Bedrohungen verstehen, Angriffe verhindern:

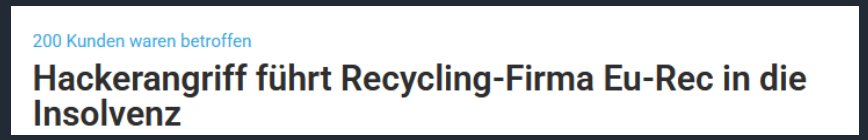
Cyber Threat Intelligence für Unternehmen

IHK Bayern | 08.05.2025

UR.ifs NTNU

Ein kurzer Blick auf die aktuelle Bedrohungslage

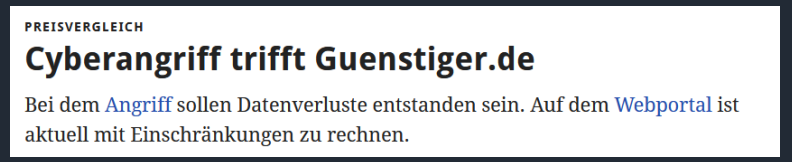
Quelle: giessener-allgemeine.de (6. Mai)



Quelle: it-daily.de (28. April)

Quelle: theguardian.com (2. Mai)

Quelle: swr.de (5. Mai)



Quelle: golem.de (24. April)

Quelle: textilwirtschaft.de (2. Mai)

Kollaborative Sicherheit durch **Cyber Threat Intelligence** wird zur neuen Notwendigkeit.

Cyber Threat Intelligence

Die Sammlung, Analyse und Verbreitung von **Informationen über aktuelle oder potenzielle Bedrohungen** in der Cybersicherheit. Ziel ist es, Organisationen dabei zu unterstützen, **proaktiv auf Cyberangriffe zu reagieren** und ihre Sicherheitsmaßnahmen zu verbessern, indem sie Einblicke in Angreifermethoden zu erhalten.

Inhalt des Workshops

1) Welche **Formen von Cyber Threat Intelligence** gibt es?

2) Wie können diese jeweils **konkret angewendet werden**, um die Sicherheit in Ihren Unternehmen zu verbessern?

3) An welchen Stellen des **Security Lifecycles** unterstützen welche Arten von CTI

Überblick

Indicators of Compromise
CVEs
Threat Reports
Threat Advisories
Strategic Reports
Playbooks

Arten von
Cyber Threat Intelligence

Indicators of Compromise (IoC)

Können auf eine mögliche Kompromittierung hinweisen. Diese können **IP-Adressen, Domain-Namen, Dateihashes, URLs** oder andere technische Artefakte sein, die verwendet werden, um bösartige Aktivitäten zu identifizieren.

Beispiele

IP-Adresse: 192.168.1.100 (bekannt als Command-and-Control-Server)

Dateihash (SHA-256): e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 (Malware-Sample)

Domain: malicious-example.com (Phishing-Seite)

1	108.62.12[.]105
2	108.62.12[.]114
3	108.62.12[.]116
4	108.62.12[.]119
5	108.62.12[.]121
6	108.177.235[.]53
7	108.62.12[.]12
8	172.241.27[.]65
9	172.241.27[.]68
10	172.241.27[.]70
11	45.153.241[.]1
12	45.138.172[.]95
13	45.147.229[.]52
14	45.147.229[.]68
15	45.147.229[.]92
16	45.147.230[.]87
17	45.147.229[.]180
18	45.147.230[.]131
19	45.147.230[.]132
20	45.147.230[.]133
21	45.147.230[.]140
22	45.147.230[.]141
23	45.147.230[.]159
24	45.147.231[.]222

Quelle: https://github.com/swisscom/detections

Indicators of Compromise (IoC)

Use Case. Unternehmen erhält E-Mail mit einem Link, der zu einem Webserver mit Malware führt (Phishing Link)
→ Domain der Phishing-Seite und/oder Mail-Adresse wurden präventiv schon blockiert

Mögliche Quellen.

1	108.62.12[.]105
2	108.62.12[.]114
3	108.62.12[.]116
4	108.62.12[.]119
5	108.62.12[.]121
6	108.177.235[.]53
7	108.62.12[.]12
8	172.241.27[.]65
9	172.241.27[.]68
10	172.241.27[.]70
11	45.153.241[.]1
12	45.138.172[.]95
13	45.147.229[.]52
14	45.147.229[.]68
15	45.147.229[.]92
16	45.147.230[.]87
17	45.147.229[.]180
18	45.147.230[.]131
19	45.147.230[.]132
20	45.147.230[.]133
21	45.147.230[.]140
22	45.147.230[.]141
23	45.147.230[.]159
24	45.147.231[.]222

Quelle: https://github.com/swisscom/detections

CVEs

Common Vulnerabilities and Exposures (CVEs) sind systematisierte und katalogisierte Schwachstellen in Software und Hardware.

Beispiel

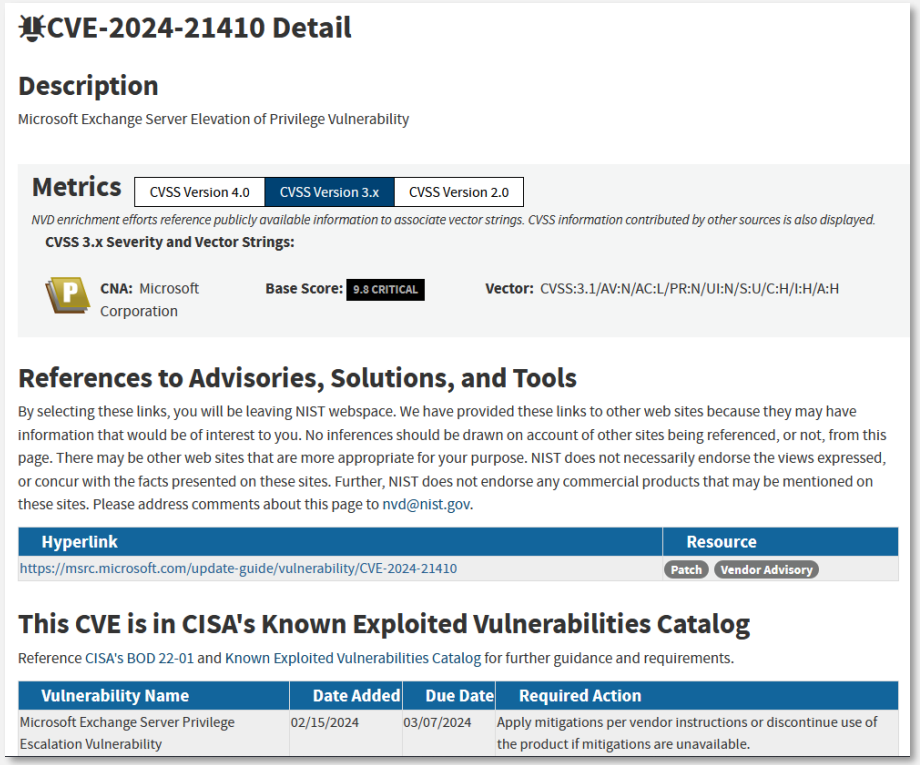
CVE-2024-38189

Description: Microsoft Project Remote Code Execution Vulnerability

Date Added: 08/13/2024

Due Date: 09/03/2024

Requried Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable



CVE-2024-21410 Detail

Description

Microsoft Exchange Server Elevation of Privilege Vulnerability

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Microsoft Corporation **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410	Patch, Vendor Advisory

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Microsoft Exchange Server Privilege Escalation Vulnerability	02/15/2024	03/07/2024	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Quelle: https://nvd.nist.gov/vuln/detail/CVE-2024-21410

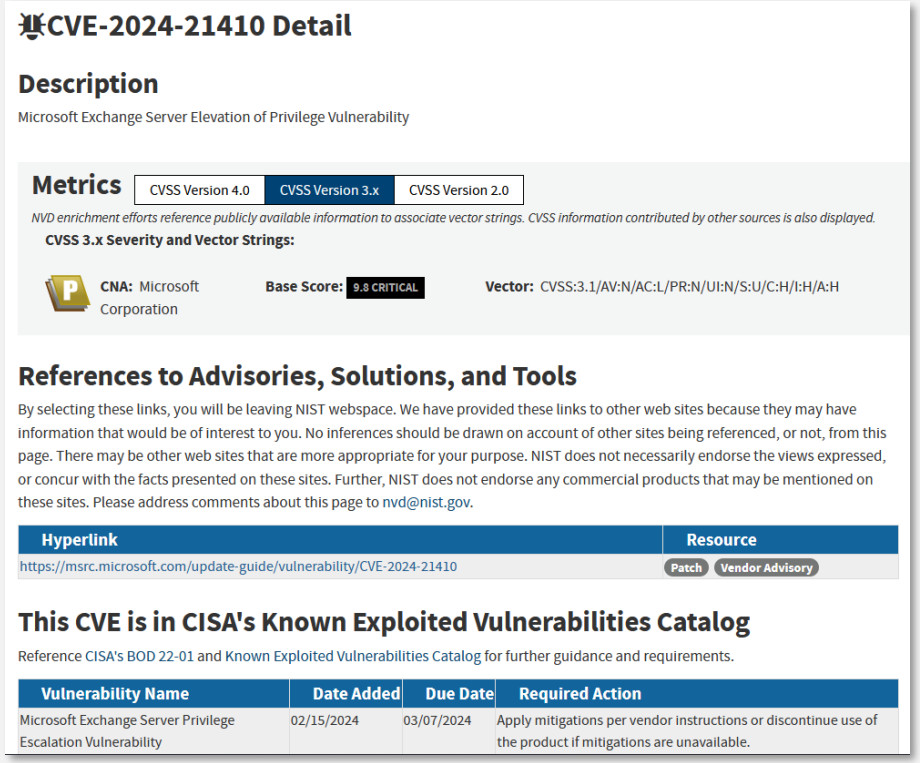
CVEs

Use Cases. Systeme (Firewall, IDS) entsprechend konfigurieren; Syteme patchen; ggf. in Kombination mit Threat Advisories

Voraussetzungen. Asset Management, Mitarbeiterexpertise

Quellen.

- cve.org (MITRE)
- NIST



CVE-2024-21410 Detail

Description

Microsoft Exchange Server Elevation of Privilege Vulnerability

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Microsoft Corporation **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

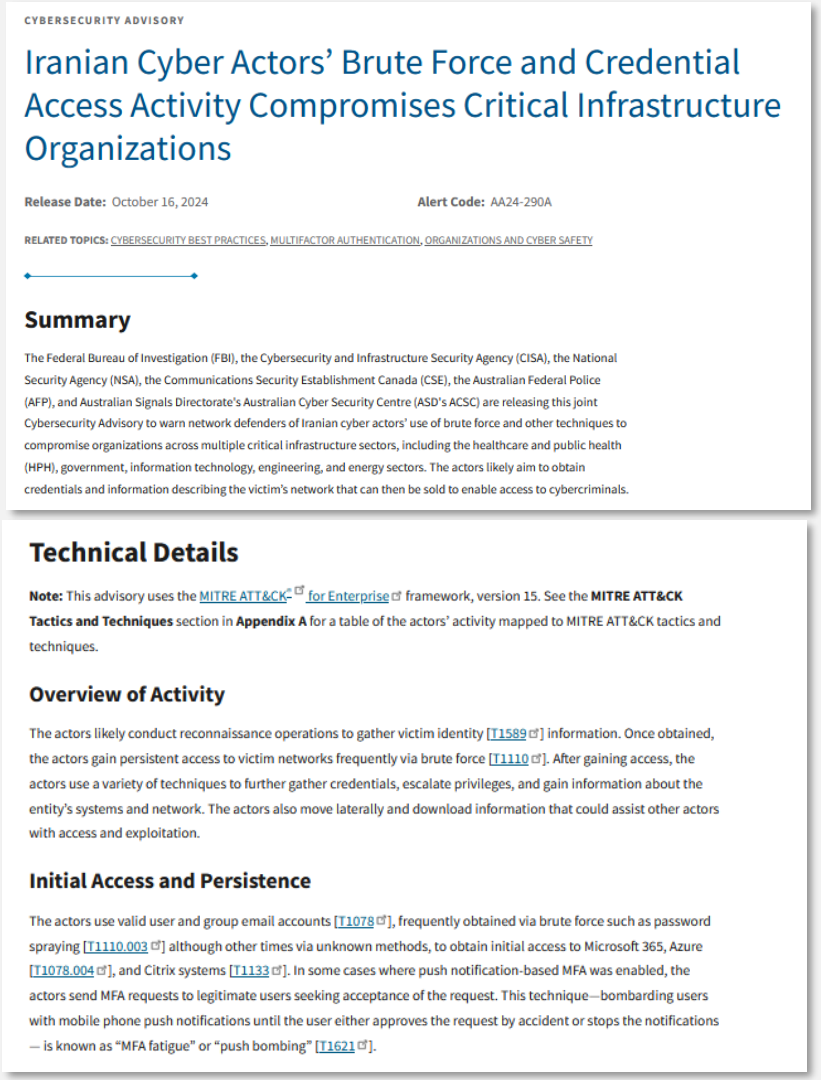
Hyperlink	Resource
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410	Patch, Vendor Advisory

This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

Vulnerability Name	Date Added	Due Date	Required Action
Microsoft Exchange Server Privilege Escalation Vulnerability	02/15/2024	03/07/2024	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Quelle: https://nvd.nist.gov/vuln/detail/CVE-2024-21410



CYBERSECURITY ADVISORY

Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations

Release Date: October 16, 2024 **Alert Code:** AA24-290A

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, MULTIFACTOR AUTHENTICATION, ORGANIZATIONS AND CYBER SAFETY

Summary

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Communications Security Establishment Canada (CSE), the Australian Federal Police (AFP), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory to warn network defenders of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The actors likely aim to obtain credentials and information describing the victim's network that can then be sold to enable access to cybercriminals.

Technical Details

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 15. See the **MITRE ATT&CK Tactics and Techniques** section in **Appendix A** for a table of the actors' activity mapped to MITRE ATT&CK tactics and techniques.

Overview of Activity

The actors likely conduct reconnaissance operations to gather victim identity [T1589] information. Once obtained, the actors gain persistent access to victim networks frequently via brute force [T1110]. After gaining access, the actors use a variety of techniques to further gather credentials, escalate privileges, and gain information about the entity's systems and network. The actors also move laterally and download information that could assist other actors with access and exploitation.

Initial Access and Persistence

The actors use valid user and group email accounts [T1078], frequently obtained via brute force such as password spraying [T1110.003] although other times via unknown methods, to obtain initial access to Microsoft 365, Azure [T1078.004], and Citrix systems [T1133]. In some cases where push notification-based MFA was enabled, the actors send MFA requests to legitimate users seeking acceptance of the request. This technique—bombarding users with mobile phone push notifications until the user either approves the request by accident or stops the notifications — is known as "MFA fatigue" or "push bombing" [T1621].

Quelle: https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

Threat Advisories

Threat Advisories sind **Benachrichtigungen über aktuelle Schwachstellen**. Sie enthalten oft sofort umsetzbare Ratschläge.

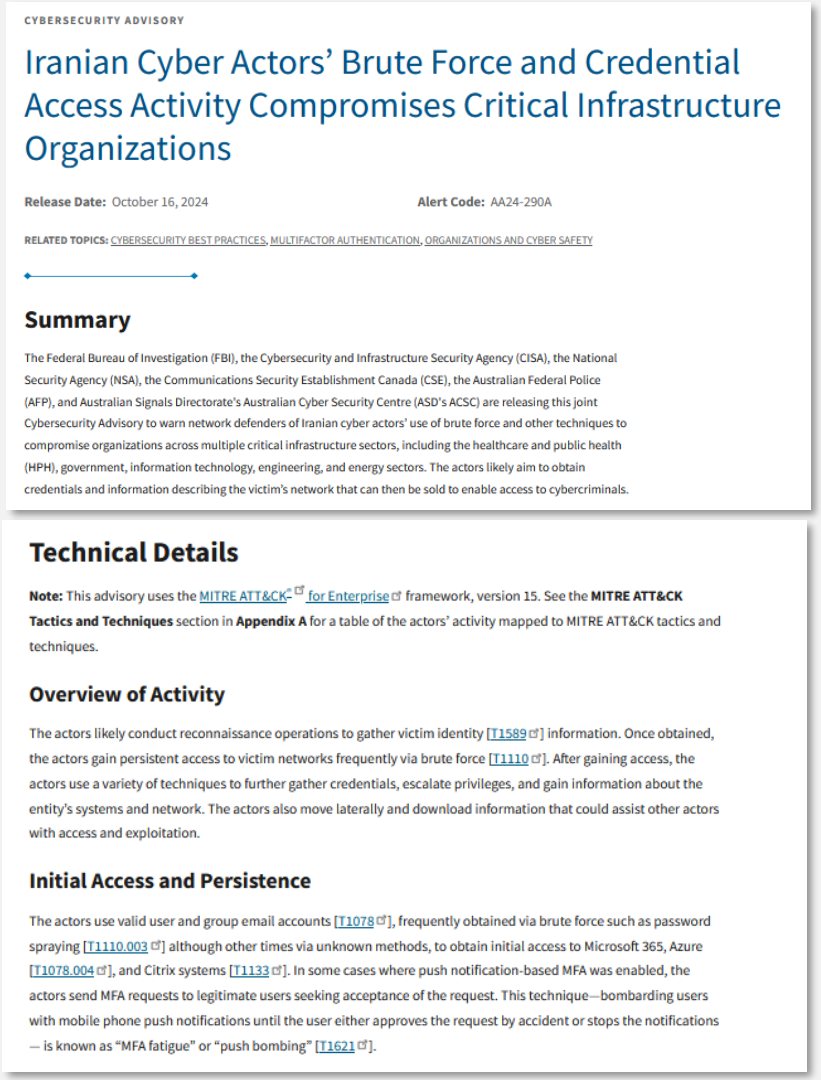
Titel: Dringende Warnung vor neuer Schwachstelle in Microsoft Exchange Server

Beschreibung: Kritische Zero-Day-Schwachstelle (CVE-2024-21410) in Microsoft Exchange Server entdeckt

Risiko: Remote Code Execution

Betroffene Versionen: Exchange Server 2013, 2016, 2019

Empfohlene Maßnahmen: Sofortige Anwendung des veröffentlichten Sicherheitsupdates, Überprüfung der Server-Logs auf verdächtige Aktivitäten



CYBERSECURITY ADVISORY

Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations

Release Date: October 16, 2024 **Alert Code:** AA24-290A

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, MULTIFACTOR AUTHENTICATION, ORGANIZATIONS AND CYBER SAFETY

Summary

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Communications Security Establishment Canada (CSE), the Australian Federal Police (AFP), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory to warn network defenders of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The actors likely aim to obtain credentials and information describing the victim's network that can then be sold to enable access to cybercriminals.

Technical Details

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 15. See the **MITRE ATT&CK Tactics and Techniques** section in **Appendix A** for a table of the actors' activity mapped to MITRE ATT&CK tactics and techniques.

Overview of Activity

The actors likely conduct reconnaissance operations to gather victim identity [T1589] information. Once obtained, the actors gain persistent access to victim networks frequently via brute force [T1110]. After gaining access, the actors use a variety of techniques to further gather credentials, escalate privileges, and gain information about the entity's systems and network. The actors also move laterally and download information that could assist other actors with access and exploitation.

Initial Access and Persistence

The actors use valid user and group email accounts [T1078], frequently obtained via brute force such as password spraying [T1110.003] although other times via unknown methods, to obtain initial access to Microsoft 365, Azure [T1078.004], and Citrix systems [T1133]. In some cases where push notification-based MFA was enabled, the actors send MFA requests to legitimate users seeking acceptance of the request. This technique—bombarding users with mobile phone push notifications until the user either approves the request by accident or stops the notifications — is known as "MFA fatigue" or "push bombing" [T1621].

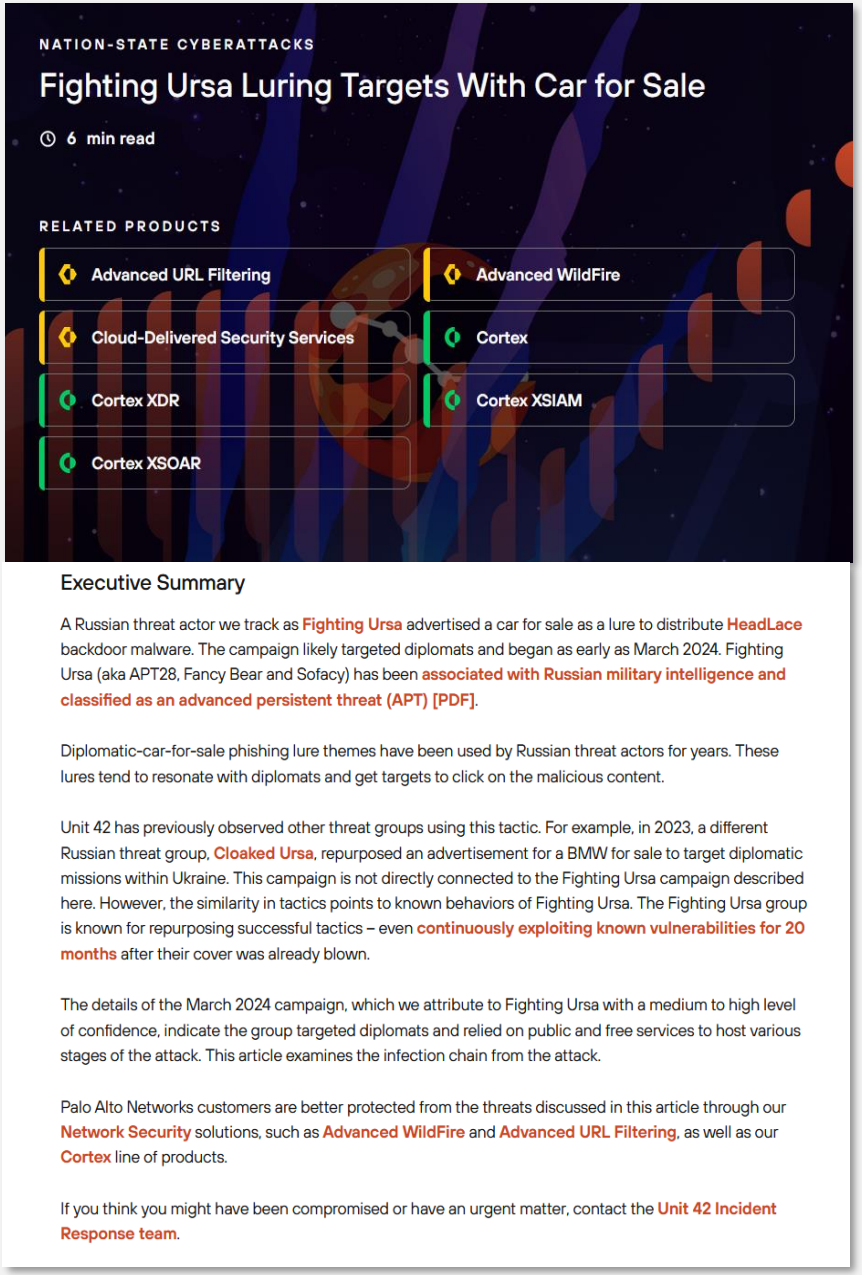
Quelle: https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

Threat Advisories

Use Case.
Advisories nach das Unternehmen betreffende Infrastruktur filter; Handlungsanweisungen in Advisories direkt umsetzen (z.B. Software-Patch).

Mögliche Quellen.

- CISA
- BSI
- Hersteller (z.B. Microsoft, Siemens, etc.)



Quelle: https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

Threat Reports

Threat Reports sind **detaillierte Berichte über spezifische Bedrohungsakteure** oder -kampagnen. Sie beinhalten Informationen über **Taktiken, Techniken und Prozeduren (TTPs),** die von Angreifern verwendet werden.

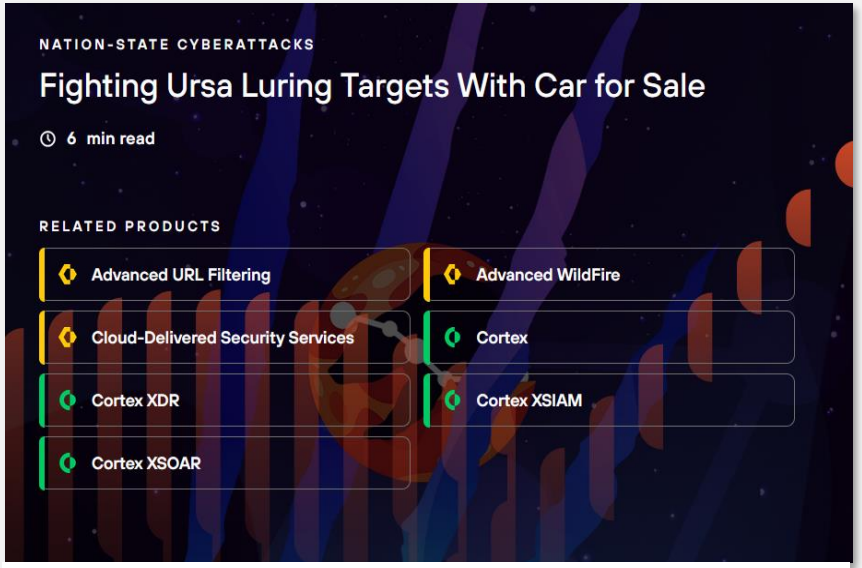
Beispiel

Titel: Analyse der APT28-Kampagne

Angreifer: APT28 (auch bekannt als Fancy Bear)

Ziel: Regierungs- und Verteidigungseinrichtungen

TTPs: Initial Access: Spear-Phishing-E-Mails, Privilege Escalation: Account Manipulation mit SMOKEDHAM Malware



Executive Summary

A Russian threat actor we track as **Fighting Ursa** advertised a car for sale as a lure to distribute **HeadLace** backdoor malware. The campaign likely targeted diplomats and began as early as March 2024. Fighting Ursa (aka APT28, Fancy Bear and Sofacy) has been **associated with Russian military intelligence and classified as an advanced persistent threat (APT) [PDF]**.

Diplomatic-car-for-sale phishing lure themes have been used by Russian threat actors for years. These lures tend to resonate with diplomats and get targets to click on the malicious content.

Unit 42 has previously observed other threat groups using this tactic. For example, in 2023, a different Russian threat group, **Cloaked Ursa**, repurposed an advertisement for a BMW for sale to target diplomatic missions within Ukraine. This campaign is not directly connected to the Fighting Ursa campaign described here. However, the similarity in tactics points to known behaviors of Fighting Ursa. The Fighting Ursa group is known for repurposing successful tactics – even **continuously exploiting known vulnerabilities for 20 months** after their cover was already blown.

The details of the March 2024 campaign, which we attribute to Fighting Ursa with a medium to high level of confidence, indicate the group targeted diplomats and relied on public and free services to host various stages of the attack. This article examines the infection chain from the attack.

Palo Alto Networks customers are better protected from the threats discussed in this article through our **Network Security** solutions, such as **Advanced WildFire** and **Advanced URL Filtering**, as well as our **Cortex** line of products.

If you think you might have been compromised or have an urgent matter, contact the **Unit 42 Incident Response team**.

Quelle: https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

Threat Reports

Use Case. Proaktives Threat Hunting. Regelmäßige Schulungen zur Phishing-Erkennung, Implementierung von Multi-Faktor-Authentifizierung und Berechtigungs-management von low-privilege Accounts.

Mögliche Quellen.

- SANS
- BSI
- Kommerzielle Anbieter (Palo Alto), zum Teil aber frei verügbar

Strategic Reports

Strategic Reports bieten einen Überblick über die **allgemeine Bedrohungslandschaft** und enthalten oft langfristige Analysen und Prognosen.

Beispiel

Deutlicher Anstieg von Ransomware-Angriffen auf kritische Infrastrukturen

Hauptakteure:
Staatlich unterstützte Gruppen: Aus China und Russland
Kriminelle Hackergruppen: Conti, LockBit, Revil

Schadensvolumen durch Ransomware-Angriffe:
Gesamtschaden: 15 Milliarden USD durch Ransomware im Jahr 2023
Energiesektor: 4 Milliarden USD
Technologiesektor: 1.5 Milliarden USD

The State of Ransomware in Critical Infrastructure 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity, including 275 from the energy, oil/gas and utilities sector, across 14 countries, conducted in January-February 2024.

A Sophos Whitepaper. July 2024

The State of Ransomware in Critical Infrastructure 2024

Introduction

Sophos' annual study of the real-world ransomware experiences of organizations around the globe explores the full victim journey, from root cause to severity of attack, financial impact, and recovery time. This report focuses on the ransomware experiences of the energy, oil/gas and utilities sector, a core element of the critical infrastructure supporting businesses around the globe.

The report combines fresh new insights, including an exploration of the role of law enforcement in ransomware remediation, with year-on-year trends leveraging learnings from our previous studies. It reveals the realities facing energy, oil/gas and utilities providers today and how the impact of ransomware has evolved over the last five years.

A note on reporting dates

To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2024. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2023.

About the survey

The report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. This included 275 respondents from the energy, oil/gas and utilities organizations. All respondents represent organizations with between 100 and 5,000 employees. The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants were asked to respond based on their experiences over the previous year.

5,000 respondents

275 from the energy, oil/gas and utilities industry

14 countries

100-5,000 employee organizations (50% 100-1,000, 50% 1,001-5,000)

15 industry segments

Quelle: https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-critical-infrastructure

Strategic Reports

Strategic Reports helfen Organisationen, **strategische Entscheidungen zu treffen und langfristige Sicherheits-strategien** zu entwickeln.

Mögliche Quellen.

- BSI
- SANS CTI Report
- ENISA Threat Landscape Report
- Kommerzielle Anbieter (z. B. FireEye)

The State of Ransomware in Critical Infrastructure 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity, including 275 from the energy, oil/gas and utilities sector, across 14 countries, conducted in January-February 2024.

A Sophos Whitepaper. July 2024

The State of Ransomware in Critical Infrastructure 2024

Introduction

Sophos' annual study of the real-world ransomware experiences of organizations around the globe explores the full victim journey, from root cause to severity of attack, financial impact, and recovery time. This report focuses on the ransomware experiences of the energy, oil/gas and utilities sector, a core element of the critical infrastructure supporting businesses around the globe.

The report combines fresh new insights, including an exploration of the role of law enforcement in ransomware remediation, with year-on-year trends leveraging learnings from our previous studies. It reveals the realities facing energy, oil/gas and utilities providers today and how the impact of ransomware has evolved over the last five years.

A note on reporting dates

To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2024. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2023.

About the survey

The report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. This included 275 respondents from the energy, oil/gas and utilities organizations. All respondents represent organizations with between 100 and 5,000 employees. The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants were asked to respond based on their experiences over the previous year.

5,000 respondents

275 from the energy, oil/gas and utilities industry

14 countries

100-5,000 employee organizations (50% 100-1,000, 50% 1,001-5,000)

15 industry segments

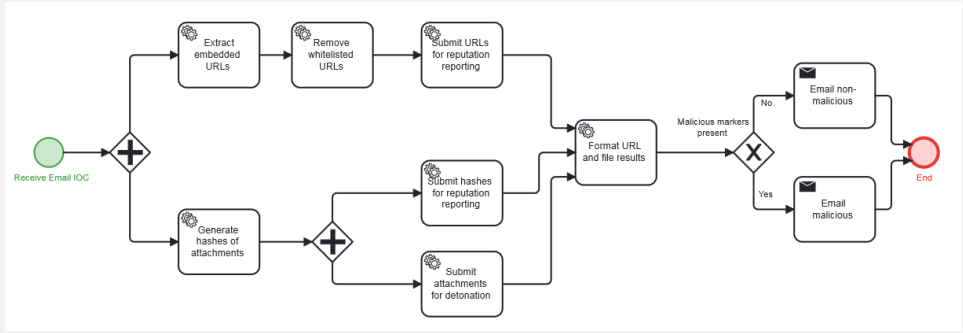
Quelle: https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-critical-infrastructure

Playbooks

Playbooks **strukturierte, schriftlich festgehaltene Anweisungen**, die detailliert beschreiben, wie auf spezifische Sicherheitsvorfälle in einer digitalen Infrastruktur reagiert werden soll.

Beispiel

1) Neue verdächtige IP-Adresse in Logs identifiziert – 203.0.113.50
2) IP-Reputationsanalyse durchführen (z.B. mit CTI-Datenbanken)
3) Bewertung der Gefahr
4) Blockieren der IP-Adresse
5) 203.0.113.50 ist bösartiger Malware Server, der an der Firewall blockiert wird
6) Isolation betroffener Systeme vom Netzwerk und starten einer Untersuchung



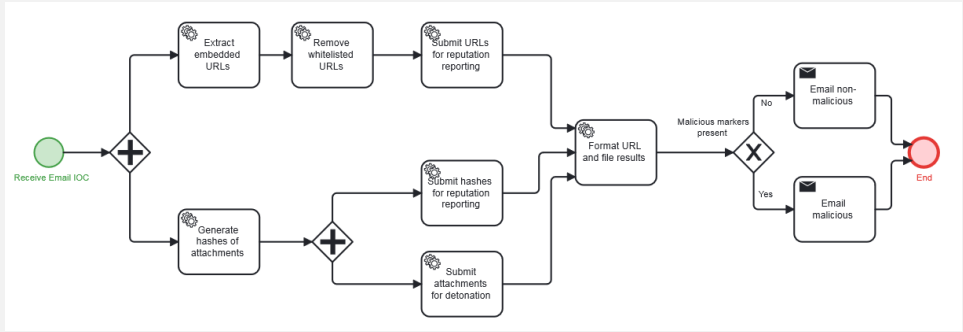
Quelle.: IACD, über Schlette et al. (2024) Do you play it by the books? A study on incident response playbooks and influencing factors.

Playbooks

Use Cases. Plyabooks bieten Schritt-für-Schritt-Anweisungen, um sicherzustellen, dass alle notwendigen Maßnahmen ergriffen werden. Zudem können sie helfen einige der Schritte zu automatisieren.

Mögliche Quellen.

- CISA
- Kommerzielle Anbieter wie Splunk, IACD etc.



Quelle.: IACD, über Schlette et al. (2024) Do you play it by the books? A study on incident response playbooks and influencing factors.

CTI im Security Lifecycle

Quellen für Cyber Threat Intelligence

Bei Quellen für CTI unterscheidet man grundsätzlich zwischen **kommerziellen Anbietern** und sog. **Sharing Communities**.

CyberSec Connect
Netzwerk für Security-Training & Wissenstransfer

Universität Regensburg

Im Rahmen eines dreijährigen Wissenstransfer-Projekts initiiert das Department für Wirtschaftsinformatik der Universität Regensburg ein Unternehmensnetzwerk zur Stärkung der Cybersicherheitskompetenzen. Das Projekt richtet sich an Unternehmen in Bayern, nicht ausschließlich aber insbesondere KMUs.

Teilnehmende Unternehmen profitieren von regelmäßigen Weiterbildungen und Workshops zu aktuellen Cybersecurity-Themen, darunter:

- **Cyber Range Training:** Hands-on-Workshop mit Fokus auf Incident Response, einschließlich Erkennung und Analyse von Ransomware sowie der Anwendung von Incident Response Playbooks in simulierten Live-Umgebungen.
- **Ethical Hacking:** Einführung in Penetration Testing und das Verständnis von Angreiferperspektiven.
- **Sichere Softwareentwicklung:** Best Practices und Techniken für Secure Programming.
- **Security Awareness in Zeiten von KI:** Bedrohungen und Schutzmaßnahmen im Zeitalter generativer KI.
- **Security-Regularien und Compliance:** Herausforderungen und Anforderungen, u. a. durch NIS2.
- **Threat Intelligence:** Erkennung und Analyse aktueller Bedrohungslagen.

Die Workshops und Vorträge werden **online oder im hybriden Format angeboten.** Ergänzend finden drei Netzwerktreffen an der Universität Regensburg statt. Die Terminplanung erfolgt in Abstimmung mit den Unternehmenspartnern. Dank einer Förderung ist die **Teilnahme für Unternehmen kostenfrei**. Zudem erhalten Teilnehmende **offizielle Teilnahmezertifikate** für jede Veranstaltung. Eine feste Verpflichtung zur Teilnahme an einer bestimmten Anzahl von Workshops besteht nicht – Unternehmen können flexibel die für sie relevanten Themen auswählen.

Anmeldung an **magdalena.glas@ur.de**

Teilnahme bei Online-Survey

- Link zur **Online Survey** im Chat
- Daten werden **anonymisiert** und ausschließlich **zu Forschungszwecken** verwendet
- **Link zu den Workshop-Folien** werden nach Abschluss der Survey bereitgestellt

Magdalena Glas
magdalena.glas@ur.de
magdalenaglas.eu

Johannes Grill
johannes.grill@ur.de

Tobias Reittinger
tobias.reittinger@ur.de