 07 Nov 2024

***TestRail CLI FieldsParser eval Injection***

While parsing test result XML files with the TestRail CLI, the presence of certain TestRail-specific fields can cause untrusted data to flow into an eval() statement, leading to arbitrary code execution. In order to exploit this, an attacker would need to be able to cause the TestRail CLI to parse a malicious XML file. Normally an attacker with this level of control would already have other avenues of gaining code execution.

- Link

—

”

## 4.2 0-Days der letzten 5 Tage

“Thu, 21 Nov 2024

***ZDI-24-1613: Intel Driver & Support Assistant Log Folder Link Following Local Privilege Escalation Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1612: Luxion KeyShot JT File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1611: Luxion KeyShot ABC File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1610: Luxion KeyShot OBJ File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1609: Luxion KeyShot 3DS File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1608: Luxion KeyShot SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1607: Luxion KeyShot 3DS File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1606: 7-Zip CopyCoder Infinite Loop Denial-of-Service Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1605: Adobe InDesign JP2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1604: IrfanView DXF File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1603: IrfanView DXF File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1602: IrfanView SVG File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1601: IrfanView ECW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1600: IrfanView JPM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1599: IrfanView ECW File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1598: IrfanView JPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1597: IrfanView JPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1596: IrfanView RLE File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1595: IrfanView RLE File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1594: IrfanView DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1593: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1592: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1591: IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1590: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1589: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1588: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1587: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1586: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1585: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1584: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1583: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1582: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1581: IrfanView DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1580: IrfanView ARW File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1579: IrfanView DJVU File Parsing Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1578: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1577: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1576: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1575: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1574: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1573: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1572: IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1571: IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1570: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1569: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1568: IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1567: IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1566: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1565: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1564: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1563: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1562: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1561: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1560: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1559: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1558: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1557: IrfanView WBZ plugin WB1 File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1556: IrfanView XCF Plugin XCF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1555: IrfanView WBZ Plugin WB1 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1554: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1553: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1552: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1551: IrfanView DXF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1550: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1549: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1548: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1547: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1546: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1545: IrfanView DWG File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1544: IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1543: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1542: IrfanView DXF File Parsing Use-After-Free Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1541: IrfanView DXF File Parsing Memory Corruption Remote Code Execution Vulnerability***
- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1540: IrfanView DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1539: IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1538: IrfanView DWG File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1537: IrfanView DWG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1536: IrfanView CGM File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

” “Thu, 21 Nov 2024

***ZDI-24-1535: IrfanView CGM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

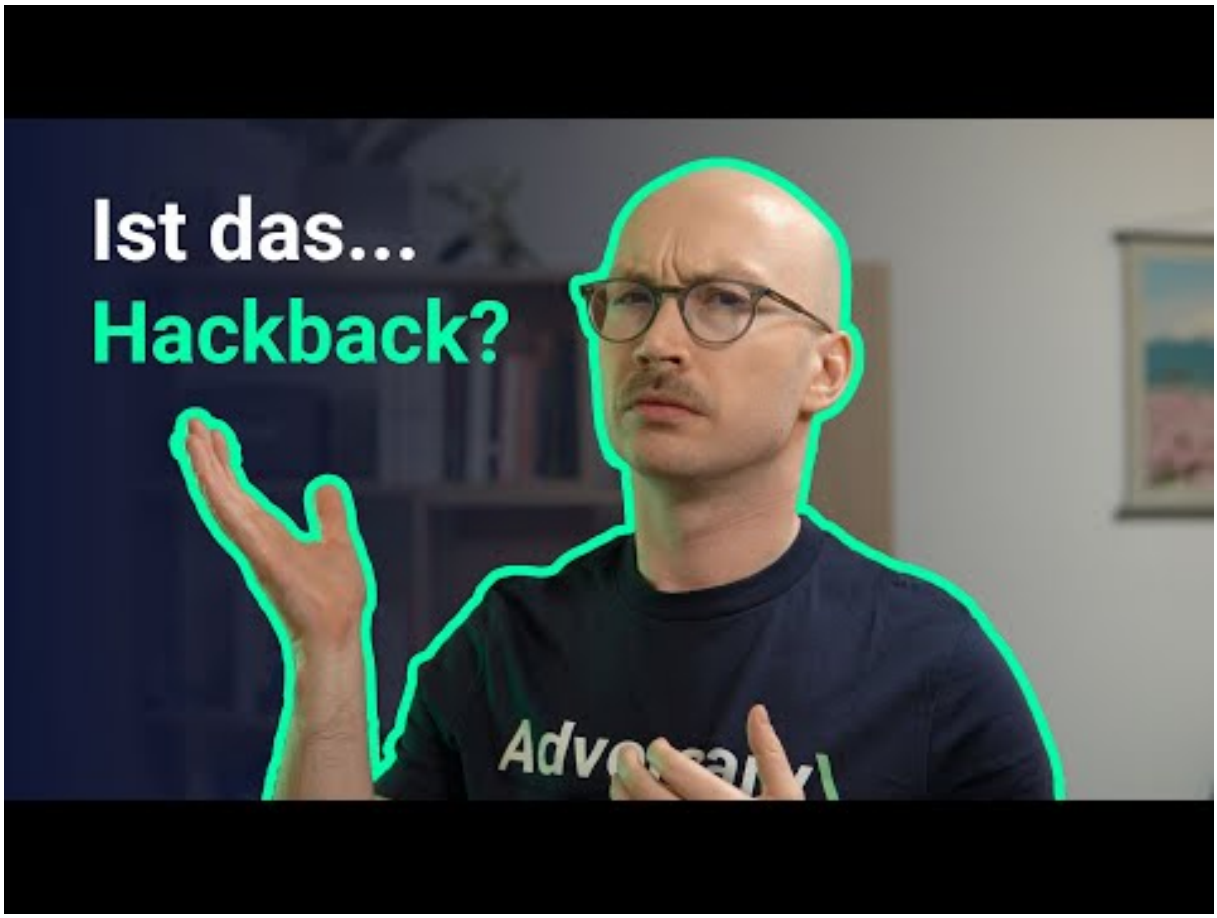
—

”

# 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Sophos spielt die UNO Reverse Karte  (+ Redline Stealer)




Zum Youtube Video

# 6 Cyberangriffe: (Nov)

| Datum | Opfer | Land | Information |
|---|---|---|---|
| 2024-11-18 | Chambre d'agriculture de la Lozère | [FRA] | Link |
| 2024-11-18 | INPS Servizi | [ITA] | Link |
| 2024-11-18 | Arrondissement de Montréal-Nord | [CAN] | Link |
| 2024-11-17 | Bergen auf Rügen | [DEU] | Link |
| 2024-11-17 | International Game Technology (IGT) | [USA] | Link |
| 2024-11-17 | SOFITEX | [BFA] | Link |
| 2024-11-13 | Alberta Innovates | [CAN] | Link |
| 2024-11-13 | Cégep de Sorel-Tracy | [CAN] | Link |
| 2024-11-13 | Aschaffenburg | [DEU] | Link |
| 2024-11-13 | Département de la Réunion | [REU] | Link |
| 2024-11-09 | Sheboygan | [USA] | Link |
| 2024-11-09 | Berufsförderungswerk Oberhausen | [DEU] | Link |
| 2024-11-09 | Southern Oregon Veterinary Specialty Center (SOVSC) | [USA] | Link |
| 2024-11-07 | Département des Hautes-Pyrénées | [FRA] | Link |
| 2024-11-07 | Ahold Delhaize | [USA] | Link |
| 2024-11-05 | Lojas Marisa | [BRA] | Link |
| 2024-11-05 | Wexford County | [USA] | Link |
| 2024-11-05 | Ridgewood Schools | [USA] | Link |
| 2024-11-04 | Avis de Torino | [ITA] | Link |
| 2024-11-03 | Washington state courts | [USA] | Link |
| 2024-11-03 | La Sauvegarde | [FRA] | Link |
| 2024-11-03 | Micon Office National | [AUS] | Link |
| 2024-11-02 | Memorial Hospital and Manor | [USA] | Link |
| 2024-11-02 | Kumla kommun | [SWE] | Link |

| Datum | Opfer | Land | Information |
|---|---|---|---|
| 2024-11-01 | South East Technological University (SETU) | [IRL] | Link |

## 7 Ransomware-Erpressungen: (Nov)

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-23 | [borohradek] | incransom | Link |
| 2024-11-23 | [atfservices.com.au] | incransom | Link |
| 2024-11-23 | [aclaser.com.au] | incransom | Link |
| 2024-11-24 | [Nicholsons Solicitors] | incransom | Link |
| 2024-11-25 | [Hadwins Volkswagen] | incransom | Link |
| 2024-11-23 | [BeClever] | lynx | Link |
| 2024-11-23 | [Extra] | lynx | Link |
| 2024-11-24 | [Hypertype] | lynx | Link |
| 2024-11-25 | [Ithbar] | killsec | Link |
| 2024-11-25 | [Dardoc] | killsec | Link |
| 2024-11-25 | [inv[…]nator] | killsec | Link |
| 2024-11-25 | [RiverRestHome] | killsec | Link |
| 2024-11-25 | [Ace Laboratories Limited] | hunters | Link |
| 2024-11-24 | [titlenine.com] | safepay | Link |
| 2024-11-24 | [Concord Orthopaedics] | everest | Link |
| 2024-11-24 | [STIIIZY] | everest | Link |
| 2024-11-24 | [Pastor Real Estate] | incransom | Link |
| 2024-11-24 | [Sa.SS Datentechnik] | incransom | Link |
| 2024-11-24 | [co.cullman.al.us] | blacksuit | Link |
| 2024-11-24 | [Silicom] | handala | Link |
| 2024-11-24 | [Nationwide Legal] | killsec | Link |

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

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-21 | [LenelS2] | play | Link |
| 2024-11-21 | [Goldsmith & Hull] | incransom | Link |
| 2024-11-21 | [Brueck Golosow Kim & Associates] | incransom | Link |
| 2024-11-21 | [United Bakery Equipment] | incransom | Link |
| 2024-11-21 | [MGEMAL] | arcusmedia | Link |
| 2024-11-21 | [Symantric IT] | arcusmedia | Link |
| 2024-11-14 | [Suneva Medical(sunevamedical.com)] | lynx | Link |
| 2024-11-21 | [ViralPitch] | killsec | Link |
| 2024-11-21 | [Zimmerei Buder] | incransom | Link |
| 2024-11-21 | [www.cobeldarou.com] | ransomhub | Link |
| 2024-11-21 | [www.damcapital.in] | ransomhub | Link |
| 2024-11-21 | [Hogan Mfg (hoganmfg.com)] | fog | Link |
| 2024-11-21 | [Fifteenfortyseven Critical Systems Realty (1547realty.com)] | fog | Link |
| 2024-11-21 | [Kellerhals Ferguson Kroblin PLLC] | bianlian | Link |
| 2024-11-21 | [Silverback Exploration] | bianlian | Link |
| 2024-11-21 | [DMF Lighting] | qilin | Link |
| 2024-11-21 | [Stalcop Metal Forming LLC] | qilin | Link |
| 2024-11-21 | [SSV Blockchain Network] | handala | Link |
| 2024-11-20 | [PK Mulyo] | arcusmedia | Link |
| 2024-11-20 | [Barneek Safety Consultancies] | arcusmedia | Link |
| 2024-11-20 | [Trust Seeds] | arcusmedia | Link |
| 2024-11-20 | [HM Environmental Services] | arcusmedia | Link |
| 2024-11-20 | [IT Networks] | arcusmedia | Link |
| 2024-11-20 | [www.microlise.com] | safepay | Link |
| 2024-11-04 | [Groupe PPA- Mahe] | qilin | Link |
| 2024-11-07 | [Berman Law Group] | qilin | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-07 | [Prime Group US] | qilin | Link |
| 2024-11-11 | [www.ekirkpatrick.com] | qilin | Link |
| 2024-11-14 | [LaMear & Rapert, LLC - Accounting Firm] | qilin | Link |
| 2024-11-19 | [Alpha Care Medical Group] | qilin | Link |
| 2024-11-20 | [Privat Spitex] | qilin | Link |
| 2024-11-20 | [James H Maloy] | akira | Link |
| 2024-11-20 | [Automation Tool & Die] | akira | Link |
| 2024-11-20 | [Tampa State Bank] | akira | Link |
| 2024-11-20 | [Ship Services] | akira | Link |
| 2024-11-19 | [Volo Internet Tech] | akira | Link |
| 2024-11-19 | [Furniture Mart USA] | akira | Link |
| 2024-11-04 | [PBS AEROSPACE] | incransom | Link |
| 2024-11-20 | [RDS Electric] | medusa | Link |
| 2024-11-20 | [Bishop Ireton High School] | rhysida | Link |
| 2024-11-20 | [scalar.co.il] | ransomhub | Link |
| 2024-11-20 | [CK Power Public Manufacturing] | hunters | Link |
| 2024-11-20 | [inthinking.net] | darkvault | Link |
| 2024-11-20 | [Amherstburg Family Health] | bianlian | Link |
| 2024-11-19 | [polaraire.com] | ransomhub | Link |
| 2024-11-14 | [Département de La Réunion] | termite | Link |
| 2024-11-20 | [Oxford Auto Insurance] | monti | Link |
| 2024-11-20 | [Camim] | killsec | Link |
| 2024-11-20 | [LiquiTech] | killsec | Link |
| 2024-11-19 | [piburners.com] | safepay | Link |
| 2024-11-19 | [onnicar.it] | safepay | Link |
| 2024-11-19 | [BusinessTraining.be] | safepay | Link |
| 2024-11-19 | [ccseniorservices] | safepay | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-19 | [Safex.us] | safepay | Link |
| 2024-11-19 | [mcauslan.com] | safepay | Link |
| 2024-11-19 | [stats.gov.bb] | safepay | Link |
| 2024-11-19 | [smartdimensions] | safepay | Link |
| 2024-11-19 | [westwood] | safepay | Link |
| 2024-11-19 | [threadfxinc/bluedogmerch] | safepay | Link |
| 2024-11-19 | [Indesign, LLC] | interlock | Link |
| 2024-11-19 | [Henderson Stamping & Production] | play | Link |
| 2024-11-19 | [Diamond Brand Gear] | play | Link |
| 2024-11-19 | [Dairy Farmers of Canada] | play | Link |
| 2024-11-19 | [Miller & Smith] | play | Link |
| 2024-11-19 | [Hive Power Engineering] | play | Link |
| 2024-11-19 | [CMD] | play | Link |
| 2024-11-19 | [IVC Technologies] | play | Link |
| 2024-11-19 | [Birdair] | play | Link |
| 2024-11-19 | [Vox Printing] | play | Link |
| 2024-11-19 | [Burkburnett Independent School District] | fog | Link |
| 2024-11-19 | [Valley Planing Mill (valleyplaning.com)] | fog | Link |
| 2024-11-19 | [IndicaOnline] | everest | Link |
| 2024-11-19 | [arabot.io] | darkvault | Link |
| 2024-11-19 | [Performance Health & Fitness] | hunters | Link |
| 2024-11-19 | [techguard.in] | darkvault | Link |
| 2024-11-18 | [wulffco.com] | ransomhub | Link |
| 2024-11-19 | [smawins.net] | ransomhub | Link |
| 2024-11-19 | [chsplumbing.com] | ransomhub | Link |
| 2024-11-19 | [tempaircompany.com] | ransomhub | Link |
| 2024-11-19 | [Anderson Miller LTD] | monti | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-19 | [Premier Tax Services] | monti | Link |
| 2024-11-19 | [KVF] | monti | Link |
| 2024-11-19 | [Southern Oregon Veterinary Specialty Center] | monti | Link |
| 2024-11-19 | [rembe.de] | blackbasta | Link |
| 2024-11-19 | [brylesresearch.com] | ransomhub | Link |
| 2024-11-19 | [hartmannbund.de] | ransomhub | Link |
| 2024-11-19 | [citywestcommercials.co.uk] | ransomhub | Link |
| 2024-11-07 | [thinkecs.com] | ransomhub | Link |
| 2024-11-19 | [San Francisco Ballet] | meow | Link |
| 2024-11-19 | [gfemlaw.com] | blackbasta | Link |
| 2024-11-19 | [instinctpetfood.com] | blackbasta | Link |
| 2024-11-19 | [eatonmetal.com] | blackbasta | Link |
| 2024-11-19 | [continentalserves.com] | blackbasta | Link |
| 2024-11-19 | [wachter.com] | blackbasta | Link |
| 2024-11-19 | [jonti-craft.com] | blackbasta | Link |
| 2024-11-19 | [isaitaly.com] | blackbasta | Link |
| 2024-11-19 | [rockportmortgage.com] | blackbasta | Link |
| 2024-11-19 | [kmcglobal.com] | blackbasta | Link |
| 2024-11-19 | [rauch.de] | blackbasta | Link |
| 2024-11-19 | [interborosd.org] | ransomhub | Link |
| 2024-11-19 | [Thebike.com] | ransomhub | Link |
| 2024-11-19 | [3ccaresystems.com] | ransomhub | Link |
| 2024-11-19 | [Equentis Wealth] | killsec | Link |
| 2024-11-19 | [Terra Energy] | killsec | Link |
| 2024-11-19 | [Find Great People1] | akira | Link |
| 2024-11-06 | [www.depewgillen.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-18 | [Fleet Equipment Center, Inc.] | ElDorado | Link |
| 2024-11-18 | [ATD-American] | ElDorado | Link |
| 2024-11-18 | [K-State College of Veterinary Medicine] | ElDorado | Link |
| 2024-11-18 | [UCC Retrievals, Inc.] | ElDorado | Link |
| 2024-11-18 | [TBM Consulting Group, Inc.] | ElDorado | Link |
| 2024-11-18 | [Premier Packaging] | ElDorado | Link |
| 2024-11-18 | [LINDOSTAR] | ElDorado | Link |
| 2024-11-18 | [Gough Construction] | ElDorado | Link |
| 2024-11-18 | [Programs Improving Public Safety] | ElDorado | Link |
| 2024-11-18 | [Palm Facility Services] | ElDorado | Link |
| 2024-11-18 | [Kennedy Funding] | ElDorado | Link |
| 2024-11-18 | [BUROTEC S.A.] | ElDorado | Link |
| 2024-11-18 | [A & L Auto Recyclers] | ElDorado | Link |
| 2024-11-18 | [Alliance Industries, LLC.] | ElDorado | Link |
| 2024-11-18 | [CelPlan Technologies, Inc.] | ElDorado | Link |
| 2024-11-18 | [Panzer Solutions LLC Business Services] | ElDorado | Link |
| 2024-11-18 | [The Recycler Core] | ElDorado | Link |
| 2024-11-18 | [Thunderbird Country Club] | ElDorado | Link |
| 2024-11-18 | [Istituto di Istruzione Superiore “Giulio Natta”] | ElDorado | Link |
| 2024-11-18 | [ANKERSKA PLOVIDBA d.d.] | ElDorado | Link |
| 2024-11-18 | [Adams Homes] | ElDorado | Link |
| 2024-11-18 | [A-1 Mobile Lock & Key] | ElDorado | Link |
| 2024-11-18 | [CURVC Corp] | ElDorado | Link |
| 2024-11-18 | [Pensacola] | ElDorado | Link |
| 2024-11-18 | [Think Simple] | ElDorado | Link |
| 2024-11-18 | [Patrick Sanders and Company, P.C.] | ElDorado | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-18 | [Mullen Wylie, LLC] | ElDorado | Link |
| 2024-11-18 | [Cmc Construction Material] | ElDorado | Link |
| 2024-11-18 | [Cucina Tagliani] | ElDorado | Link |
| 2024-11-18 | [Data Campos Sistemas] | ElDorado | Link |
| 2024-11-18 | [GC Custom Metal Fabricationsoon] | ElDorado | Link |
| 2024-11-18 | [Business Systems House FZ-LLC] | ElDorado | Link |
| 2024-11-18 | [Aberdeen] | ElDorado | Link |
| 2024-11-18 | [Compra LTD Aruba] | ElDorado | Link |
| 2024-11-18 | [Minuteman Press] | ElDorado | Link |
| 2024-11-18 | [Keizer’s Collision CSN & Automotive] | ElDorado | Link |
| 2024-11-18 | [The Municipal Administration of Barranquitas and its Department of Finance] | ElDorado | Link |
| 2024-11-18 | [The PHOENIX] | ElDorado | Link |
| 2024-11-18 | [PC AfterHours] | ElDorado | Link |
| 2024-11-18 | [Bells Tax Service] | ElDorado | Link |
| 2024-11-18 | [Tiendas Carrion & Fernandez] | ElDorado | Link |
| 2024-11-01 | [LA LUCKY Brand] | ElDorado | Link |
| 2024-11-18 | [SUSTA S.r.l.] | dragonforce | Link |
| 2024-11-18 | [Maxeon] | medusa | Link |
| 2024-11-18 | [eastgateauto.com] | blacksuit | Link |
| 2024-11-18 | [kciaviation.com] | blacksuit | Link |
| 2024-11-16 | [totaldevelopmentsolutions.com] | ransomhub | Link |
| 2024-11-18 | [jergenspiping.com] | ransomhub | Link |
| 2024-11-18 | [sealevelinc.com] | ransomhub | Link |
| 2024-11-18 | [Jornstax.com] | ransomhub | Link |
| 2024-11-18 | [waive.com.au] | ransomhub | Link |
| 2024-11-18 | [allconstructiongroupwv.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-18 | [Waters Truck and Tractor (waterstruck.com)] | fog | Link |
| 2024-11-18 | [Dorner Law & Title Services] | hunters | Link |
| 2024-11-18 | [Maxus Group] | akira | Link |
| 2024-11-18 | [Bulbrite Industries] | akira | Link |
| 2024-11-18 | [HUTTER ACUSTIX] | akira | Link |
| 2024-11-18 | [Followup CRM] | killsec | Link |
| 2024-11-17 | [Mantinga] | hunters | Link |
| 2024-11-14 | [Apple Electric Ltd] | medusa | Link |
| 2024-11-15 | [LEGO Construction Co] | medusa | Link |
| 2024-11-15 | [Logistical Software Ltd] | medusa | Link |
| 2024-11-15 | [Manens-Tifs SpA] | medusa | Link |
| 2024-11-14 | [Conseil scolaire Viamonde] | termite | Link |
| 2024-11-13 | [Lebenshilfe Heinsberg] | termite | Link |
| 2024-11-12 | [Oman Oil] | termite | Link |
| 2024-11-12 | [Nifast] | termite | Link |
| 2024-11-16 | [uatf.edu.bo] | stormous | Link |
| 2024-11-15 | [Nunziaplast Srl] | dragonforce | Link |
| 2024-11-15 | [Grupo Trisan] | lynx | Link |
| 2024-11-17 | [Buddy Loan] | killsec | Link |
| 2024-11-17 | [hetrhedens.nl] | blacksuit | Link |
| 2024-11-17 | [texanscan.org] | chort | Link |
| 2024-11-17 | [edwardsburgschoolsfoundation.org] | chort | Link |
| 2024-11-17 | [Tri-TechElectronics.com] | chort | Link |
| 2024-11-17 | [bartow.k12.ga.us] | chort | Link |
| 2024-11-17 | [paaf.gov.kw] | chort | Link |
| 2024-11-17 | [hartwick.edu] | chort | Link |
| 2024-11-17 | [The Egyptian Tax Authority (ETA)] | moneymessage | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-17 | [Dragon Capital] | killsec | Link |
| 2024-11-15 | [kapurinc.com] | blacksuit | Link |
| 2024-11-16 | [American Addiction Centers] | rhysida | Link |
| 2024-11-15 | [Grupo_Trisan] | lynx | Link |
| 2024-11-15 | [klarenbeek-transport.nl] | blacksuit | Link |
| 2024-11-15 | [kenmore.com] | blacksuit | Link |
| 2024-11-15 | [www.gob.mx] | ransomhub | Link |
| 2024-11-15 | [jhs.co.uk] | ransomhub | Link |
| 2024-11-15 | [potteau.com] | ransomhub | Link |
| 2024-11-15 | [A&O IT Group] | hunters | Link |
| 2024-11-15 | [Vector Transport (vectortransport.com)] | fog | Link |
| 2024-11-15 | [Bio-Clima Service Srl] | everest | Link |
| 2024-11-15 | [Total Patient Care LLC] | everest | Link |
| 2024-11-15 | [A Sensitive Touch Home Health;Alphastar Home Health Care;Heart of Texas Home Healthcare Se] | everest | Link |
| 2024-11-15 | [PHARMATIS-SAS] | incransom | Link |
| 2024-11-13 | [fortinainvestments.com] | ransomhub | Link |
| 2024-11-15 | [BluMed Health] | killsec | Link |
| 2024-11-14 | [Datron WorldCommunications] | akira | Link |
| 2024-11-14 | [Xtrim TVCable] | akira | Link |
| 2024-11-14 | [SKS Bottle &Packaging] | akira | Link |
| 2024-11-14 | [REV Engineering] | akira | Link |
| 2024-11-14 | [Bergeron LLC] | akira | Link |
| 2024-11-14 | [mk Technology Group] | akira | Link |
| 2024-11-14 | [Saint Andrews Bureau] | akira | Link |
| 2024-11-14 | [Ascend Packaging Systems] | akira | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-14 | [Tedkomp AB] | akira | Link |
| 2024-11-14 | [Pemberton Fabricators, Inc (Sexual Harassment videos inside)] | akira | Link |
| 2024-11-14 | [Burmeister &Wain Scandinavian Contractor] | akira | Link |
| 2024-11-14 | [Optical Cable Corporation] | akira | Link |
| 2024-11-14 | [Ultimus] | akira | Link |
| 2024-11-14 | [Tennis Canada] | akira | Link |
| 2024-11-14 | [Don’s MobileGlass] | akira | Link |
| 2024-11-14 | [Zyloware] | meow | Link |
| 2024-11-14 | [Pine Belt Cars] | meow | Link |
| 2024-11-14 | [DieTech North America] | meow | Link |
| 2024-11-14 | [Cottles Asphalt Maintenance Inc] | meow | Link |
| 2024-11-14 | [Herron Todd White] | meow | Link |
| 2024-11-14 | [J.S.T. Espana] | meow | Link |
| 2024-11-14 | [Karl Malone Toyota] | meow | Link |
| 2024-11-14 | [OMara Ag Equipment] | meow | Link |
| 2024-11-14 | [Pincu Barkan, Law Office and Notary] | everest | Link |
| 2024-11-14 | [ADT Freight Services Australia Pty Lt] | sarcoma | Link |
| 2024-11-14 | [Kumla Kommun] | hunters | Link |
| 2024-11-14 | [CP Construplan] | sarcoma | Link |
| 2024-11-13 | [Dumont Printing] | akira | Link |
| 2024-11-13 | [Berexco LLC] | akira | Link |
| 2024-11-13 | [Intercomp] | akira | Link |
| 2024-11-12 | [DynamicSystems] | medusa | Link |
| 2024-11-14 | [Popular Life Insurance] | sarcoma | Link |
| 2024-11-14 | [Micon National] | sarcoma | Link |
| 2024-11-14 | [Kelowna Springs] | sarcoma | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-13 | [stalyhill-inf.tameside.sch.uk] | blacksuit | Link |
| 2024-11-13 | [AXEON 360] | ciphbit | Link |
| 2024-11-13 | [COOPERATIVA TELEFONICA DE CALAFATE LTD.] | BrainCipher | Link |
| 2024-11-13 | [G-One Auto Parts de México S.A. de C.V.] | BrainCipher | Link |
| 2024-11-13 | [Schmack] | hunters | Link |
| 2024-11-13 | [Sercomm] | hunters | Link |
| 2024-11-13 | [midstatesindustrial.com] | threeam | Link |
| 2024-11-13 | [nanolive.ch 2.0] | apt73 | Link |
| 2024-11-05 | [formosacpa.com.tw] | kairos | Link |
| 2024-11-05 | [askyouraccountant.com] | kairos | Link |
| 2024-11-13 | [kansasrmc.com] | kairos | Link |
| 2024-11-13 | [Value Dental Center] | everest | Link |
| 2024-11-13 | [Artistic Family Dental] | everest | Link |
| 2024-11-13 | [Asaro Dental Aesthetics] | everest | Link |
| 2024-11-13 | [Axpr Valve Science] | killsec | Link |
| 2024-11-12 | [American Associated Pharmacies] | embargo | Link |
| 2024-11-12 | [Giggle Finance] | killsec | Link |
| 2024-11-12 | [Orange County Pathology Medical Group] | raworld | Link |
| 2024-11-12 | [SK Gas] | raworld | Link |
| 2024-11-03 | [Medigroup.ca] | ransomhub | Link |
| 2024-11-12 | [Hillandale Farms] | akira | Link |
| 2024-11-12 | [jst.es] | blacksuit | Link |
| 2024-11-12 | [jarrellimc.com] | blacksuit | Link |
| 2024-11-06 | [Banco de Fomento Internacional] | lynx | Link |
| 2024-11-11 | [TaxPros of Clermont] | lynx | Link |
| 2024-11-11 | [National Institute of Administration] | killsec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-07 | [DSZ] | lynx | Link |
| 2024-11-07 | [Future Metals] | lynx | Link |
| 2024-11-07 | [Plowman Craven] | lynx | Link |
| 2024-11-11 | [Supply Technologies] | blacksuit | Link |
| 2024-11-11 | [Maxxis International] | blacksuit | Link |
| 2024-11-11 | [potteau.be] | ransomhub | Link |
| 2024-11-11 | [Followmont TransportPty Ltd] | akira | Link |
| 2024-11-11 | [dezinecorp.com] | blacksuit | Link |
| 2024-11-11 | [Amourgis & Associates] | hunters | Link |
| 2024-11-11 | [Dietzgen Corporation] | hunters | Link |
| 2024-11-01 | [nynewspapers.com] | ransomhub | Link |
| 2024-11-11 | [comarchs.com] | ransomhub | Link |
| 2024-11-11 | [tolbertlegal.com] | ransomhub | Link |
| 2024-11-10 | [OxyHealth] | killsec | Link |
| 2024-11-10 | [Immuno Laboratories, Inc] | bianlian | Link |
| 2024-11-05 | [bitquail.com] | ransomhub | Link |
| 2024-11-09 | [ATSG, Inc] | bianlian | Link |
| 2024-11-09 | [Mizuno (USA)] | bianlian | Link |
| 2024-11-09 | [Palmisano & Goodman, P.A.] | bianlian | Link |
| 2024-11-09 | [Finger Beton Unternehmensgruppe] | meow | Link |
| 2024-11-09 | [Karman Inc] | meow | Link |
| 2024-11-09 | [Siltech (siltechcorp.local)] | lynx | Link |
| 2024-11-09 | [emefarmario.com.br] | apt73 | Link |
| 2024-11-09 | [Granite School District] | rhysida | Link |
| 2024-11-09 | [WimCoCorp] | lynx | Link |
| 2024-11-09 | [NEBRASKALAND] | lynx | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-08 | [MENZIES CNAC (Jardine Aviation Services, Agility)] | spacebears | Link |
| 2024-11-08 | [bartleycorp.com] | ransomhub | Link |
| 2024-11-08 | [interlabel.be] | ransomhub | Link |
| 2024-11-07 | [del-electric.com] | ransomhub | Link |
| 2024-11-08 | [liftkits4less.com] | apt73 | Link |
| 2024-11-08 | [www.lamaisonducitron.com] | apt73 | Link |
| 2024-11-08 | [www.baldinger-ag.ch] | apt73 | Link |
| 2024-11-07 | [Marisa S.A] | medusa | Link |
| 2024-11-08 | [www.assurified.com] | apt73 | Link |
| 2024-11-08 | [www.botiga.com.uy] | apt73 | Link |
| 2024-11-08 | [Healthcare Management Systems] | bianlian | Link |
| 2024-11-08 | [MedElite Group] | everest | Link |
| 2024-11-07 | [nelconinc.biz] | ransomhub | Link |
| 2024-11-07 | [www.bluco.com] | ransomhub | Link |
| 2024-11-07 | [naj.ae] | darkvault | Link |
| 2024-11-07 | [Equator Worldwide] | meow | Link |
| 2024-11-07 | [Lexco] | meow | Link |
| 2024-11-07 | [europe-qualité] | incransom | Link |
| 2024-11-07 | [Winnebago Public School Foundation] | interlock | Link |
| 2024-11-05 | [Alliance Technical Group] | medusa | Link |
| 2024-11-06 | [Jomar Electrical Contractors] | medusa | Link |
| 2024-11-06 | [Howell Electric Inc] | medusa | Link |
| 2024-11-06 | [www.msdl.ca] | ransomhub | Link |
| 2024-11-07 | [Postcard Mania] | play | Link |
| 2024-11-07 | [New Law] | hunters | Link |
| 2024-11-06 | [klinkamkurpark] | helldown | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-06 | [AMERICANVENTURE] | helldown | Link |
| 2024-11-06 | [CSIKBS] | helldown | Link |
| 2024-11-06 | [SANJACINTOCOUNY] | helldown | Link |
| 2024-11-06 | [brandenburgerplumbing.com] | ransomhub | Link |
| 2024-11-06 | [arcoexc.com] | ransomhub | Link |
| 2024-11-06 | [Lincoln University] | meow | Link |
| 2024-11-06 | [Cape Cod Regional Technical High School (capetech.us)] | fog | Link |
| 2024-11-06 | [GSR Andrade Architects (gsr-andrade.com)] | fog | Link |
| 2024-11-05 | [metroelectric.com] | ransomhub | Link |
| 2024-11-05 | [sector5.ro] | ransomhub | Link |
| 2024-11-05 | [Paragon Plastics] | play | Link |
| 2024-11-05 | [Delfin Design & Manufacturing] | play | Link |
| 2024-11-05 | [Smitty’s Supply] | play | Link |
| 2024-11-05 | [S & W Kitchens] | play | Link |
| 2024-11-05 | [Dome Construction] | play | Link |
| 2024-11-06 | [Interoute agency] | lynx | Link |
| 2024-11-06 | [LmayInteroute agency] | lynx | Link |
| 2024-11-05 | [pacificglazing.com] | ransomhub | Link |
| 2024-11-05 | [nwhealthporter.com] | ransomhub | Link |
| 2024-11-05 | [wexfordcounty.org] | embargo | Link |
| 2024-11-05 | [ebrso] | qilin | Link |
| 2024-11-05 | [Model Die & Mold] | lynx | Link |
| 2024-11-04 | [mh-m.org] | embargo | Link |
| 2024-11-05 | [Falco Sult] | bianlian | Link |
| 2024-11-05 | [apoyoconsultoria.com] | ransomhub | Link |
| 2024-11-05 | [Webb Institute] | incransom | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-05 | [Fylde Coast Academy Trust] | rhysida | Link |
| 2024-11-04 | [sundt.com] | ransomhub | Link |
| 2024-11-04 | [Memorial Hospital & Manor] | embargo | Link |
| 2024-11-02 | [Scolari] | dragonforce | Link |
| 2024-11-05 | [McMillan Electric Company] | medusa | Link |
| 2024-11-04 | [maxdata.com.br] | ransomhub | Link |
| 2024-11-04 | [goodline.com.au] | ransomhub | Link |
| 2024-11-04 | [kenanasugarcompany.com] | ransomhub | Link |
| 2024-11-04 | [www.schweiker.de] | ransomhub | Link |
| 2024-11-04 | [www.drbutlerandassociates.com] | ransomhub | Link |
| 2024-11-04 | [www.mssupply.com] | ransomhub | Link |
| 2024-11-04 | [fullfordelectric.com] | ransomhub | Link |
| 2024-11-04 | [College of Business - Tanzania] | hellcat | Link |
| 2024-11-04 | [Ministry of Education - Jordan] | hellcat | Link |
| 2024-11-04 | [Schneider Electric - France] | hellcat | Link |
| 2024-11-04 | [International University of Sarajevo] | medusa | Link |
| 2024-11-04 | [Whitaker Construction Group] | medusa | Link |
| 2024-11-04 | [European External Action Service (EEAS)] | hunters | Link |
| 2024-11-04 | [csucontracting.com] | ransomhub | Link |
| 2024-11-04 | [redphoenixconstruction.com] | ransomhub | Link |
| 2024-11-04 | [Air Specialists Heating & Air Conditioning] | hunters | Link |
| 2024-11-03 | [krigerconstruction.com] | ransomhub | Link |
| 2024-11-03 | [caseconstruction.com] | ransomhub | Link |
| 2024-11-03 | [lambertstonecommercial.com] | ransomhub | Link |
| 2024-11-04 | [Doctor 24x7] | killsec | Link |
| 2024-11-03 | [Hemubo] | hunters | Link |
| 2024-11-03 | [Elad municipality] | handala | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-11-03 | [Russell Law Firm, LLC] | bianlian | Link |
| 2024-11-03 | [L & B Transport, L.L.C.] | bianlian | Link |
| 2024-11-03 | [guardianhc] | stormous | Link |
| 2024-11-02 | [bravodigitaltrader.co.uk] | ransomhub | Link |
| 2024-11-02 | [SVP Worldwide] | blacksuit | Link |
| 2024-11-02 | [Sumitomo] | killsec | Link |
| 2024-11-01 | [DieTech North America] | qilin | Link |
| 2024-11-01 | [www.fatboysfleetandauto.com] | ransomhub | Link |
| 2024-11-01 | [lighthouseelectric.com] | ransomhub | Link |
| 2024-11-01 | [JS McCarthy Printers] | play | Link |
| 2024-11-01 | [CGR Technologies] | play | Link |
| 2024-11-01 | [United Sleep Diagnostics] | medusa | Link |
| 2024-11-01 | [eap.gr] | ransomhub | Link |
| 2024-11-01 | [vikurverk.is] | lockbit3 | Link |
| 2024-11-01 | [mirandaproduce.com.ve] | lockbit3 | Link |
| 2024-11-01 | [Cerp Bretagne Nord] | hunters | Link |
| 2024-11-01 | [Hope Valley Recovery] | rhysida | Link |
| 2024-11-01 | [lsst.ac] | cactus | Link |
| 2024-11-01 | [MCNA Dental] | everest | Link |
| 2024-11-01 | [Arctrade] | everest | 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
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

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