

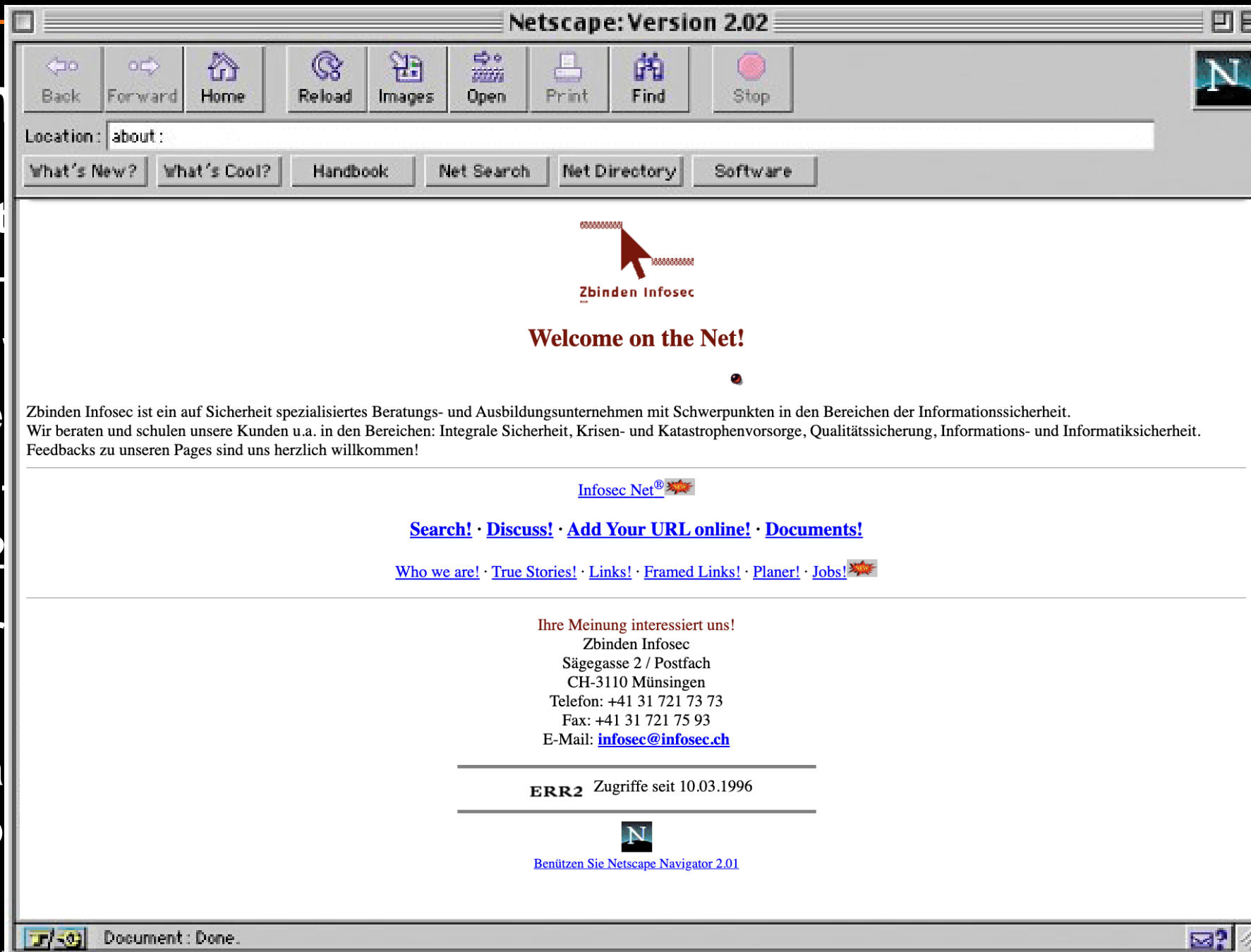


Anatomie des Cyberangriffs: Häufigste Beobachtungen und typische Vorgehensmuster

Felix Guggenheim, Sr. Solutions Engineer, CISSP
46. MEET SWISS INFOSEC! Swiss Infosec on Fire

1989 in

- Der Dat
- Presse-
- WANK
- DECNe
- Aids In
- (!) auf 2
- IBM Vir
- Antivire
- In Holla
- Ausgab



viren viel
sich via
via Post
ersten
(letzte





Kurzvorstellung Arctic Wolf

SOC-Partner für über 7000 Kunden in der Schweiz, Europa, Nordamerika und Australien:

- 24/7 Monitoring von Netzwerk, Endpunkten, Identitäts- und Cloudsystemen (“MDR”)
- Erarbeiten und Durchführen von Security-Strategien zur Härtung von Kundenumgebungen durch persönliche Betreuung (“Concierge Team”)
- Weitere SOC-Leistungen wie Threat Research, Schwachstellen-Management, User-Awareness-Trainings, Toolings für Assessments, Versicherbarkeitsabschätzung, Incident Response Planung, etc

Incident Response Team mit über 100 Spezialisten zur Unterstützung im Notfall:

- 24/7 Rufbereitschaft für Notfälle, auch mit 1h SLA
- Verhandlungsführerschaft, Digitale Forensik, Systemwiederherstellungen mit viel Erfahrung (1000+ Fälle / Jahr)



- 01** Review: Häufigste Angriffsarten
- 02** Review: Ursachen und Methoden
- 03** Case: Fluggesellschaft (Negativbeispiel)
- 04** Empfehlungen



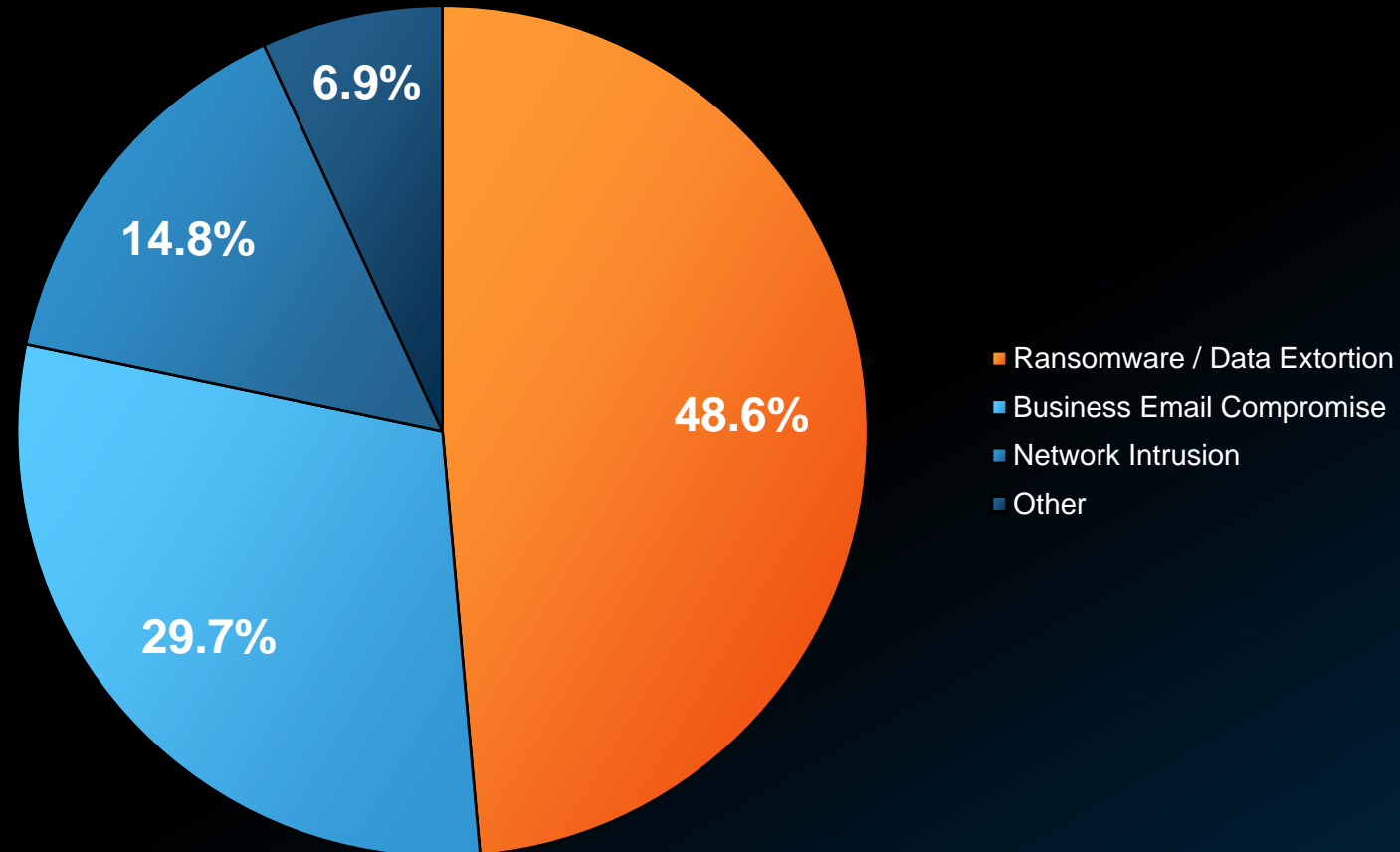
Threat Report 2024: Angriffsarten



Incident Response Investigations

Was haben wir bearbeitet?

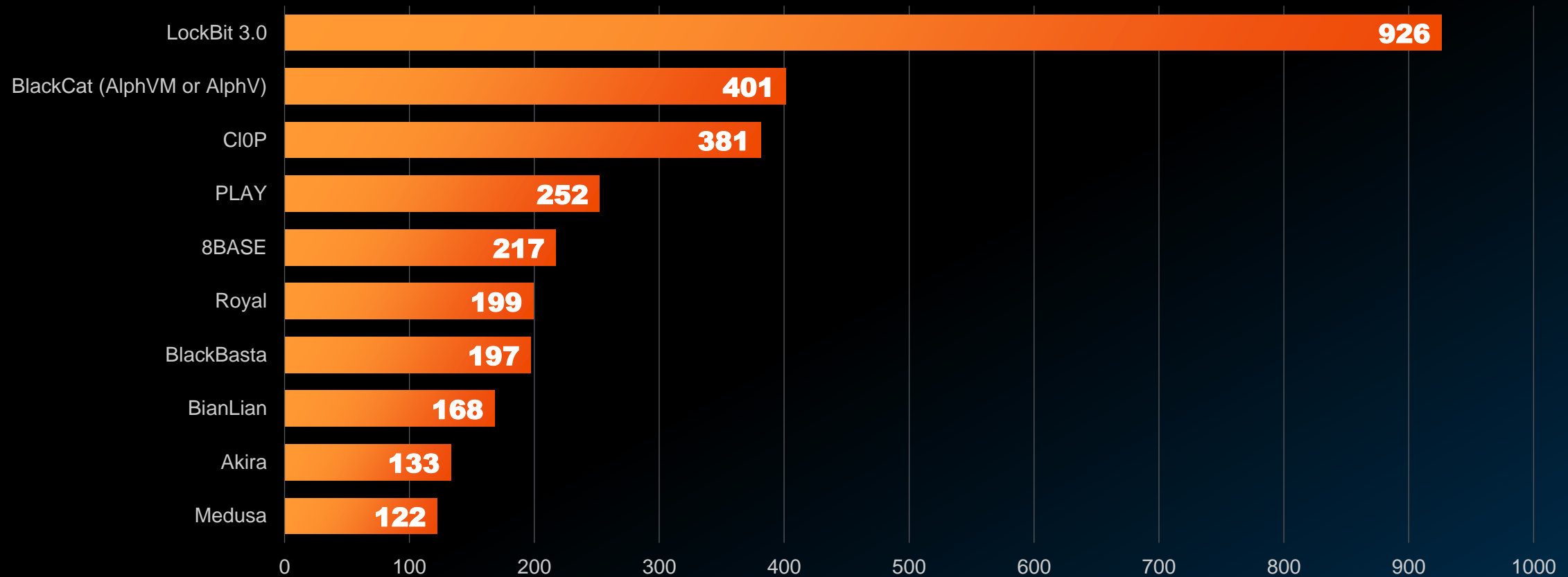
Incident Response Investigations nach Typ



Ransomware Groups





Wiederholungstätter, Newcomers, Leavers...

Top 10 Ransomware Gruppen nach Anzahl Opfer



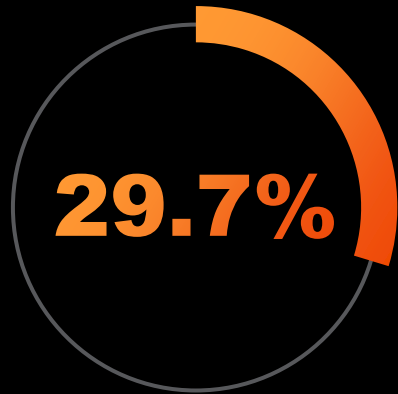
Lösungsgeldforderungen nach Branche

20 Prozent Steigerung (Median) gegenüber Vorjahr

| | 2022 | 2023 |
|--|-----------|--------------------|
|  Healthcare | \$275,000 | \$450,000 |
|  Construction | \$375,000 | \$500,000 |
|  All Industries | \$500,000 | \$600,000 |
|  Finance & Insurance | \$500,000 | \$900,000 |
|  Legal & Government | \$420,000 | \$1,000,000 |
|  Retail | \$627,500 | \$1,500,000 |



Business Email Compromise



Business Email Compromise ursächlich für über einen Viertel (29.7%) aller Incident Response Fälle im letzten Jahr.

Warum ist Business Email Compromise (BEC) attraktiv für Threat Actors?

- BEC ist einfach auszuführen
- BEC funktioniert

Meist-betroffene Branchen

- 01 Finance & Insurance
- 02 Construction
- 03 Education & Non-Profit
- 04 Manufacturing
- 05 Legal & Government
Healthcare
(Gleichermassen)



Threat Report 2024: Ursachen und Methoden



Root Cause

(Fälle ohne BEC)

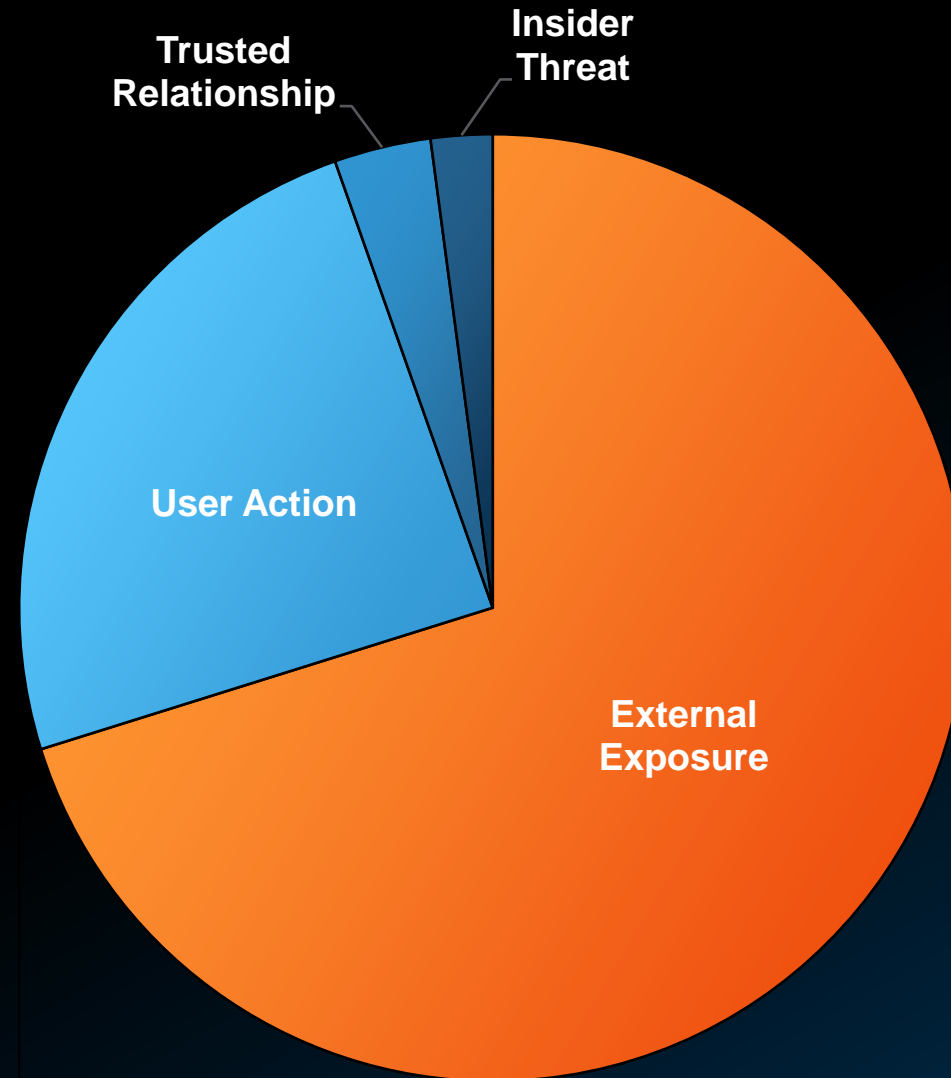
Die Ursache der Incidents fiel jeweils in eine dieser vier Kategorien:

70.1% External Exposure

24.4% User Action

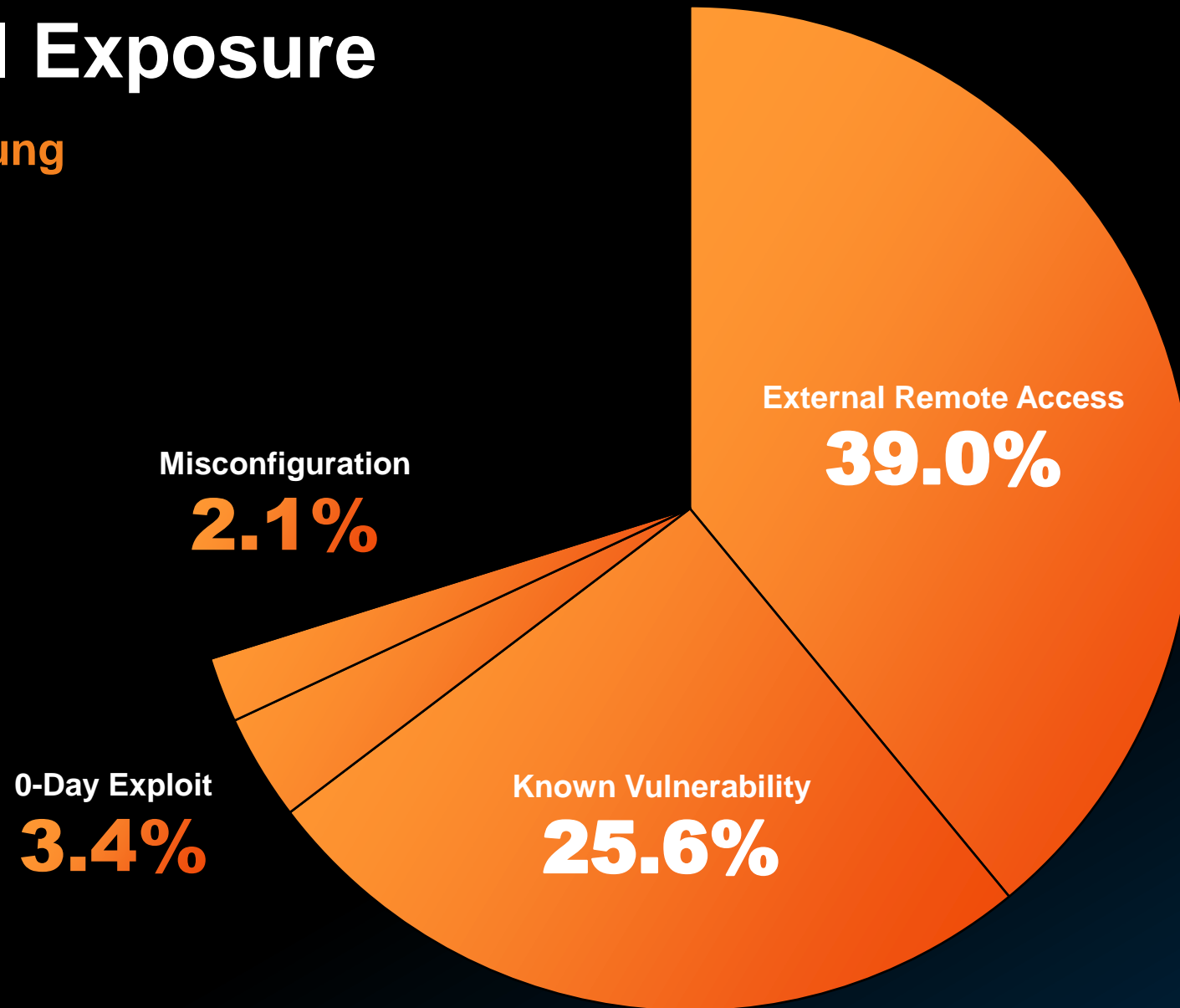
3.3% Trusted Relationship

2.1% Insider Threat



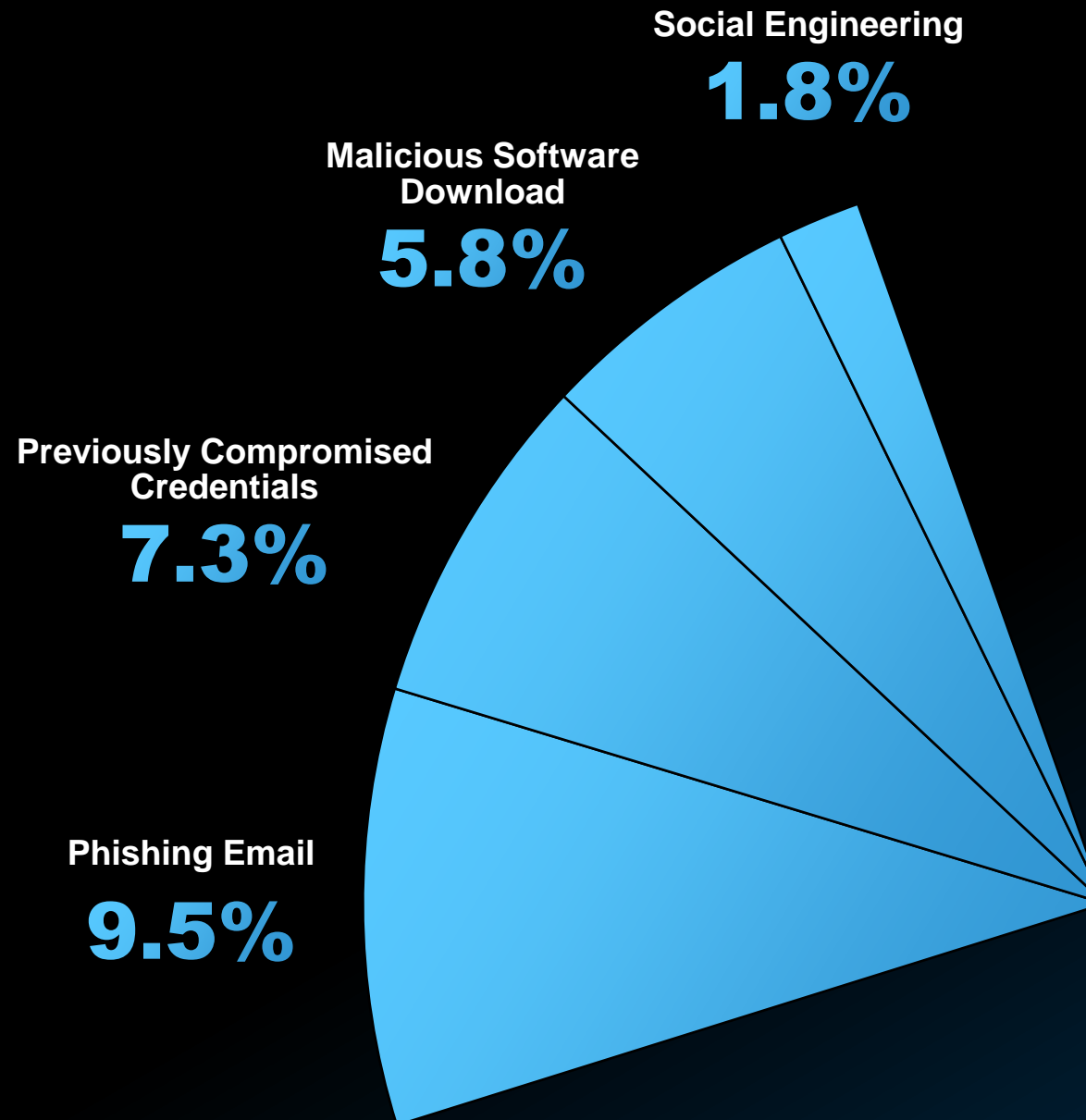
External Exposure

Aufschlüsselung



User Action

Aufschlüsselung



Top Vulnerabilities



53%

In über der Hälfte der Incidents (53%) war mindestens eine von **10 spezifischen Schwachstellen involviert**



25%

Drei dieser 10 Schwachstellen wurden in 25% der Intrusions genutzt:
CVE-2023-34362 – MOVEit Transfer
CVE-2022-47966 – ManageEngine
CVE-2022-41080 & 41082 – Microsoft Exchange

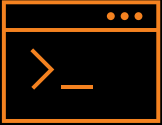


60%

60% der Incidents beinhalteten eine Schwachstelle mit **einer CVE-Zuweisung vor 2023**



TTPs to Watch



T1059.001 – Command and Scripting Interpreter: PowerShell



T1105 – Ingress Tool Transfer



T1047 – Windows Management Instrumentation



T1027.010 – Obfuscated Files or Information: Command Obfuscation



T1608.006 – Stage Capabilities: SEO Poisoning



Case: Negativbeispiel Ransomware / Fluggesellschaft



Shodan Maps Images Monitor Developer More...

SHODAN Maps veeam

Total Results: 1,081

Top Services

| | |
|----------------|-----|
| RDP | 333 |
| 135 | 232 |
| WinRM 2.0 | 120 |
| 9443 | 77 |
| MS-SQL Monitor | 42 |

Top Countries

| | |
|----|-----|
| US | 242 |
| DE | 114 |
| FR | 103 |
| RU | 40 |
| GB | 39 |

Top Organizations

| | |
|-----------------------|----|
| Microsoft Corporation | 84 |
| Cloud Propeller | 64 |
| Hetzner Online GmbH | 41 |
| OVH SAS | 31 |
| Google LLC | 16 |

Stephan Berger
Head of Investigations at InfoGuard AG
3w

During a recent Incident Response case, it was evident that the attacker disabled Defender on various hosts during a timeframe of a few hours.

Would you detect such behavior in your environment? Do you monitor for AV disabling and, on top of that, monitor for a threshold of systems left unprotected within a certain period?

Windows Defender creates the EventID 5001 = "Real-time protection is disabled."

<https://lnkd.in/e8SNdkMZ>

```
{
  "Provider": {
    "Name": "Microsoft-Windows-Windows Defender",
    "Guid": "11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78"
  },
  "EventID": {
    "Value": 5001
  },
  "Version": 0,
  "Level": 4,
  "Task": 0,
  "Opcode": 0,
  "Keywords": 9223372036854775808,
  "TimeCreated": {
    "SystemTime": 1717799555.6239376
  }
}
```

1,473 · 72 Comments

Like Comment Share

Jackson Draper
Detection and Response at Anduril
3w

Depending on the operating system, an attacker could just tamper with the EDR and overwrite it to stop functioning while the process still technically is running on the system. A holistic approach to this could be to monitor check-ins to your various tools. If the host is checking in to your other tools, but not your

THE LEADER IN SECURITY OPERATIONS

Leaflet | © MapTiler © OpenStreetMap contributors

Empfehlungen



Wichtigste Safeguards

Empfehlungen bezogen auf bearbeitete Fälle



Ein solides Verständnis für die eigene Angriffsfläche entwickeln



Zero-Trust für Identitäten und Netzwerk



Visibilität! Breite und Schnelligkeit vor Tiefe, in die Umgebung und in die einzelnen Assets



Cloud: Verantwortung wahrnehmen



Identity Controls: Ohne Ausnahmen



Etablieren einer Sicherheitskultur



Weitere Ressourcen



Threat Report

arcticwolf.com/2024threatreport



Predictions Report

arcticwolf.com/2024predictions



Trials für Cyberplanung

arcticwolf.com/solutions/cyber-jumpstart/

Response Team
Capture response team contact info so your internal stakeholders can respond efficiently to an incident.

- Executive Response Leader**
Ross Test
+1 (555) 555-5555
ross@arcticwolf.com
- Technical Leader**
Technical person facilitating infrastructure information, system capabilities and cybersecurity procedures.
- Financial Leader**
Stakeholder managing all financial factors of payroll, cash flow, business impact analysis and business interruption.
- Primary Legal Leader**
Team member reviewing cybersecurity agreements, coordinating with the data law firm and reviewing legal strategies.

Incident Response Plan
Retainer Active: Ends 2/2/24

- 1 45+ Minutes
- 2 Response Team Information
- 3 Cyber Insurance Documentation
- 4 Exposure & Detection Info

Cyber Resilience Assessment
CIS v8 | All Time | Download

624 Index

| Score Range | Category |
|-------------|---------------------|
| < 200 | Critically Exposed |
| 200-399 | Exposed |
| 400-599 | Viable Protection |
| 600-799 | Advanced Protection |
| 800 + | Protected In-depth |

Progress Tracker
Timeline Controls

| Control | Value |
|---------|-------|
| 1 | 25 |
| 2 | 40 |
| 3 | 50 |
| 4 | 100 |
| 5 | 75 |
| 6 | 100 |
| 7 | 75 |
| 8 | 25 |
| 9 | 75 |
| 10 | 60 |
| 11 | 75 |
| 12 | 25 |
| 13 | 50 |
| 14 | 60 |
| 15 | 10 |
| 16 | 10 |
| 17 | 75 |
| 18 | 10 |





Danke

www.linkedin.com/in/fguggenheim