NOZOMI NETWORKS LABS

Zusammenfassung

OT-/IoT-Sicherheitsbericht

Ein genauer Blick auf die ICS-Bedrohungslandschaft

2022 2H Rezension | Januar 2023

Zusammenfassung

Angesichts ständig neuer böswilliger Akteure und Taktiken befindet sich die Landschaft der Cyber-Bedrohungen in einem ständigen Wandel.

Mit dem technologischen Fortschritt nutzen Cyberkriminelle immer fortschrittlichere Methoden, um Zugang zu vertraulichen Informationen zu erhalten oder gefährliche Cyberangriffe zu starten. Mit dem Aufkommen des Internet of Things (IoT) haben Kriminelle nun Zugang zu einer Vielzahl von vernetzten Geräten und können nun über verschiedene Einstiegspunkte in die Netzwerke eindringen.

Die Zahl der Cyberangriffe hat in den letzten sechs Monaten immens zugenommen und zu erheblichen Störungen in verschiedenen Branchen geführt – vom Verkehrssektor bis hin zum Gesundheitswesen. Vor allem der Eisenbahnsektor war Gegenstand von Angriffen, die zur Einführung von Maßnahmen zum Schutz der Bahnbetreiber und ihrer Vermögenswerte führten.

Daneben haben Hacktivisten Wiper-Malware eingesetzt, um kritische Infrastrukturen zu destabilisieren und damit ihre politische Position im russisch-ukrainischen Krieg zu stärken.

Angesichts der Weiterentwicklung und Intensivierung von Cyber-Bedrohungen ist es für Organisationen und Unternehmen wichtig zu verstehen, welche Ziele Bedrohungsakteure im Bereich OT/IoT verfolgen und welche Maßnahmen erforderlich sind, um kritische Anlagen vor Bedrohungsakteuren zu schützen.

Dieser Bericht befasst sich mit folgenden Themen:

- **Cyberangriffe** auf kritische Infrastrukturen in den letzten 6 Monaten
- **Hacktivisten** nutzen Malware, um destruktive Angriffe zu starten
- **Krankenhaussysteme** geraten zunehmend ins Visier
- **Cyberangriffe auf den Schienenverkehr** und neue Schutzrichtlinien
- **OT-Umgebungen** betreffende Warnungen vor unbefugtem Zugriff
- **Malware-Kategorien**, die Unternehmen, OT und IoT beeinträchtigen
- **Empfehlungen** und Prognose für 2023

2022 2H BEDROHUNGSLANDSCHAFT

Juli bis September 2022

Exklusive Einblicke aus den IoT-Honeypots von Nozomi Networks:

Protokolle mit fest codierten Anmeldeinformationen

Länder mit den meisten Angreifern

Am häufigsten verwendete Anmeldeinformationen

Eindeutige IP-Adressen der Angreifer

IP-Adressen der Angreifer

Am häufigsten ausgeführte Befehle

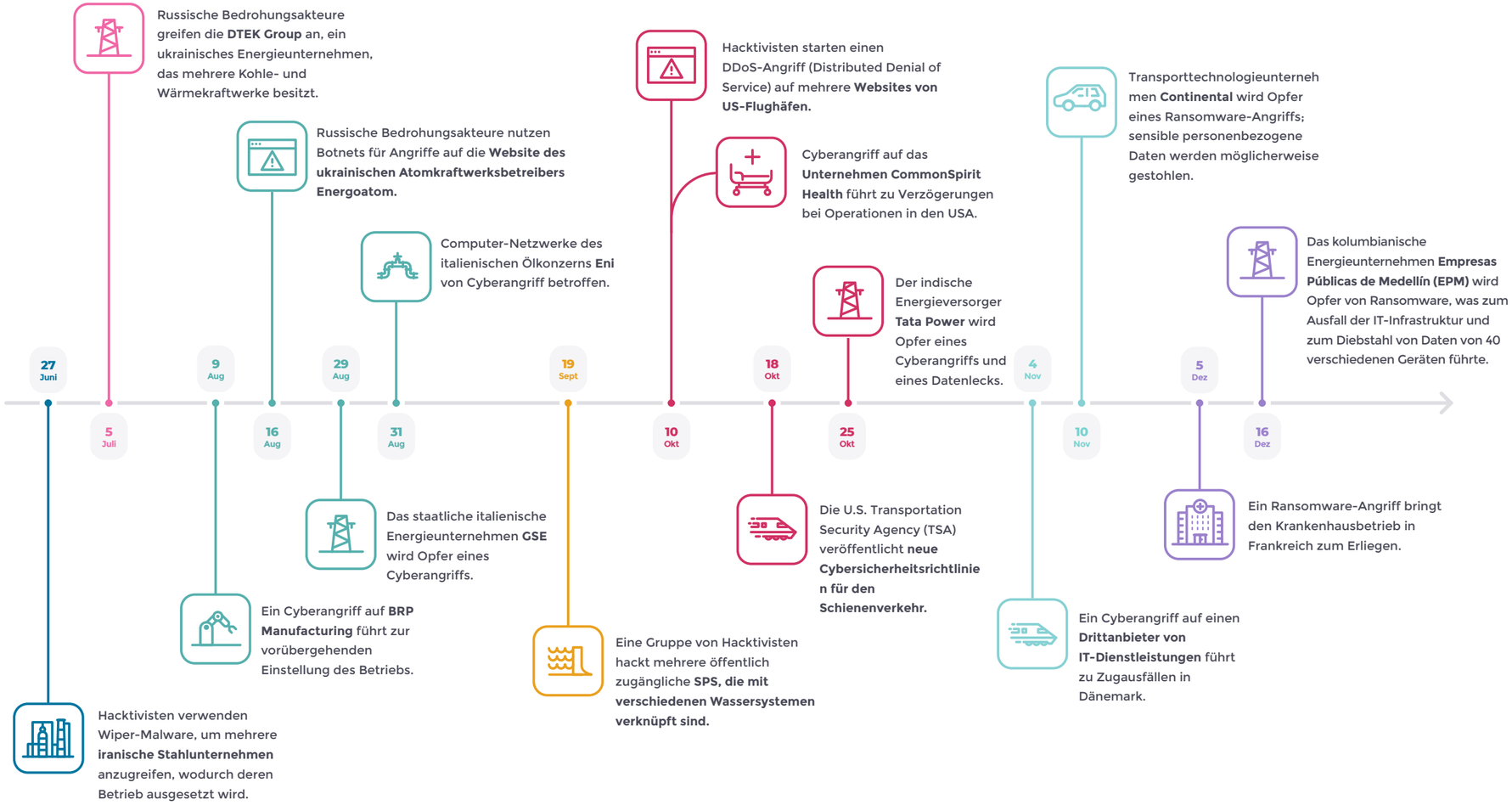
Zeitleiste bemerkenswerter Cyber-Ereignisse in der zweiten Hälfte des Jahres 2022:

Diese Zeitleiste fasst die wichtigsten Cyber-Ereignisse – Cyberangriffe, neue Richtlinien, Malware usw. – von Juli bis Dezember 2022 zusammen.

In der ersten Jahreshälfte haben wir die Auswirkungen des Krieges zwischen Russland und der Ukraine auf die Cyber-Bedrohungslandschaft gesehen.

In der zweiten Jahreshälfte 2022 fanden weiterhin disruptive Cyberangriffe auf kritische Infrastrukturen statt, einschließlich des Schienenverkehrs, der Krankenhäuser, des verarbeitenden Gewerbes und des Energiesektors.

Hacktivisten verlagern ihre Taktik von Datendiebstahl und DDoS-Angriffen (Distributed Denial of Service) auf den Einsatz von Wiper-Malware, um kritische Infrastrukturen zu stören.



Dieser Bericht enthält einzigartige Daten, die aus den IoT-Honypots von Nozomi Networks Labs gesammelt wurden. Diese passiven Sicherheitssysteme werden eingesetzt, um potenzielle Angreifer aufzuspüren, indem sie ein Objekt simulieren, das für den Angreifer von Wert ist. In der zweiten Hälfte des Jahres 2022 haben wir Folgendes erfasst:

- **Protokolle mit fest codierten Anmeldeinformationen:** Telnet ist derzeit häufiger Ziel von Angriffen als SSH, wobei Telnet zu 70 % und SSH zu 30 % betroffen ist.
- **Länder mit den meisten Angreifern:** Geräte in den Vereinigten Staaten, China und Südkorea werden von Angreifern häufiger für Angriffe genutzt als Geräte in anderen Ländern.
- **Am häufigsten verwendete Anmeldeinformationen:** Die Standard-Anmeldeinformationen werden weiterhin verwendet, allerdings doppelt oder dreimal so häufig, was auf die Anwesenheit zusätzlicher Botnets hinweist, die versuchen, sich Zugang zu verschaffen.
- **Höchste Anzahl eindeutiger IP-Adressen der Angreifer:** Im Juli, Oktober und November gab es deutliche Spitzen bei der Anzahl der eindeutigen IP-Adressen, die auf OT/IoT abzielten.
- **Häufigste IP-Adressen der Angreifer:** Bösartige IP-Adressen versuchten auf unsere IoT-Honeypots zuzugreifen, wobei der Top-Eintrag mit über 60.000 Zugriffsversuchen verbunden war – eine Verdoppelung seit unserem letzten Bericht.

DIE 4 AM HÄUFIGSTEN AUSGEFÜHRTEN BEFEHLE

1. enable
2. shell
3. sh
4. system

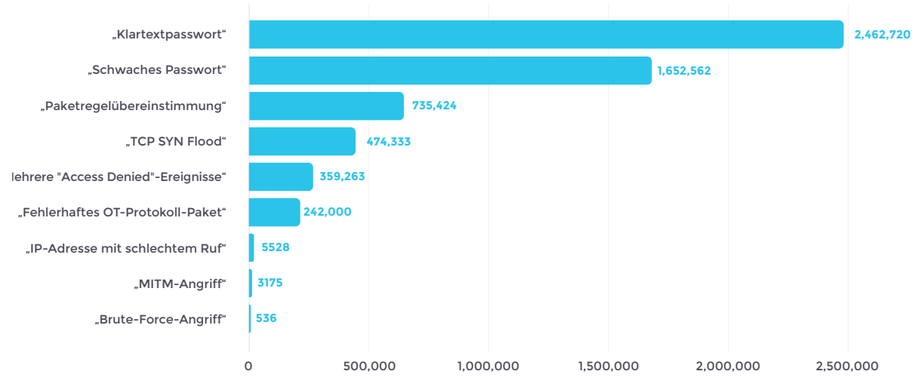
Diese Befehle sind im Vergleich zu den anderen Befehlen **weiter verbreitet** und in den **Skripten mehrerer Malware-Familien zu finden**.

Angriffsstatistiken aus dem ICS-Bereich

Juli bis September 2022

Kritischste Arten von Warnungen vor unbefugtem Zugriff

Bedrohungsakteure können **„Klartextkennwörter“** und **„schwache Kennwörter“** stehlen, um sich unbefugten Zugang zu Geräten zu verschaffen. Diese Warnungen können in Verbindung mit **„mehreren verweigerten Zugriffsereignissen“** innerhalb einer kurzen Zeitspanne auf einen potenziellen Brute-Force-Angriff hindeuten. Andere Warnungen wie **„TCP SYN Flood“**, bei denen der Bedrohungsakteur einen Server mit Verbindungsanfragen überflutet, könnten auch auf einen versuchten Denial-of-Service-Angriff (DoS) hinweisen.



Eine vollständige Auflistung der Daten ist im ausführlichen Bericht zu finden.

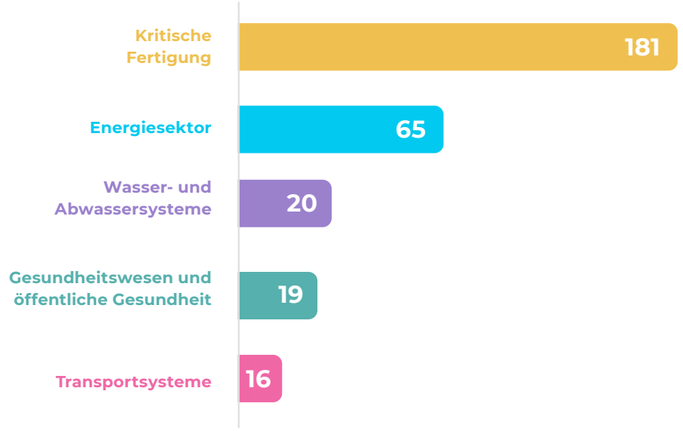
Die am häufigsten erkannten Malware-Kategorien

In den letzten sechs Monaten waren **Trojaner** die am häufigsten entdeckte Malware, mit der Unternehmensnetzwerke angegriffen wurden, **Remote Access Tools (RATs)** zielten auf OT und **DDoS-Malware** auf IoT-Geräte.

Die Bedrohungslandschaft durch Schwachstellen

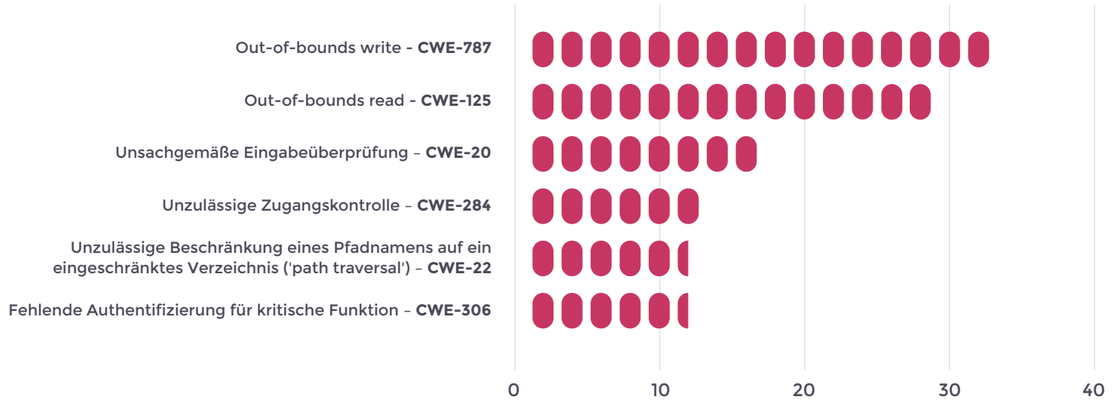
Wir haben die von der CISA veröffentlichten ICS-CERT-Hinweise von Juli bis Dezember 2022 analysiert.

Die 5 wichtigsten Branchen, die von den gemeldeten Schwachstellen betroffen sind



Es sind zwei weitere gefährdete Branchen hinzugekommen: Wasser- und Abwassersysteme sowie Transportsysteme.
Dies spiegelt die verschiedenen Cyberangriffe wider, die wir in diesem Jahr auf Wasseraufbereitungsanlagen und Bahn-/Transitsysteme gemeldet haben.

Diese Grafik veranschaulicht die wichtigsten Common Weakness Enumerations (CWEs) im Zusammenhang mit CVEs, die in der zweiten Hälfte des Jahres 2022 veröffentlicht wurden.



Out-of-Bounds Write (CWE – 787) und Out-of-Bounds Read (CWE – 125) sind im Vergleich zur ersten Jahreshälfte deutlich gestiegen.
Die Kenntnis dieser häufigen Software- und Hardwaresicherheitslücken kann Organisationen Aufschluss darüber geben, wie sie ihre Netzwerke besser schützen können.

Empfehlungen

Nach den Beobachtungen im Jahr 2022 wird die Cyber-Bedrohungslandschaft im Jahr 2023 voraussichtlich weiterhin von Komplexität und Raffinesse geprägt sein, da die Angreifer ihre Strategien zur Ausnutzung anfälliger Systeme und Netzwerke weiterentwickeln.

Um sich vor potenziellen Bedrohungen zu schützen, sollten Organisationen mit kritischen Infrastrukturen proaktiven Verteidigungsstrategien Vorrang einräumen:

- Segmentierung des Netzwerks
- Erkennung von Geräten
- Schwachstellenmanagement
- Patching
- Protokollierung
- Endpunkt-Erkennung
- Threat Intelligence

Organisationen sollten ihre Systeme jetzt proaktiv schützen, damit sie 2023 besser gegen mögliche Cyber-Bedrohungen gewappnet sind.

Was ist im Jahr 2023 zu erwarten?

1. Taktiken der hybriden Bedrohung

Es wird immer schwieriger werden, die Arten von Bedrohungsakteuren anhand von TTPs und Motiven zu kategorisieren, was in der Vergangenheit bei der Zuordnung von Angriffen hilfreich war.

3. Exploits bei medizinischen Geräten

Neben der Nutzung von Scannern zur Ausnutzung von Schwachstellen können Bedrohungsakteure auch auf medizinische Systeme zugreifen, die zur Sammlung von Gerätedaten für eine umfassendere Analyse und Überwachung verwendet werden. Diese Manipulation kann zu Fehlfunktionen, Fehleinschätzungen oder sogar Überdosierungen bei der automatischen Medikamentenabgabe führen.

5. KI-gesteuerte Chatbots, die für bösartige Zwecke eingesetzt werden

Mit der zunehmenden Komplexität dieser Systeme können böswillige Akteure sie zum Schreiben von Schadcode oder zum Ausnutzen von Sicherheitslücken nutzen. Sie können auch missbraucht werden, um überzeugendere und grammatikalisch korrekte Phishing-/Social-Engineering-Texte zu erstellen. All dies könnte die Zeit, die für die Entwicklung gezielter Bedrohungskampagnen benötigt wird, verkürzen und damit die Häufigkeit von Cyberangriffen erhöhen.

2. Quantenbedrohungen und Vorbereitung

Da Bedrohungsakteure in Vorbereitung auf die Quantenentschlüsselung die Technik „Jetzt speichern, später entschlüsseln“ (SNDL) anwenden, bietet die CISA einen Leitfaden an, der Unternehmen helfen soll, ihren Datenbestand bereits jetzt zu schützen, um das Risiko einer späteren Quantenentschlüsselung zu verringern.

4. Wendepunkt bei der Cyberversicherung

Cyber-Kriminelle informieren sich über Versicherungspolicen und passen ihre Lösegeldforderungen so an, dass sie der Höhe der Auszahlung einer Cyber-Versicherung entsprechen. Dies könnte entweder zu einem erheblichen Anstieg der Prämien führen oder sogar die Ressourcen von Cyber-Versicherungen erschöpfen, so dass die Geltendmachung schwerwiegender Schäden und die Erstattung entsprechender Zahlungen erschwert werden.

6. Fachleute für Cybersicherheit müssen neue Fähigkeiten erlernen

Fachleute für Cybersicherheit müssen sich schnell auf neue Bedrohungen einstellen und neue Wege zum Schutz ihrer Umgebungen finden.

OT-/IoT-Sicherheitsbericht herunterladen

Nozomi Networks Labs analysiert die aktuelle Bedrohungslandschaft und teilt Folgendes mit:

- Jüngste Hacktivisten-Angriffe auf kritische Infrastrukturen
- Schwachstellen von ICS-/OT-/IoT-Geräten und Ausnutzungstrends
- Prognosen für die Cybersicherheitslandschaft im Jahr 2023

Herunterladen

nozominetworks.com

Cybersicherheit und Analysen für Ihre vernetzten Geräte

Nozomi Networks ist der führende Anbieter von Lösungen für OT- und IoT-Sicherheit und -Transparenz. Nozomi Networks beschleunigt die digitale Transformation, indem es kritische Infrastrukturen, Industrie und Regierungsorganisationen der Welt vor Cyber-Bedrohungen schützt. Unsere Lösung bietet außergewöhnliche Netzwerk- und Asset-Visibilität, Bedrohungserkennung und Einblicke in OT- und IoT-Umgebungen. Kunden verlassen sich auf uns, um Risiken und Komplexität zu minimieren und gleichzeitig die betriebliche Ausfallsicherheit zu maximieren.

NN-SEC-RP-ES-2022-2H-DE-001