Berner
Fachhochschule

Analyse von Scans im Internet

Master Thesis MAS Cyber Security HS24

26. März 2025

Mauro Guadagnini

Berner Fachhochschule | Haute école spécialisée bernoise | Bern University of Applied Sciences

Scans im Internet

- Dauerhaft Scans im Internet [1, 2, 3]
- Ping-Anfragen und Port-Scans
- Bekannte Organisationen:
  Shodan [4], Censys [5] oder Shadowserver-Stiftung [6]
- Auch für Angriffe verwendet [7, 8, 9]
- Woher stammen die Scans? Welche Absichten haben sie?

Titel-/Sidebar-Grafik: *Fingerprint scanning on circuit board. secure system concept with a fingerprint. Cyber security technology concept abstract background futuristic Hi-tech style* (S and V Design 2024) [10]

Stand der Forschung

- Ursprungsländer der Scans [2, 11, 3, 12, 13]
- Anvisierte Serverdienste bzw. Port-Adressen [11, 14, 3, 15, 13]
- Anwendung von IPv6 [16, 17, 15, 18]
- Heo und Shin (2018): 5 % der Scan-Quellen weisen sich öffentlich aus [13]
  Prüfen der Quell-IP-Adresse mittels DNS und HTTP-GET-Anfrage

RFC 9511

- Titel „Attribution of Internet Probes“
- Nov. 2023
- Out-of-Band Probe Attribution
  `https://example.net/.well-known/probing.txt`
- In-Band Probe Attribution
  URI direkt in Anfrage bzw. Scan

RFC 9511

Beispiel einer `probing.txt`-Datei entsprechend RFC 9511 [9]

```
# Canonical URI (if any)
Canonical: https://example.net/measurement.txt

# Contact address
Contact: mailto:lab@example.net

# Validity
Expires: 2023-12-31T18:37:07z

# Languages
Preferred-Languages: en, es, fr

# Probes description
Description: This is a one-line string description of the probes.
```


JA4+

- Netzwerk-Fingerprinting-Methoden seit 2023 [19]
- TLS Client (JA4), TLS Server (JA4S), HTTP Client (JA4H), SSH (JA4SSH), TCP Client (JA4T), TCP Server (JA4TS) und mehr [19]

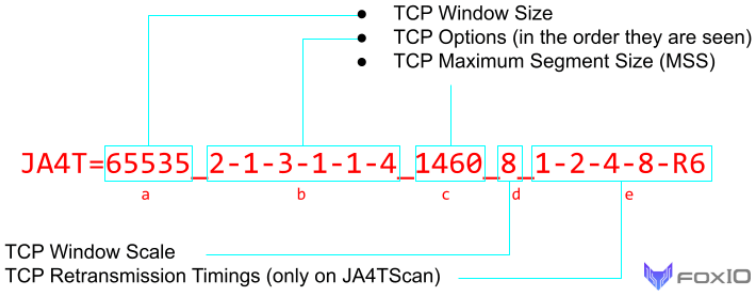

Abbildung: JA4T/S/Scan: TCP Fingerprint [20]

Analyse-Umgebung

- Malcolm [21]
  - Software-Sammlung zur Netzwerkverkehrsanalyse
  - Komponenten: Arkime [22], Zeek [23], OpenSearch Dashboards [24] und mehr
- Sensor [25]
  - Auswertung des Netzwerkverkehrs
  - Weiterleitung an Malcolm
  - VPN-Server
- Scan-Ziele

Analyse-Umgebung

- Scan-Ziele verbinden über VPN zu Sensor
  - `st001` CH
  - `st002` NG
  - `st003` DE
  - `st004` US
  - `st005` HK
  - `st006` AU
  - `st007` BR
  - `st008` RU
  - `st009` SG
  - `st010` GB
- Kapselung und Weiterleitung des Netzwerkverkehrs
- ERSPAN: **E**ncapsulated **R**emote **S**witch **P**ort **An**alyzer [26, 27]
- Nur auf Ping-Anfragen geantwortet, aber alle Pakete weitergeleitet

Analyse-Umgebung

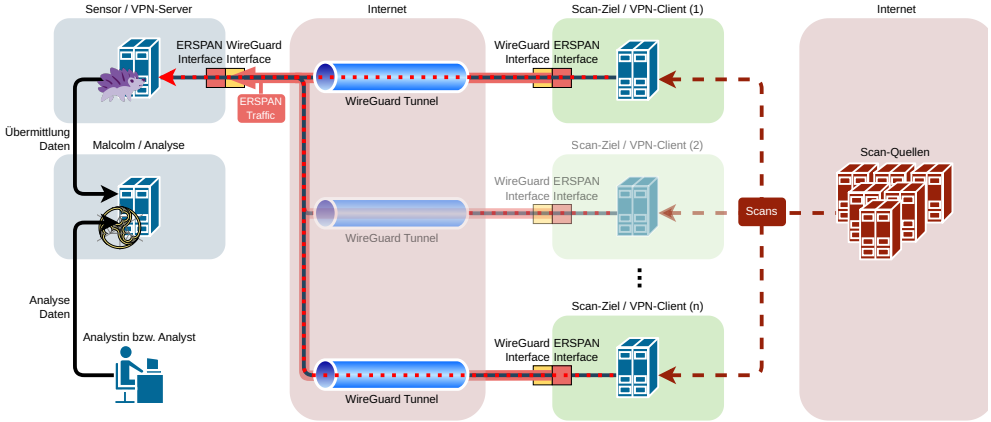

Abbildung: Aufbau Analyse-Umgebung inklusive Port-Mirroring mittels ERSPAN [25, 28]

Erweiterung mit Zeek-Skript

- Bekannte bzw. sich ausweisende Scan-Institutionen/-Anwendungen "good" 👍
- Quellen in Verbindung mit Malware oder Ähnlichem "bad" 👎
- Probe Attribution gemäss RFC 9511 [9]
- ZMap (Wert `54321` im IPv4-Identifikations-Feld [3, 11])
- Tabellen mit bekannten Scannern (IP-Adressen/-Subnetze, Domains, FQDNs)
- Quellen für Tabellen
  - 👍 Diverse Scan-Institutionen (Shodan, Censys, etc.) [4, 5]
  - 👍 Scanner-Listen von Collins [29] und ShadowWhisperer [30]
  - 👍 RIPE Atlas Probe Liste [31, 32]
  - 👎 Malware-Listen von ShadowWhisperer [30]
  - 👎 IoC-Listen von ThreatFox (abuse.ch) [33]
  - 👎 Tor Exit Node Liste [34]

Handzeichen-Symbole: *The fontawesome5 package* (Font Awesome und Krüger 2022) [35]

Ergebnisse allgemein

- Zeitraum: Januar 2025 + Tage in angrenzenden Monaten (Total 40 Tage)
- Keine Probe Attribution gemäss RFC 9511 detektiert
- ≈ 6,5 Millionen Verbindungen und 3,3 Millionen Scan-Detektionen
- ≈ 150'000 JA4T-Fingerprints von Scan-Anwendungen
- IPv6-Anteil: 0,007 % (494 Verbindungen, 279 Scan-Detektionen)
  - Trotz DNS-Einträge ab Mitte Januar
  - 6to4-Verbindungen entdeckt
  - Keine Detektionen mit "bad" 👎

Intention der Scan-Quellen

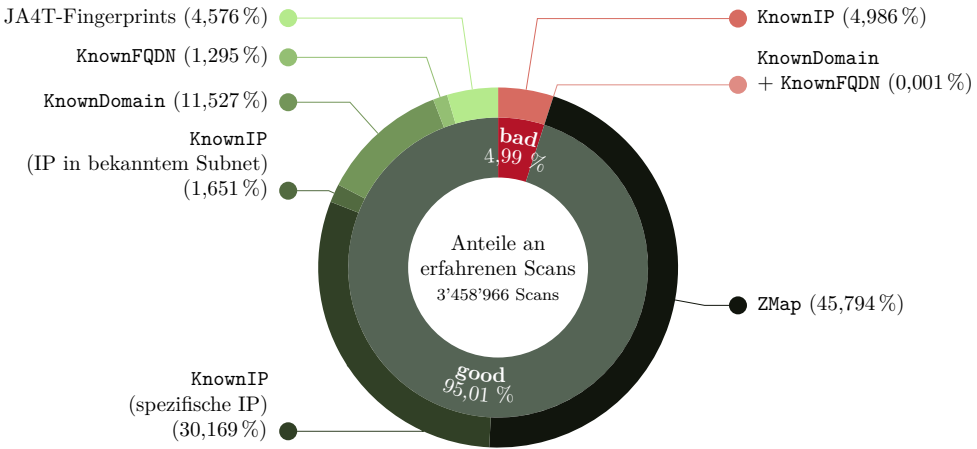

Abbildung: Anteile an detektierten Intentionen, aufgeteilt nach Detektion-Typ des Zeek-Skripts plus JA4T-Fingerprints

Intention der Scan-Quellen

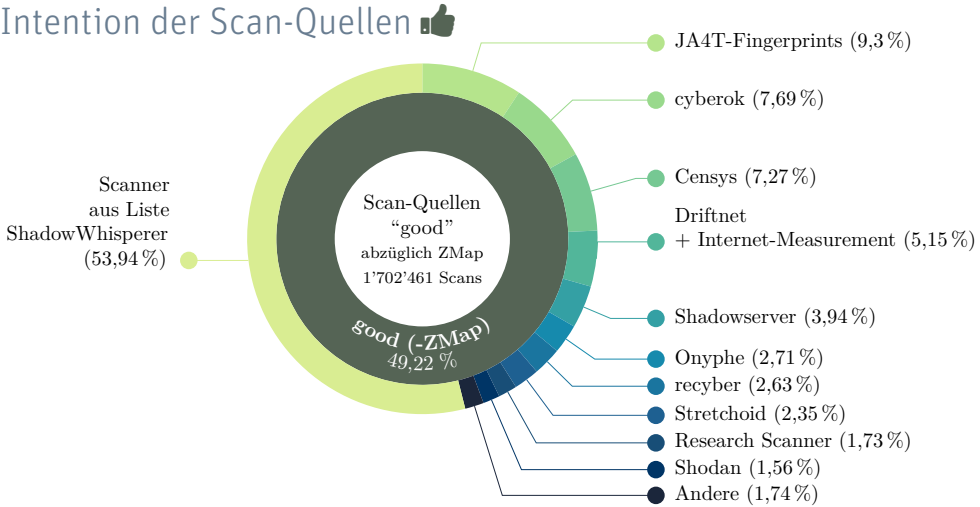

Abbildung: Anteile detektierter Scan-Quellen mit Intention „good“ (Abzüglich ZMap-Detektionen) [30, 5, 36, 37, 38, 39, 6, 40, 41, 42]

Intention der Scan-Quellen

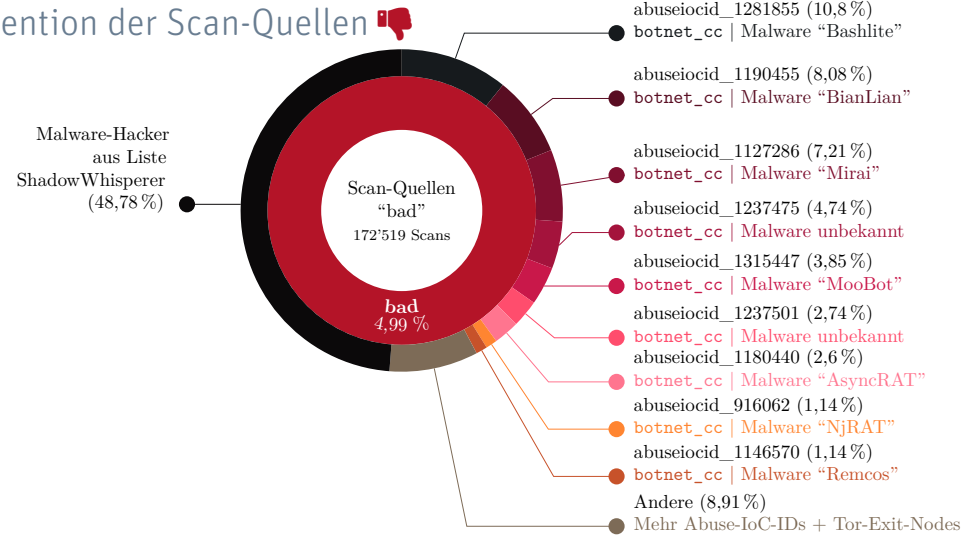

Abbildung: Anteile detektierter Scan-Quellen mit Intention „bad“ und allfälligen IoC-Informationen [30, 43, 44, 45, 46, 47, 48, 49, 50, 51]

Zusammenfassung

- Analyse-Umgebung mit Zeek-Skript
- Ungefähr 5 % Scan-Detektionen mit Intention „bad“
  Einzelne Scan-Ziele 2,5 bis 10,5 %
- Grossteil detektiert anhand bekannter Adressen (IP, DNS)
- Scan-Ziele antworten nur auf Ping-Anfragen (Firewall-Konfiguration)

Ausblick

- Dienste unter entsprechenden Ports aufschalten
- Zeek-Skript um JA4+-Detektionen erweitern (hier manuell ausgewertet)
- Auswertung Protokoll-spezifische Verhalten (z.B. DNS oder NTP)
- Logs der Analyse-Umgebung führen zur Aufdeckung neuer Scan-Quellen
  - Beispiel: Scan von `159.65.216.50` trifft ein
    → `49824f5c.tidalcoinage.internet-measurement.com` (Reverse DNS)
    → `https://49824f5c.tidalcoinage.internet-measurement.com/.well-known/probing.txt` "not found" in Log
    → `https://internet-measurement.com` weist Scans mit IP-Adressen aus
    → Neue manuelle Einträge in Tabellen für Zeek-Skript

Thesis und Code unter `https://guadm.github.io`

Literatur I

[1] Tariq Ahamad Ahanger. “Port Scan - A Security Concern”. In: *International Journal of Engineering and Innovative Technology (IJEIT)* 13.10 (2014), S. 241–246. ISSN: 2277-3754. URL: https://www.ijeit.com/archive/30/volume-3issue-10april-2014.html.

[2] Alexandru Vlad Serbanescu, Sebastian Obermeier und Der-Yeuan Yu. “ICS threat analysis using a large-scale honeynet”. In: *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*. ICS-CSR ’15. Ingolstadt, Germany: BCS Learning & Development Ltd., 2015, S. 20–30. ISBN: 9781780173177. DOI: 10.14236/ewic/ICS2015.3. URL: https://doi.org/10.14236/ewic/ICS2015.3.

[3] Zakir Durumeric, Michael Bailey und J. Alex Halderman. “An internet-wide view of internet-wide scanning”. In: *Proceedings of the 23rd USENIX Conference on Security Symposium*. SEC’14. San Diego, CA: USENIX Association, 2014, S. 65–78. ISBN: 9781931971157.

[4] Shodan. *Shodan Search Engine - Search Engine for the Internet of Things*. URL: https://www.shodan.io/ (besucht am 16. 10. 2024).

[5] Censys. *Censys Search*. URL: https://search.censys.io/ (besucht am 16. 10. 2024).

Literatur II

[6] The Shadowserver Foundation. *Shadowserver - Lighting the way to a more secure Internet*. URL: https://www.shadowserver.org/ (besucht am 16. 10. 2024).

[7] Xinyuan Wang. "On the feasibility of real-time cyber attack attribution on the Internet". In: *MILCOM 2016 - 2016 IEEE Military Communications Conference*. 2016, S. 289–294. DOI: 10.1109/MILCOM.2016.7795341.

[8] Roman Trapickin. "Who Is Scanning the Internet?" In: *Proceedings of the Seminars Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM), Summer Semester 2015*. Hrsg. von Georg Carle, Daniel Raumer und Lukas Schwaighofer. Bd. NET-2015-09-1. Network Architectures and Services (NET). Munich, Germany: Chair for Network Architectures und Services, Department of Computer Science, Technische Universität München, März 2015, S. 81–88. DOI: 10.2313/NET-2015-09-1_11. URL: http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-09-1/NET-2015-09-1_11.pdf.

[9] Éric Vyncke, Benoit Donnet und Justin Iurman. *Attribution of Internet Probes*. RFC 9511. Nov. 2023. DOI: 10.17487/RFC9511. URL: https://www.rfc-editor.org/info/rfc9511.

Literatur III

[10] S and V Design. *Fingerprint scanning on circuit board. secure system concept with a fingerprint. Cyber security technology concept abstract background futuristic Hi-tech style*. 24. März 2024. URL: https://www.shutterstock.com/image-vector/fingerprint-scanning-on-circuit-board-secure-2441137059 (besucht am 07. 08. 2024).

[11] Zakir Durumeric u. a. *Ten Years of ZMap*. 2024. arXiv: 2406.15585 [cs.CR]. URL: https://arxiv.org/abs/2406.15585.

[12] Gerry Wan u. a. "On the Origin of Scanning: The Impact of Location on Internet-Wide Scans". In: *Proceedings of the ACM Internet Measurement Conference*. IMC '20. Virtual Event, USA: Association for Computing Machinery, 2020, S. 662–679. ISBN: 9781450381383. DOI: 10.1145/3419394.3424214. URL: https://doi.org/10.1145/3419394.3424214.

[13] Hwanjo Heo und Seungwon Shin. "Who is knocking on the Telnet Port: A Large-Scale Empirical Study of Network Scanning". In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ASIACCS '18. Incheon, Republic of Korea: Association for Computing Machinery, 2018, S. 625–636. ISBN: 9781450355766. DOI: 10.1145/3196494.3196537. URL: https://doi.org/10.1145/3196494.3196537.

Literatur IV

[14] Philipp Richter und Arthur Berger. “Scanning the Scanners: Sensing the Internet from a Massively Distributed Network Telescope”. In: *Proceedings of the Internet Measurement Conference*. IMC ’19. Amsterdam, Netherlands: Association for Computing Machinery, 2019, S. 144–157. ISBN: 9781450369480. DOI: 10.1145/3355369.3355595. URL: https://doi.org/10.1145/3355369.3355595.

[15] Philipp Richter, Oliver Gasser und Arthur Berger. “Illuminating Large-Scale IPv6 Scanning in the Internet”. In: *ACM Internet Measurement Conference 2022*. Okt. 2022. DOI: 10.1145/3517745.3561452.

[16] Austin Murdock u. a. “Target generation for internet-wide IPv6 scanning”. In: *Proceedings of the 2017 Internet Measurement Conference*. IMC ’17. London, United Kingdom: Association for Computing Machinery, 2017, S. 242–253. ISBN: 9781450351188. DOI: 10.1145/3131365.3131405. URL: https://doi.org/10.1145/3131365.3131405.

[17] Oliver Gasser u. a. *Scanning the IPv6 Internet: Towards a Comprehensive Hitlist*. 2016. arXiv: 1607.05179 [cs.NI]. URL: https://arxiv.org/abs/1607.05179.

Literatur V

[18] Oliver Gasser. “Evaluating Network Security Using Internet-wide Measurements”. en. Diss. Technische Universität München, 2019, S. 212. URL: https://mediatum.ub.tum.de/1473343.

[19] John Althouse. *JA4+ Network Fingerprinting*. 14. Okt. 2024. URL: https://github.com/FoxIO-LLC/ja4/blob/main/README.md (besucht am 25. 10. 2024).

[20] John Althouse. *JA4T: TCP Fingerprinting*. 23. Apr. 2024. URL: https://blog.foxio.io/ja4t-tcp-fingerprinting (besucht am 31. 01. 2025).

[21] Seth Grover, Melanie Pierce u. a. *Malcolm*. 10. Sep. 2024. URL: https://github.com/cisagov/Malcolm/blob/main/README.md (besucht am 25. 10. 2024).

[22] Arkime. *Arkime FAQ*. URL: https://arkime.com/faq (besucht am 25. 10. 2024).

[23] The Zeek Project. *About Zeek*. URL: https://docs.zeek.org/en/master/about.html (besucht am 25. 10. 2024).

Literatur VI

[24] OpenSearch contributors. *OpenSearch Dashboards*. URL: https://opensearch.org/docs/latest/dashboards/ (besucht am 08. 01. 2025).

[25] Seth Grover u. a. *Malcolm Components*. 12. Sep. 2024. URL: https://github.com/cisagov/Malcolm/blob/main/docs/hedgehog.md (besucht am 02. 11. 2024).

[26] Marco Foschiano, Kalyan Ghosh und Munish Mehta. *Cisco Systems' Encapsulated Remote Switch Port Analyzer (ERSPAN)*. Internet-Draft draft-foschiano-erspan-03. Work in Progress. Internet Engineering Task Force, Feb. 2017. 16 S. URL: https://datatracker.ietf.org/doc/draft-foschiano-erspan/03/.

[27] ashirkar. *Understanding SPAN,RSPAN,and ERSPAN*. 3. Jan. 2019. URL: https://community.cisco.com/t5/networking-knowledge-base/understanding-span-rspan-and-erspan/ta-p/3144951 (besucht am 30. 10. 2024).

[28] Seth Grover. *Malcolm Components*. 11. Juni 2019. URL: https://github.com/cisagov/Malcolm/blob/main/docs/images/logo/Malcolm.svg (besucht am 02. 11. 2024).

Literatur VII

[29] Michael Collins. *Acknowledged Scanners*. 17. Dez. 2023. URL: https://gitlab.com/mcollins_at_isi/acknowledged_scanners (besucht am 18. 09. 2024).

[30] ShadowWhisperer. *Various lists to be used with an IP blocker*. URL: https://github.com/ShadowWhisperer/IPs (besucht am 30. 11. 2024).

[31] RIPE. *RIPE Atlas Docs. Query Parameters for Probes*. 31. Mai 2024. URL: https://atlas.ripe.net/docs/apis/rest-api-manual/probes/queryparameters.html (besucht am 30. 11. 2024).

[32] RIPE. *RIPE Atlas API Probe List*. URL: https://atlas.ripe.net/api/v2/probes/ (besucht am 30. 11. 2024).

[33] abuse.ch. *ThreatFox Export IOCs*. URL: https://threatfox.abuse.ch/export/ (besucht am 30. 11. 2024).

[34] The Tor Project. *Tor Bulk Exit List exporting tool*. URL: https://check.torproject.org/api/bulk (besucht am 06. 12. 2024).

Literatur VIII

[35] Font Awesome und Marcel Krüger. *The fontawesome5 package*. 2. Mai 2022. URL: http://mirrors.ibiblio.org/CTAN/fonts/fontawesome5/doc/fontawesome5.pdf (besucht am 30. 11. 2024).

[36] The Recyber Project. *The Recyber Project*. URL: https://www.recyber.net/ (besucht am 18. 12. 2024).

[37] CyberOK. *Abuse (responsible scanning) Policy*. 10. Nov. 2024. URL: https://www.cyberok.ru/docs/cyberok_scan_policy_en.pdf (besucht am 18. 12. 2024).

[38] Sharashka Inc. *Driftnet*. URL: https://driftnet.io/ (besucht am 19. 02. 2025).

[39] Sharashka Inc. *internet-measurement.com*. URL: https://www.internet-measurement.com/ (besucht am 18. 12. 2024).

[40] ONYPHE. *About Us*. URL: https://www.onyphe.io/about (besucht am 08. 01. 2025).

[41] Stretchoid. *Stretchoid Opt-Out*. URL: https://stretchoid.com/ (besucht am 30. 12. 2024).

Literatur IX

[42] research-scanner.com. *Research Scanner*. URL: http://research-scanner.com/ (besucht am 18. 12. 2024).

[43] Gi7wOrm. *ThreatFox database entry for ip:port 78.128.114.66:8888*. URL: https://threatfox.abuse.ch/ioc/1281855 (besucht am 14. 02. 2025).

[44] drb_ra. *ThreatFox database entry for ip:port 122.226.191.252:8443*. URL: https://threatfox.abuse.ch/ioc/1190455 (besucht am 14. 02. 2025).

[45] abuse.ch. *ThreatFox database entry for ip:port 194.180.48.84:59666*. URL: https://threatfox.abuse.ch/ioc/1127286 (besucht am 14. 02. 2025).

[46] abus3reports. *ThreatFox database entry for ip:port 204.76.203.70:1311*. URL: https://threatfox.abuse.ch/ioc/1237475 (besucht am 14. 02. 2025).

[47] DonPasci. *ThreatFox database entry for ip:port 154.213.187.164:25000*. URL: https://threatfox.abuse.ch/ioc/1315447 (besucht am 14. 02. 2025).

[48] abus3reports. *ThreatFox database entry for ip:port 204.76.203.71:1311*. URL: https://threatfox.abuse.ch/ioc/1237501 (besucht am 14. 02. 2025).

Literatur X

[49] abuse.ch. *ThreatFox database entry for ip:port 194.180.49.190:9254*. URL: https://threatfox.abuse.ch/ioc/1180440 (besucht am 14. 02. 2025).

[50] abuse.ch. *ThreatFox database entry for ip:port 194.180.48.115:4042*. URL: https://threatfox.abuse.ch/ioc/916062 (besucht am 14. 02. 2025).

[51] abuse.ch. *ThreatFox database entry for ip:port 194.180.48.113:1190*. URL: https://threatfox.abuse.ch/ioc/1146570 (besucht am 14. 02. 2025).