VECTRA

# Attacker Behavior Industrie Report

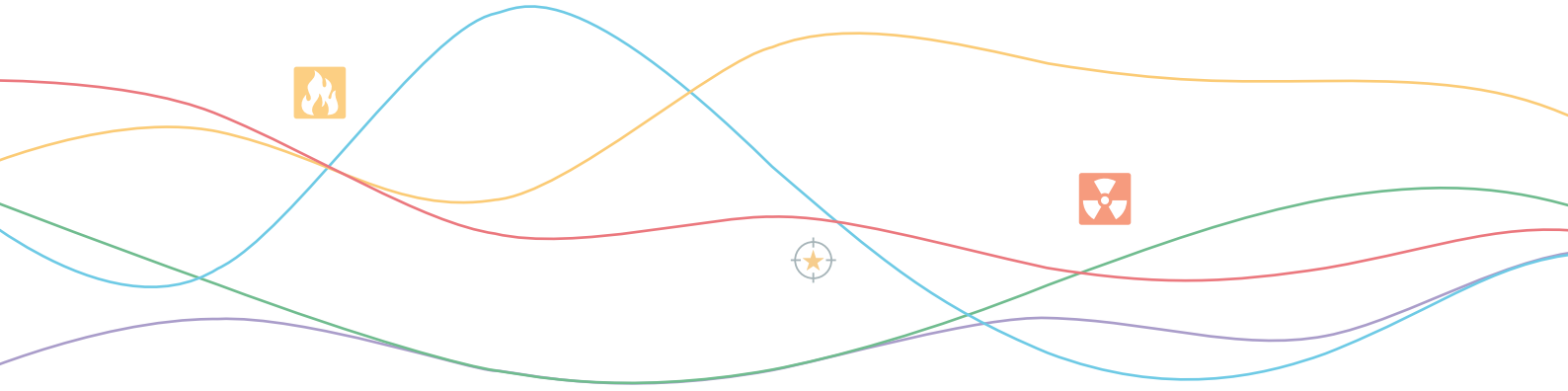
## 2018 (RSA Conference Edition)


*Ich bin eine künstliche Intelligenz.*
*Die treibende Kraft hinter der Jagd auf Cyber-Angreifer.*
*Ich bin Cognito.*

VECTRA

## INHALTSVERZEICHNIS





Der Vectra Attacker Behavior Industrie Report 2018 (RSA Edition) bietet Analysen aus erster Hand zu Verhaltensweisen, die auf laufende, beharrliche Aktivitäten von Angreifern in Cloud-, Rechenzentrums- und Unternehmensumgebungen von Vectra-Kunden hindeuten und in der Zeit von August 2017 bis Januar 2018 auftraten.

Dieser Report verfolgt einen multidisziplinären Ansatz, der alle strategischen Phasen einer Attacke erfasst. Mithilfe seiner KI-gestützten Cognito-Plattform, die das spezifische Vorgehen von Angreifern identifiziert, kann Vectra zeigen, wo Organisationen besonderen Gefahren ausgesetzt sind, wo für sie besondere Risiken liegen und welche aussagekräftigen Indikatoren auf schädliche Verletzungen der Informationssicherheit hinweisen.

### Die wichtigsten Resultate

- Über alle Branchen hinweg wurden im Durchschnitt 1.403 Fälle von Angriffsverhalten pro 10.000 Geräte aufgedeckt.
- Die höchste Zahl an Hinweisen auf konkrete Angriffsschritte gab es im Bereich Hochschulwesen (3.715 Meldungen pro 10.000 Geräte), gefolgt vom Maschinenbau (2.918 Meldungen pro 10.000 Geräte). Dieses Ergebnis geht primär auf Command-and-Control-Aktivitäten (C&C) im Hochschulwesen und Reconnaissance-Aktivitäten im Maschinenbau-Sektor zurück.
- Die C&C-Aktivitäten im Hochschulwesen liegen mit 2.205 erkannten Fällen pro 10.000 Geräte viermal höher als im Branchenmittel, das 460 Fälle pro 10.000 Geräte verzeichnet. Diese frühen Indikatoren für eine Attacke gehen gewöhnlich weiteren Schritten voraus und stehen im Hochschulwesen häufig mit opportunistischen Botnet-Aktivitäten in Verbindung.
- Regierungsinstitutionen und die Technologiebranche weisen mit 496 bzw. 349 Fällen pro 10.000 Geräte die geringsten Erkennungsraten auf. Dies könnte auf die Präsenz strenger Richtlinien, ausgereifte Response-Fähigkeiten und eine bessere Kontrolle der Angriffsflächen hindeuten.
- Botnet-Aktivitäten treten mit 151 Fällen pro 10.000 Geräte am häufigsten im Hochschulwesen auf, die Frequenz ist damit fünfmal so hoch wie im Durchschnitt aller Branchen mit 33 Fällen pro 10.000 Geräte. Diese opportunistischen Attacken nutzen gekaperte Geräte, um mit deren Hilfe Gewinne zu erzielen – etwa durch Bitcoin-Mining oder Spamversand.
- Vectra-Kunden erreichten eine 32-fache Reduzierung der Arbeitslast für Tier-1-Analysten im Bereich der Erkennung, Triage, Korrelation und Priorisierung von Security-Incidents. Sie konnten sich deshalb auf diejenigen kompromittierten Geräte konzentrieren, von denen das höchste Risiko ausgeht.
- Normalisiert man die erfassten Detektionen auf eine Rate pro 10.000 Geräte im Vergleich zum Vorjahr, zeigt sich in allen Branchen ein starker Anstieg bei C&C-Aktivitäten, Reconnaissance, Lateral Movement und bei der Exfiltration von Daten.

## Hintergrundinformationen und Methodik

Die Informationen in diesem Report stützen sich auf anonymisierte Metadaten von Vectra-Kunden, die einer Auswertung von Erkennungs-Kennzahlen zugestimmt haben. Vectra identifiziert Verhaltensweisen, die auf aktive Angriffe schließen lassen, durch ein direktes Monitoring des gesamten Netzwerk-Traffics und aller relevanten Log-Daten. Erfasst werden Traffic von und zum Internet, interner Traffic zwischen den Geräten im Netz, virtualisierte Workloads in eigenen Rechenzentren und Public-Cloud-Umgebungen.

Diese Form der Analyse erlaubt wichtige Einblicke in fortgeschrittene Stadien von Attacken. Vectras Cognito-Plattform erkennt Bedrohungen, die die Sicherheitsbarrieren am Netzwerk-Perimeter überwinden, und beobachtet das Voranschreiten einer Attacke nach der initialen Kompromittierung.

Der Attacker Behavior Industrie Report wertet die Daten zusätzlich nach Branchen aus und arbeitet relevante Unterschiede zwischen den Industriezweigen heraus.

Vectra hat von **August 2017 bis Januar 2018** insgesamt **4,6 Millionen Geräte und Workloads** überwacht. Dabei wurde Vectra auf über **12 Millionen verschiedene Vorgehensweisen von Angreifern** aufmerksam, die sich zu **652.000 „Detektionen“** (per Korrelation ermittelte Hinweise auf definierbare Bedrohungen) kondensieren ließen.

Bei der weiteren Sichtung wurden **373.000 Geräte und Workloads** selektiert. Über alle teilnehmenden Organisationen hinweg wurden innerhalb eines Monats **6.000** Geräte und Workloads als **kritisch** und über **9.000 als Hoch-Risiko-Fälle** eingestuft. Security-Analysten hatten so die Möglichkeit, schnell zu reagieren und die Bedrohungen zu entschärfen.

## Operationale Effizienz und Return-on-Investment

Cybersecurity stellt eine fortwährende Übung in operationaler Effizienz dar. Organisationen müssen eine nahezu unbegrenzte Zahl an Risiken, Bedrohungen und Angreifern mit limitierten Ressourcen bekämpfen. Sicherheitsprodukte sollten deshalb immer auch unter Effizienzgesichtspunkten ausgewählt werden und danach, welchen Einfluss sie auf die operationale Fitness einer Organisation haben.

Zeit ist der wichtigste Faktor, wenn es darum geht, Verletzungen der Netzwerksicherheit aufzudecken. Um mögliche Schäden in Grenzen zu halten, müssen Organisationen Attacken möglichst in Echtzeit erkennen, bevor Angreifer wichtige Assets stehlen oder beschädigen. Unglücklicherweise aber ist es ein langwieriger Prozess, zielgerichtete Attacken ausfindig zu machen und

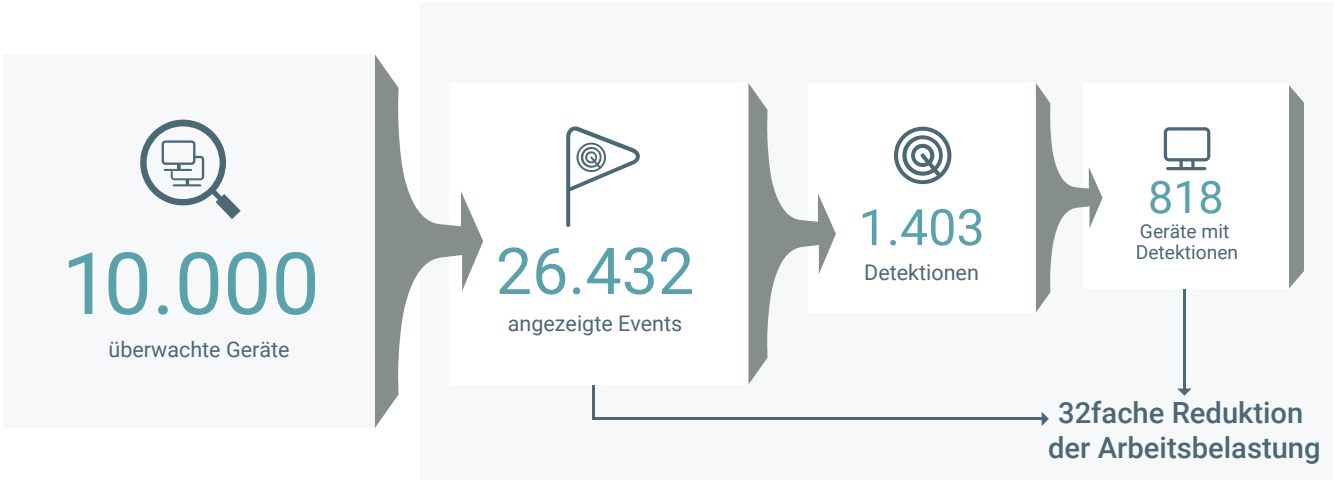
effektive Response-Maßnahmen einzuleiten. Er zwingt Security-Teams dazu, sich manuell durch Berge von Alerts zu kämpfen.

Mittels KI geht Cognito von Vectra ununterbrochen automatisiert auf die Jagd nach Bedrohungen, um in Echtzeit Angreiferverhalten aufzuspüren. Verhaltensweisen, die auf Attacken hindeuten, werden zu den kompromittierten Geräten in Beziehung gesetzt. Die Ergebnisse wiederum korreliert Vectra mit bekannten Angriffsvektoren und größeren Angriffskampagnen. Tausende von Bedrohungsindikatoren lassen sich so auf wenige hundert Varianten verdächtigen Angreifer-Verhaltens reduzieren, die an ein paar Dutzend Geräten zutage treten, die wiederum Teil groß angelegter Angriffskampagnen sein können.

Es ist wichtig zu verstehen, dass die Verhaltensweisen von Angreifern Anzeichen für Kompromittierungen darstellen (Indicators of Compromise). Es sind die Security-Analysten, die am Ende verifizieren müssen, ob eine Attacke real ist oder nicht. Cognito versorgt sie dazu mit den wichtigsten Informationen im Kontextzusammenhang. Dies hilft den Analysten bei der Entscheidung über die beste Response, bevor eine Attacke Schäden verursacht.

Die für die Studie ausgewerteten Netzwerke waren von sehr unterschiedlicher Größe. Die kleinsten wiesen ein paar hundert Geräte und Workloads auf, die größten mehr als 400.000. Um dieser Bandbreite Rechnung zu tragen, wurden die Daten auf eine Netzwerkgröße von 10.000 Geräten und Workloads hin normalisiert. So fällt es leichter, die Verbreitung von Bedrohungen in Netzwerken auf eine Pro-Kopf-Basis zu beziehen und zu vergleichen. Jedes beliebige Gerät mit einer IP-Adresse wird überwacht – über Server und virtualisierte Workloads hinaus auch IoT-Devices, Mobiltelefone, Tablets und Laptops.

### Reduktion der Arbeitsbelastung für Tier-1-Security-Analysten




**Insgesamt reduzierte Vectra die Arbeitslast der Security-Analysten für Nachforschungen um den Faktor 32, verglichen mit der manuellen Analyse aller Vorgehensweisen von Angreifern und aller kompromittierten Host-Geräte.**

## Scoring

Vectras Cognito überwacht einzelne Geräte und Workloads über ausgedehnte Zeiträume hinweg und gleicht erkannte Auffälligkeiten mit den Eigenschaften jedes Geräts oder Workloads ab, an dem sich verdächtiges Verhalten zeigt. Jeder Erkennung wird ein Score zugewiesen. Zusammen mit dem Zeitpunkt der Aufdeckung bildet dieser Wert den Haupt-Input für den Host-Geräte-Score.

Das Scoring von Cognito stützt sich auf zwei dynamische Metriken: den Threat Score und den Certainty Score. Die Metriken werden auf die jeweiligen Detektionen angewendet und auf jene Host-Geräte, auf die sich die Detektionen beziehen.

Der Threat-Score eines Erkennungsfalls drückt das Gefährdungspotenzial aus, das von einem Event ausgeht, wenn es echt ist (z.B. wenn tatsächlich Spam versandt oder Daten exfiltriert wurden). Als Wert für den maximalen Schaden, der durch eine Bedrohung entstehen könnte, beschreibt der Threat-Score immer das jeweilige Worst-Case-Szenario.

Der Certainty-Score zu einer Detektion gibt auf der Grundlage aller bereits verfügbaren Hinweise die Wahrscheinlichkeit an, mit der hinter einem gemeldeten Security-Event auch ein echter Vorfall steckt (z.B. die Wahrscheinlichkeit, mit der ein vermuteter Spamversand tatsächlich stattgefunden hat oder mit der Daten tatsächlich aus einem Unternehmen herausgeschmuggelt wurden).

Der Certainty-Score basiert darauf, wie weit ein Bedrohungsverhalten, das eine Meldung ausgelöst hat, vom normalen Verhalten abweicht. Deshalb ändert sich der Certainty-Score eines einzelnen Vorfalls im Verlauf der Zeit.

Weil Detektionen ein dynamisches Phänomen sind, haben Änderungen ihrer Scores auch Änderungen der Scores zur Folge, die Vectra den Host-Geräten zuweist. Kritische und hohe Scoring-Werte dienen den Security-Analysten als Anhaltspunkte dafür, ihre

Nachforschungen zu priorisieren, denn solche Scores repräsentieren Verhaltensweisen, die mit höchster Wahrscheinlichkeit

als echt zu betrachten sind und zugleich das höchste Potenzial haben, signifikanten Schaden anzurichten.

Andere Faktoren, die den Host-Geräte-Score beeinflussen, sind das wiederholte Auftreten einer bereits registrierten Detektion oder das Auftreten einer Kombination von Detektionen, die darauf hindeuten, dass eine Cyber-Attacke auf ein bestimmtes Ziel hin fortschreitet.

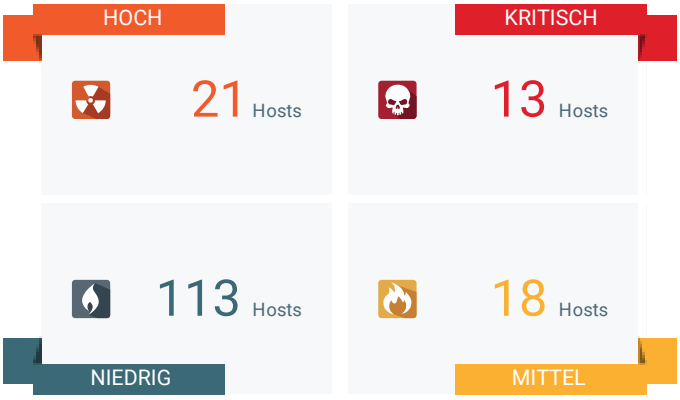
Für jeden Detektionstyp gilt eine maximale Lebensdauer von ein paar Tagen bis hin zu einem Monat. Wenn eine Detektion keine wiederkehrenden Aktivitäten erkennen lässt, sinkt ihre Wirkung auf den Host-Geräte-Score langsam gegen Null. Eine Detektion, die die ihr zugeordnete maximale Lebensdauer überschreitet, wird als inaktiv betrachtet und beeinflusst den Host-Geräte-Score überhaupt nicht mehr.

Bei jeweils 10.000 Geräten und Workloads, die einen Monat lang unter Überwachung standen, wurden im Durchschnitt 13 als kritisch eingeschätzt und 21 mit der Risiko-Stufe „hoch“ belegt. Solche Geräte und Workloads stellen die größte Bedrohung für eine Organisation dar und erfordern die unmittelbare Aufmerksamkeit eines Security-Analysten.

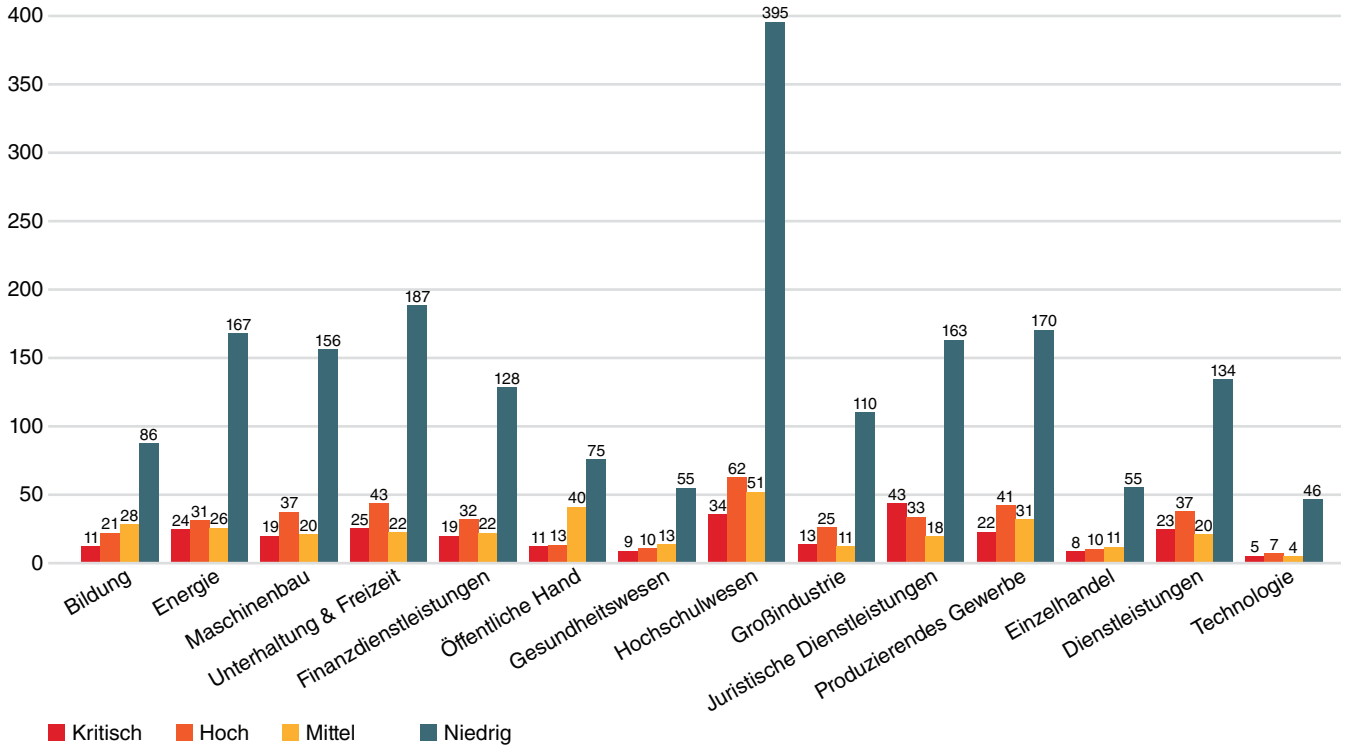
Vectra hat die Zahl der Host-Geräte und -Workloads, die anhand der jeweiligen Schweregrade priorisiert wurden, auf jede vertikale Branche hin ausgewertet und zum Gesamt-Durchschnittswert in Beziehung gesetzt, wie die Balkengrafik unten zeigt.

Die Zahl von Alarmen mit der Gewichtung „gering“ ist im Hochschulwesen beispielsweise mehr als dreimal so hoch wie der Normalwert – ein Indiz für vorwiegend opportunistisches Angriffsverhalten.

Die Technologiebranche wiederum zeigt eine geringe Zahl von Geräten, die mit den Stufen „hoch“ oder „kritisch“ priorisiert wurden. Die bedeutet, dass es die Cyber-Angreifer in diesem Bereich selten schaffen, ihre Attacken weit voranzutreiben.




## Ein Überblick über die Detektionen pro 10.000 Geräte und Workloads



## Allgemeine Trends bei den Detektionen

- Detektionsraten: Die Organisationen kamen auf eine mittlere Zahl von 818 Geräten, an denen Bedrohungen erkannt wurden, pro 10.000 Geräte während eines Monats. Hieraus ergibt sich eine 32-fache Reduktion der Zahl an Events, die nähere Untersuchungen und Selektion (Triage) erfordern.
- C&C repräsentierte den höchsten Prozentanteil an Detektionen: C&C-Traffic stellt eine zentrale Komponente von Botnet-Attacken dar und bildet den Ausgangspunkt für spätere Phasen eines gezielten Angriffs. Häufig ist C&C das erste Anzeichen dafür, dass gezielte und opportunistische Angriffsaktivitäten stattfinden.
- Cognito von Vectra liefert Security-Teams die Basis für einen erhöhten Wirkungsgrad: Während die Symptome gezielter Angriffe weiterhin verbreitet auftreten, gibt es ermutigende Anzeichen dafür, dass die Sicherheitsabteilungen Attacken schneller aufdecken und stoppen, und zwar bevor Schaden entsteht.
- Bitcoin stellt ein wachsendes Problem dar: Bitcoin-Mining wird zwar als opportunistische Aktivität verstanden, nimmt aber offenbar jedes Mal rapide zu, sobald der Bitcoin-Preis Spitzenwerte erreicht. Mit Bitcoin-Mining verbundenes Verhalten findet sich in erster Linie im Hochschulwesen, wo die Systeme der Studenten allzu leicht missbraucht werden können oder wo die Studenten selbst Mining-Software betreiben.

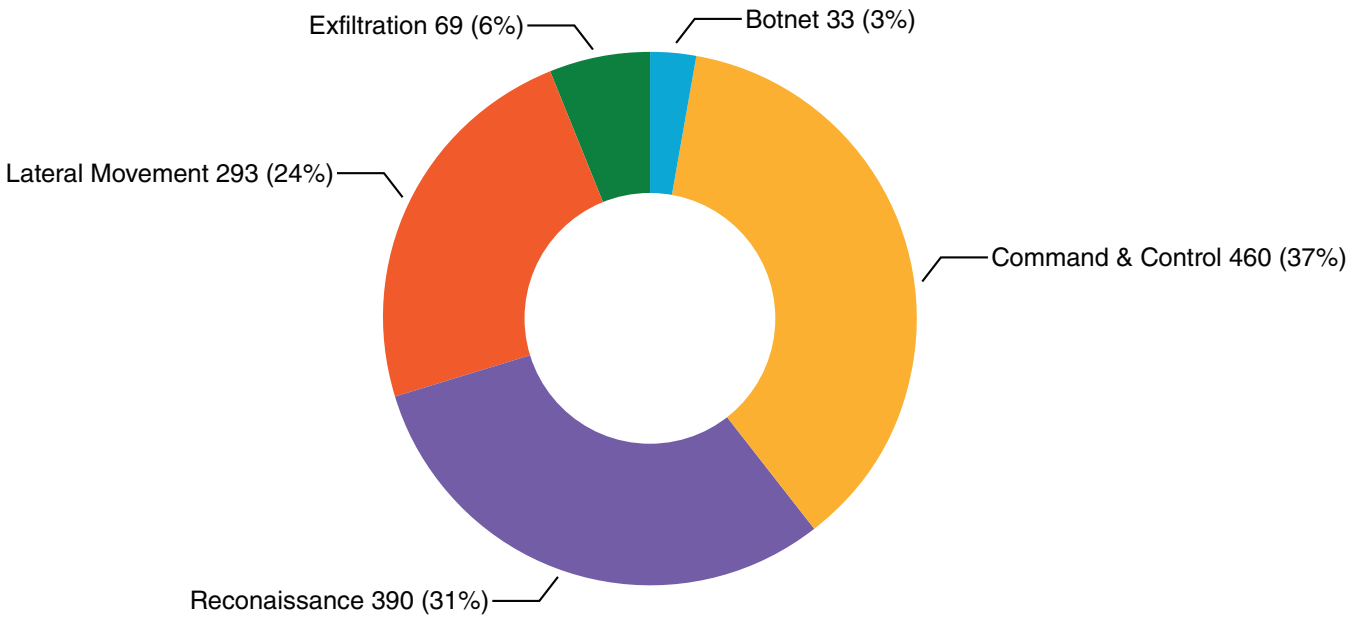
## Bedrohungen pro Typ und 10.000 Geräte

Für eine tiefergehende Analyse hat Vectra die Erkennungs-Statistiken auf einzelne Industriezweige heruntergebrochen. Die Tortengrafik unten zeigt Typen des Bedrohungsverhaltens über den Lebenszyklus einer Attacke hinweg. Diese Verhaltensweisen stellen starke Indikatoren dafür dar, in welchem Maße eine Organisation Gefahren ausgesetzt ist und welche Risiken daraus resultieren. Den Security-Analysten helfen diese Daten dabei, Zeit und Mühen bei ihrer Arbeit auf die wichtigsten Punkte zu konzentrieren.

Nicht jede Phase muss während einer Attacke notwendigerweise beschritten werden, aber die Stadien sind grundsätzlich untereinander verbunden und laufen häufig Phase für Phase auf maximalen finanziellen Gewinn für den Angreifer, auf Datendiebstahl oder Sabotage hinaus.

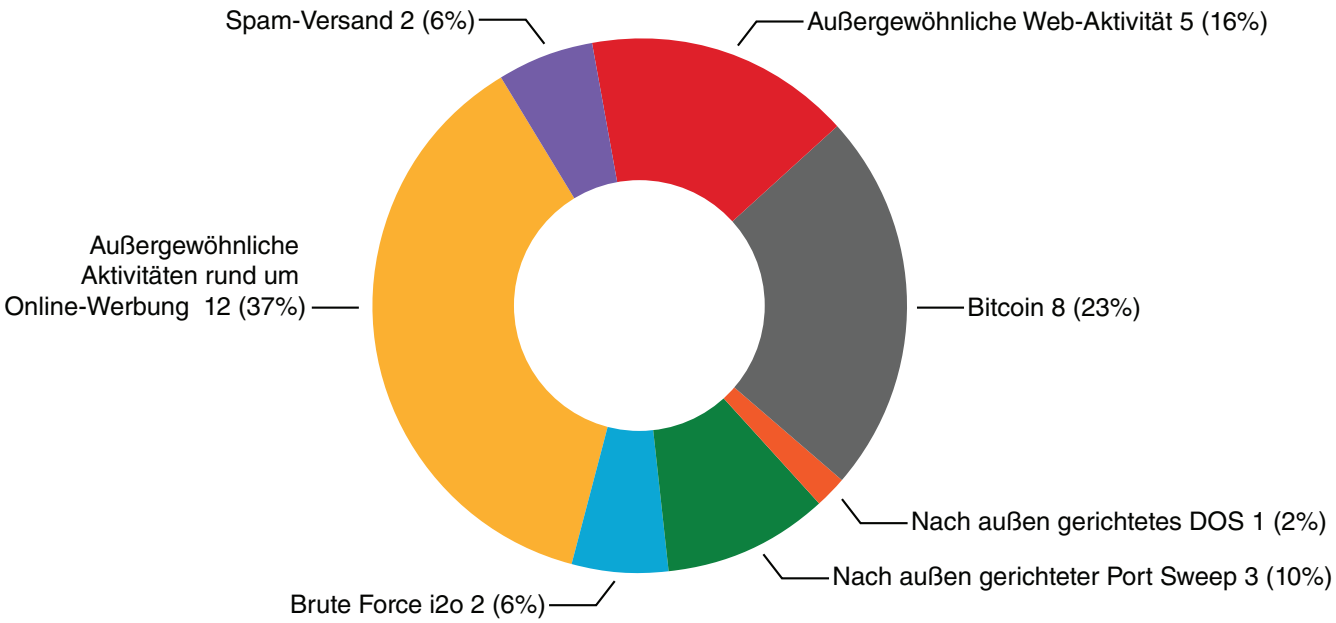
Die erfassten Daten repräsentieren Verhaltensweisen, wie sie sich im Verlauf eines Angriffs zeigen. Aktivitäten wie C&C und Reconnaissance treten in den frühen Stadien einer Attacke auf. Organisationen, die darauf aufmerksam werden, können die jeweilige Bedrohung eindämmen, bevor sie es schafft, sich auszubreiten. C&C und Reconnaissance sind die am häufigsten beobachteten Erscheinungsformen von Angreiferverhalten.

Aktivitäten wie Lateral Movement sind späteren Phasen im Lebenszyklus einer Cyber-Attacke zugeordnet. Sie festigen den Halt der Angreifer in der Infrastruktur einer Organisation – etwa, indem die Cyberkriminellen die Anmeldedaten von Administratoren stehlen, um Zugriff auf Server zu erlangen. Werden derartige Vorgehensweisen erkannt, rechtfertigt dies hoch priorisierte Aktionen der Incident-Response-Teams, um irreversiblen Schäden als Folge einer Daten-Exfiltration vorzubeugen.



## Botnets

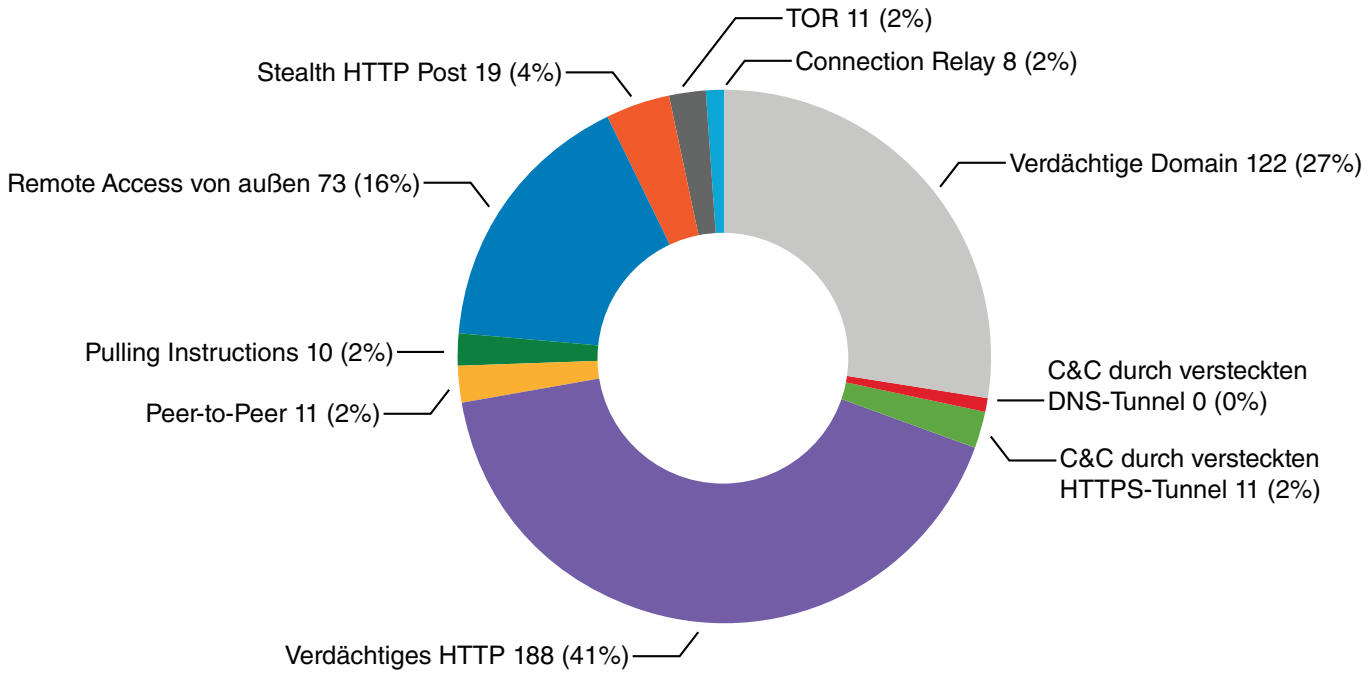
Botnets gehören zur Kategorie opportunistischer Angriffe – gekaperte Geräte werden dazu eingesetzt, für den Betreiber des Botnets Geld zu verdienen. Die Bandbreite unterschiedlicher Nutzungsweisen infizierter Systeme reicht dabei vom Bitcoin-Mining über den Spam-Versand bis zur Auslösung gefälschter Klicks auf Online-Anzeigen. Ihren Profit erzielen die Angreifer, indem sie die Geräte selbst, deren Netzwerkverbindungen und – dies vor allem – die gute Reputation der ihnen zugeordneten IP-Adressen ausnutzen.




## Command and control

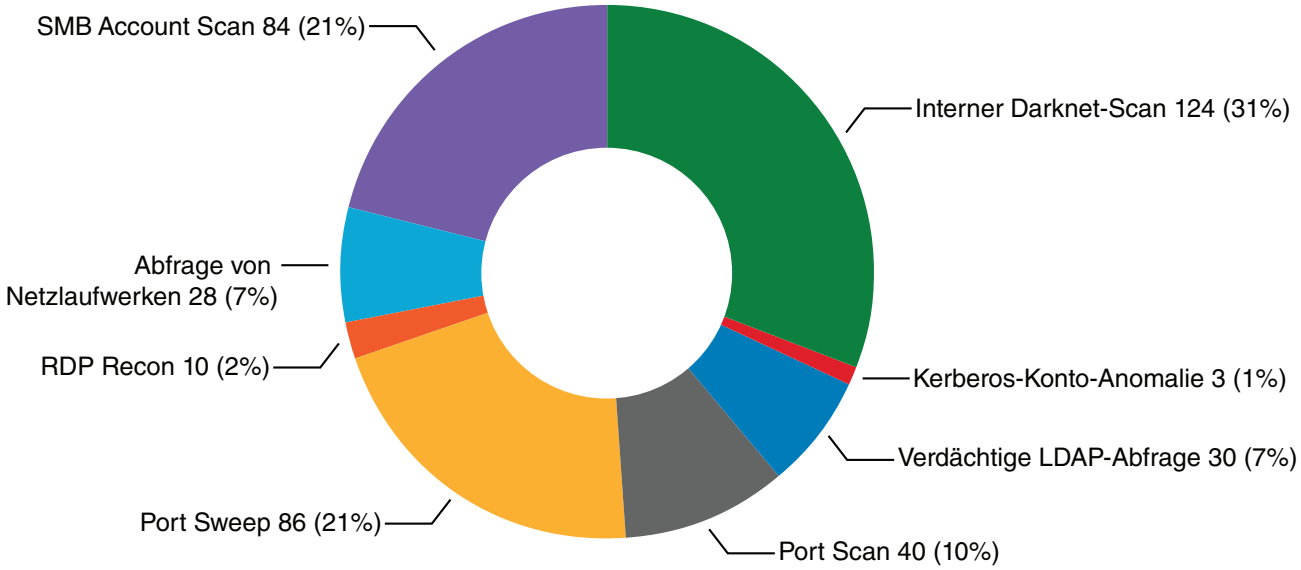
C&C-Traffic tritt auf, wenn ein Gerät offenbar unter der Kontrolle einer externen schädlichen Entität steht. In den meisten Fällen sind die Kontrollvorgänge automatisiert, weil das betroffene Gerät Teil eines Botnets ist oder weil darauf Adware oder Spyware installiert wurde.

Manchmal kontrollieren verbrecherische Angreifer Geräte auch manuell – dies sind seltene, aber höchst bedeutsame Fälle. Sie gehören zu den bedrohlichsten Erscheinungen und lassen oft auf einen gezielten Angriff schließen, der eine spezifische Organisation betrifft.



## Reconnaissance

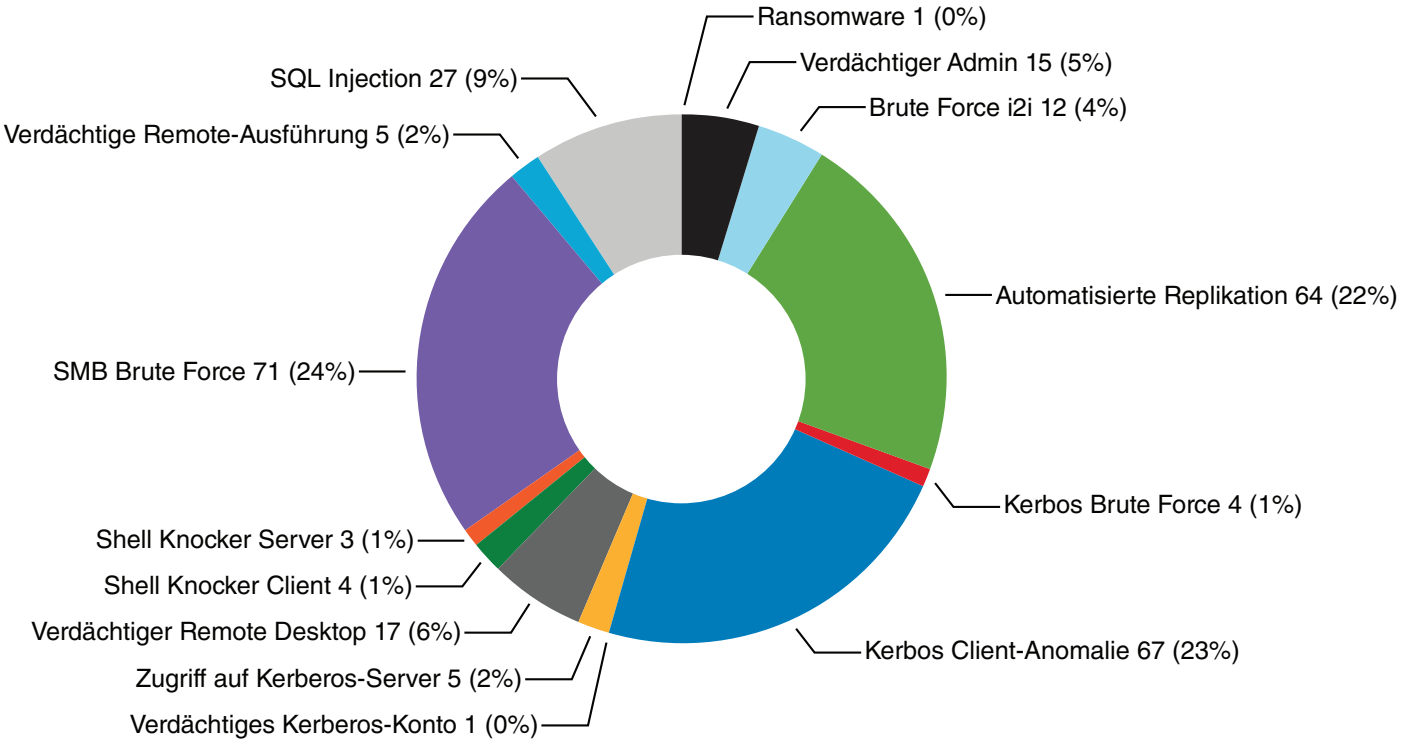
Reconnaissance ist ein Angreiferverhalten, das immer dann auftritt, wenn ein Gerät zur Erkundung einer Unternehmens-Infrastruktur genutzt wird. Diese Aktivität ist oft Teil eines gezielten Angriffs, kann aber auch auf Botnets hinweisen, die sich intern auf weitere Geräte auszudehnen versuchen. Zu den Erkennungsmerkmalen gehören Fast Scans und Slow Scans, die auf Systeme, Netzwerk-Ports und Anwenderkonten gerichtet sind.




## Lateral movement

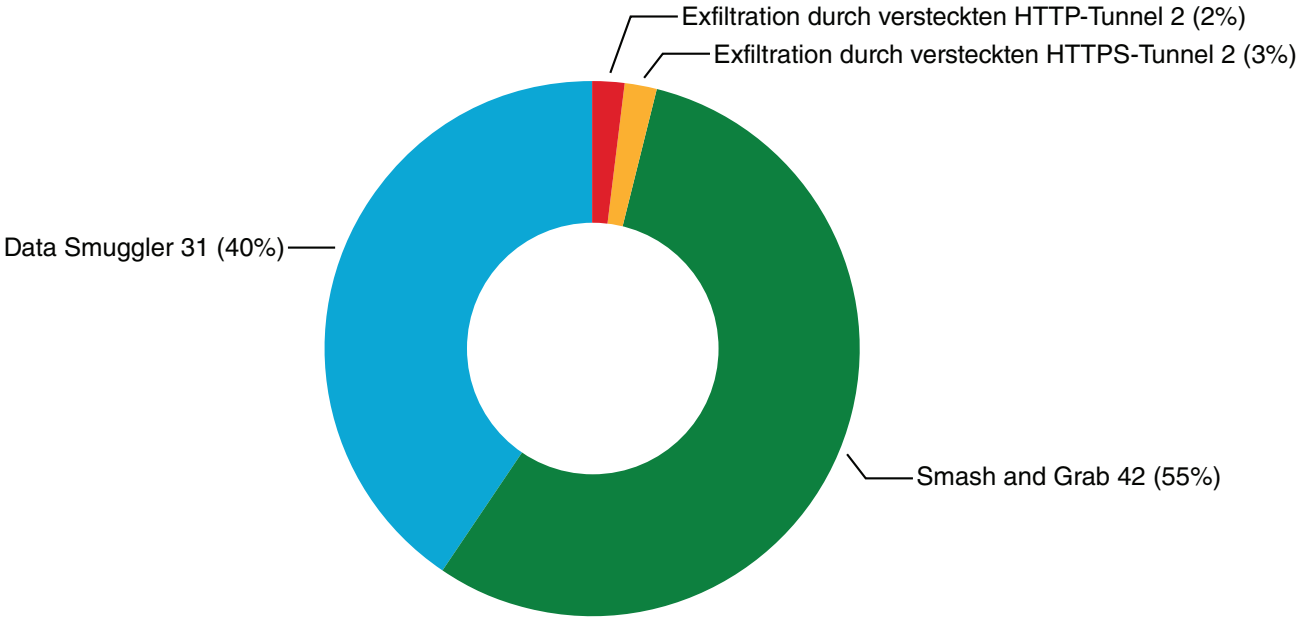
Lateral Movement steht für Szenarien, bei denen spezielle Ausbreitungsaktivitäten dazu dienen, eine gezielte Attacke weiter voranzutreiben. Dazu können Versuche gehören, Anmeldedaten von Konten an sich zu bringen oder Daten von einem anderen Gerät zu stehlen.

Lateral Movement kann auch mit der Kompromittierung eines weiteren Geräts einhergehen, um dem Angreifer dauerhaften Halt zu bieten oder ihn näher an die Zieldaten heranzurücken zu lassen. Diese Angriffsphase ist die Vorstufe zum Eindringen in private Rechenzentren oder Public Clouds.



## Exfiltration von Daten

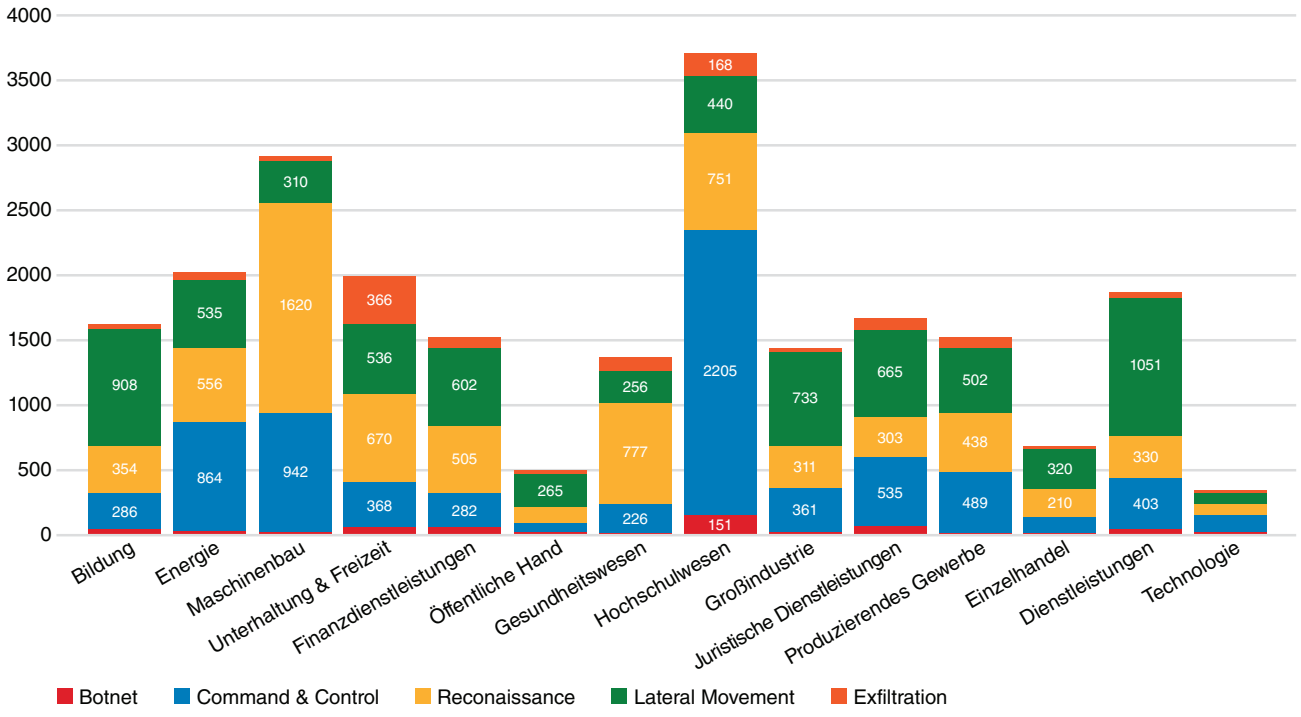
Verhaltensweisen, die der Exfiltration von Daten dienen, zeigen sich als Transfers nach außen, die im Verborgenen bleiben sollen. Legitime Datentransfers schließen gewöhnlich nicht den Gebrauch von Verschleierungstechniken ein. Indikatoren für eine Exfiltration sind das Gerät, das den Transfer ausführt, das Ziel des Transfers, das Datenvolumen und die Methode des Übertragungsvorgangs.




## Bedrohungen nach Branchen pro 10.000 Geräte

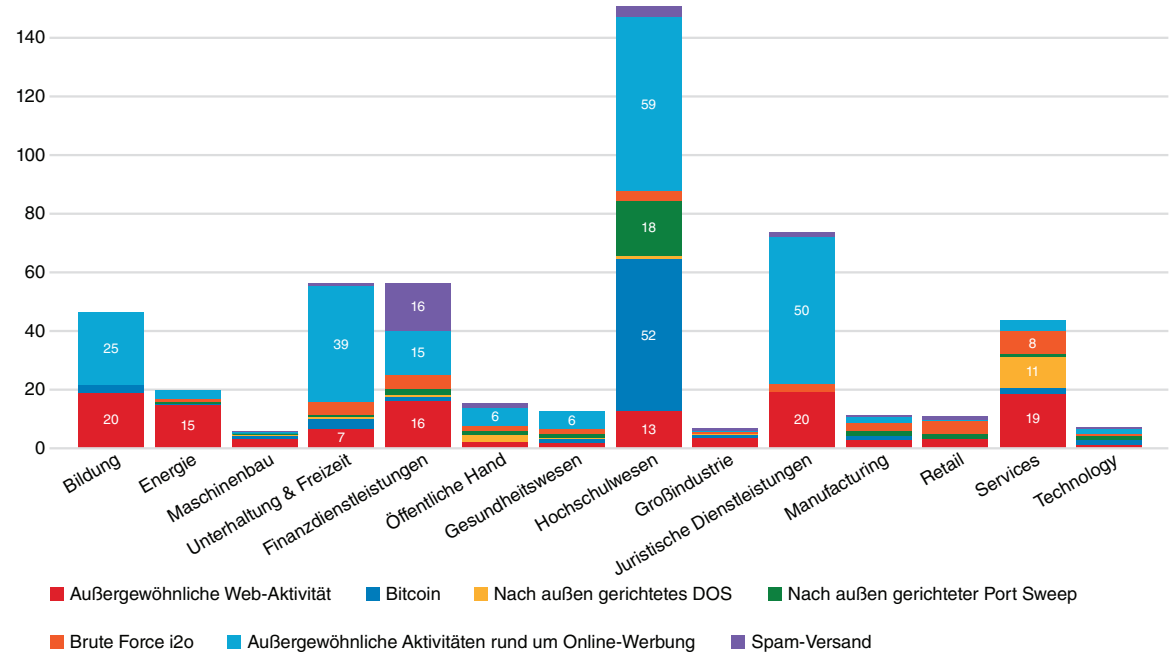
Die Balkengrafik unten gibt wieder, wie viele Bedrohungen pro Branche erkannt wurden. Die Darstellung zeigt, wie es jeder Branche auf einer Pro-Kopf-Basis erging und welche Branchen die meisten Detektionen verzeichneten.

Das Hochschulwesen und der Maschinenbau lassen die höchsten Prozentanteile an Detektionen über alle Branchen hinweg erkennen, hauptsächlich aufgrund hoher Werte bei C&C (Hochschulwesen) und Reconnaissance (Maschinenbau).



## Botnets nach Branchen

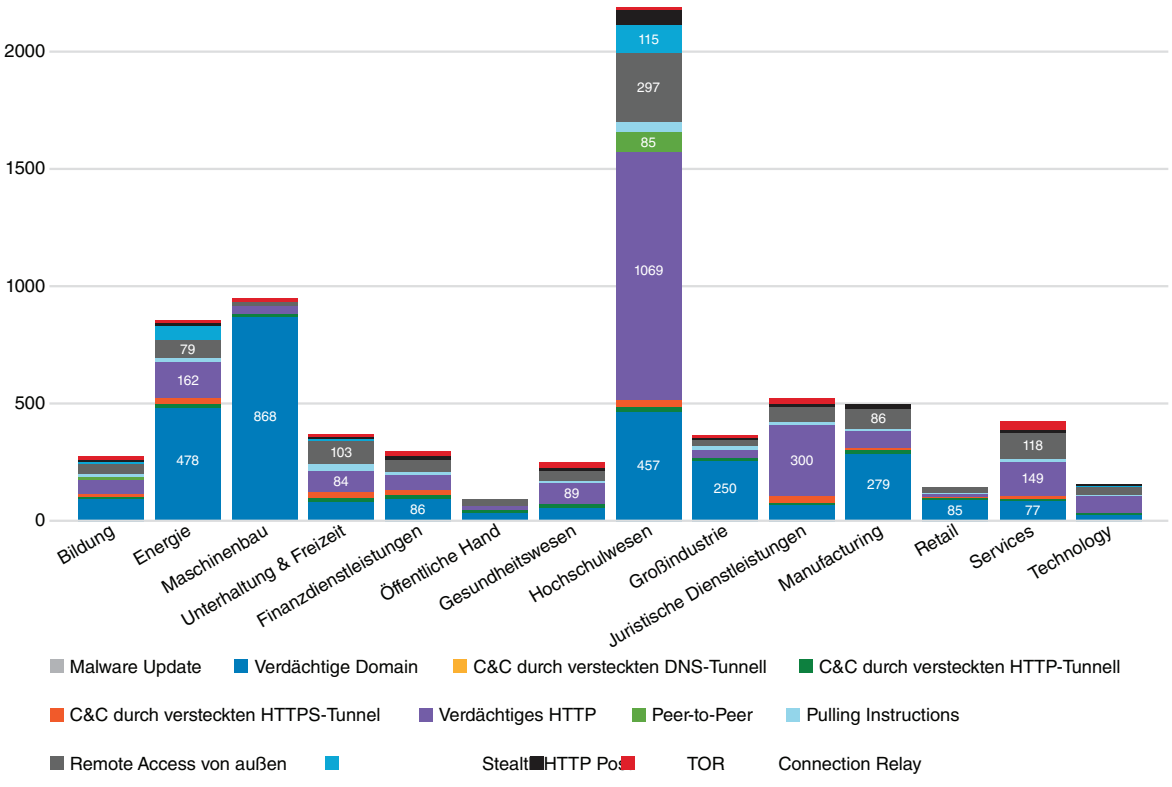
Cognito von Vectra beobachtete einen alarmierenden Trend hin zum Bitcoin-Mining und zu außergewöhnlichen Web-Aktivitäten im Bereich des Hochschulwesens. Bitcoin-Mining hat einen abrupten Popularitätsgewinn bei Cyberkriminellen erlebt, insbesondere innerhalb großer Studentengemeinschaften. Wahrscheinlich beruht dieses Phänomen auf mangelnden Sicherheitsmaßnahmen, die die Studenten zu lukrativen Zielen für Botnet-Betreiber machen.




## C&C nach Branchen

Bedingt durch die Verbindung zwischen Botnet- und C&C-Traffic fand Cognito von Vectra heraus, dass das Hochschulwesen das höchste Vorkommen an C&C-Vorgängen zeigte. Die Fälle hatten vornehmlich mit verdächtigem HTTP-Verkehr zu tun.

Studentischen Computersystemen fehlen häufig Sicherheitsvorkehrungen, die das C&C-Verhalten normalerweise erkennen und unterbinden würden. Deshalb sind C&C-Attacken in Hochschul-Umgebungen viel einfacher auszuführen.

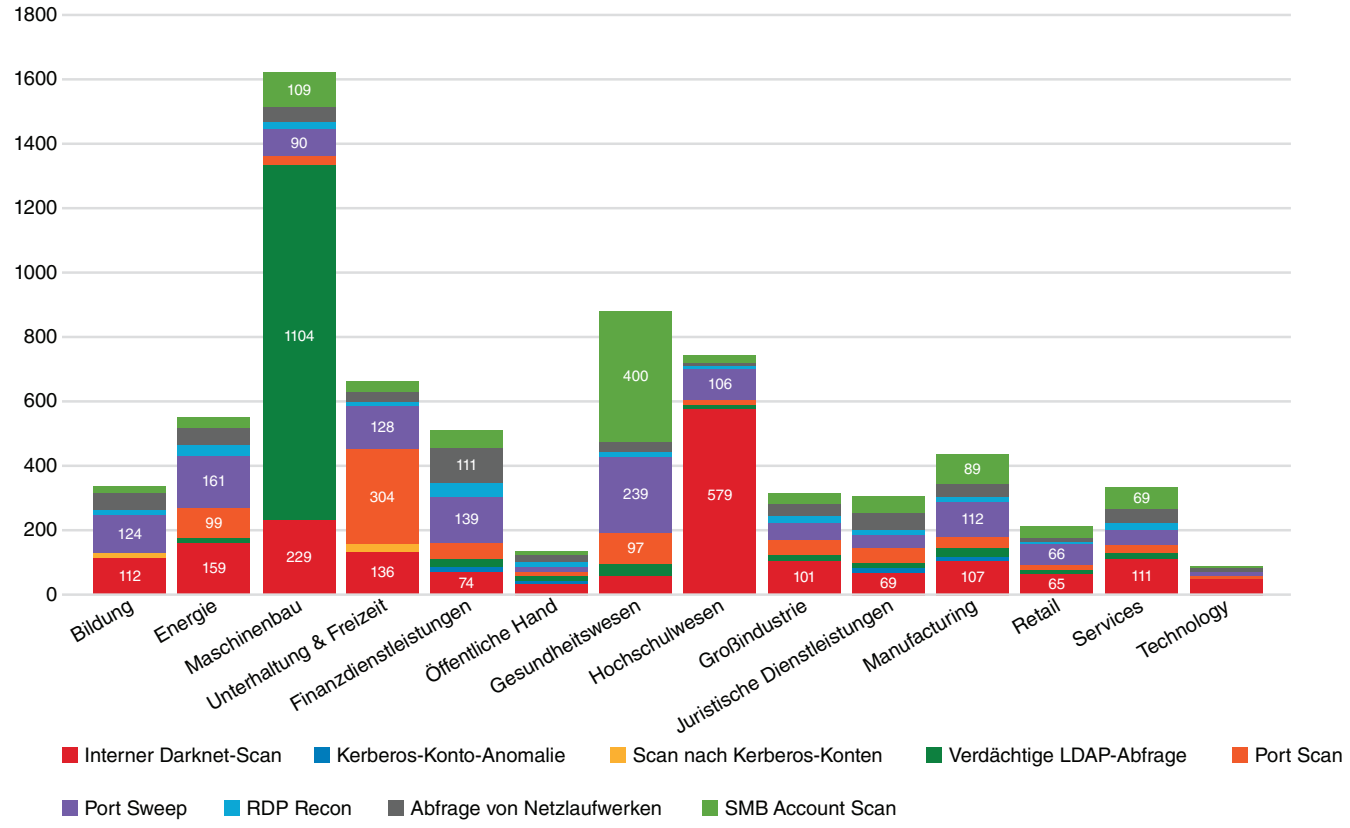


## Reconnaissance nach Branchen

Pauschal registrierte Cognito von Vectra eine hohe Anzahl an Darknet-Scans, worunter man Scans nach nicht existenten IP-Adressen im Netzwerk versteht. Dieses Vorgehen findet man bei Angreifern recht häufig, es ist die erste von ihnen verwendete Form der Reconnaissance. Das Verhalten tritt auf, wenn die Kommunikationswege für C&C eingerichtet sind und wenn der Angreifer dann nach tiefer im Netz verborgenen Zielen sucht.

Cognito stieß außerdem auf ein großes Volumen verdächtiger LDAP-Abfragen in der Maschinenbau-Branche. Ein Scan der Informationen in einem Active-Directory-Server stellt für die Angreifer eine effektive Methode dar, herauszufinden, welche Anwenderkonten im Netz einer Organisation privilegiert sind und wie die Namen der Server und Infrastruktur-Komponenten lauten.

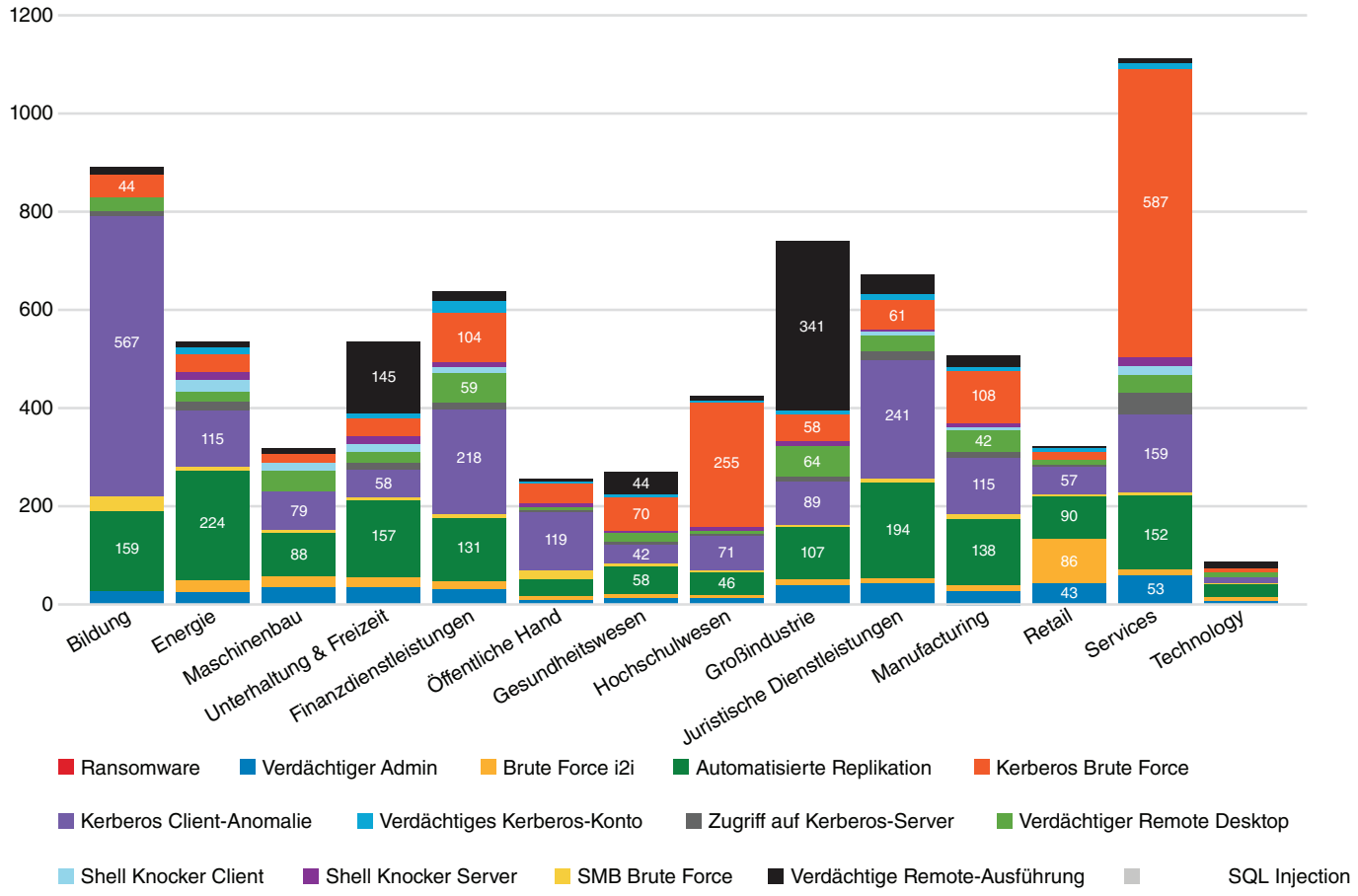
Angreifer präferieren diese Form der Reconnaissance, weil das Risiko einer Entdeckung relativ gering ist und das Verfahren weniger auffällt als ein Port-Sweep oder Port-Scan.



## Lateral Movement nach Branchen

Im Bildungswesen beobachtete Cognito einen hohen Spitzenwert an Verhaltensanomalien im Zusammenhang mit Kerberos-Clients. Sie zeigen an, dass ein Kerberos-Konto auf eine oder verschiedene Weisen anders genutzt wird als im vorher registrierten Normalbetrieb – etwa für Verbindungen zu sonst nicht kontaktierten Domain-Controllern oder für die Nutzung ungewöhnlicher Geräte oder Dienste. Außerdem fielen ungewöhnliche Mengen von Kerberos-Requests auf, für die ganz normale Domain-Controller, Geräte oder Dienste eingesetzt wurden.

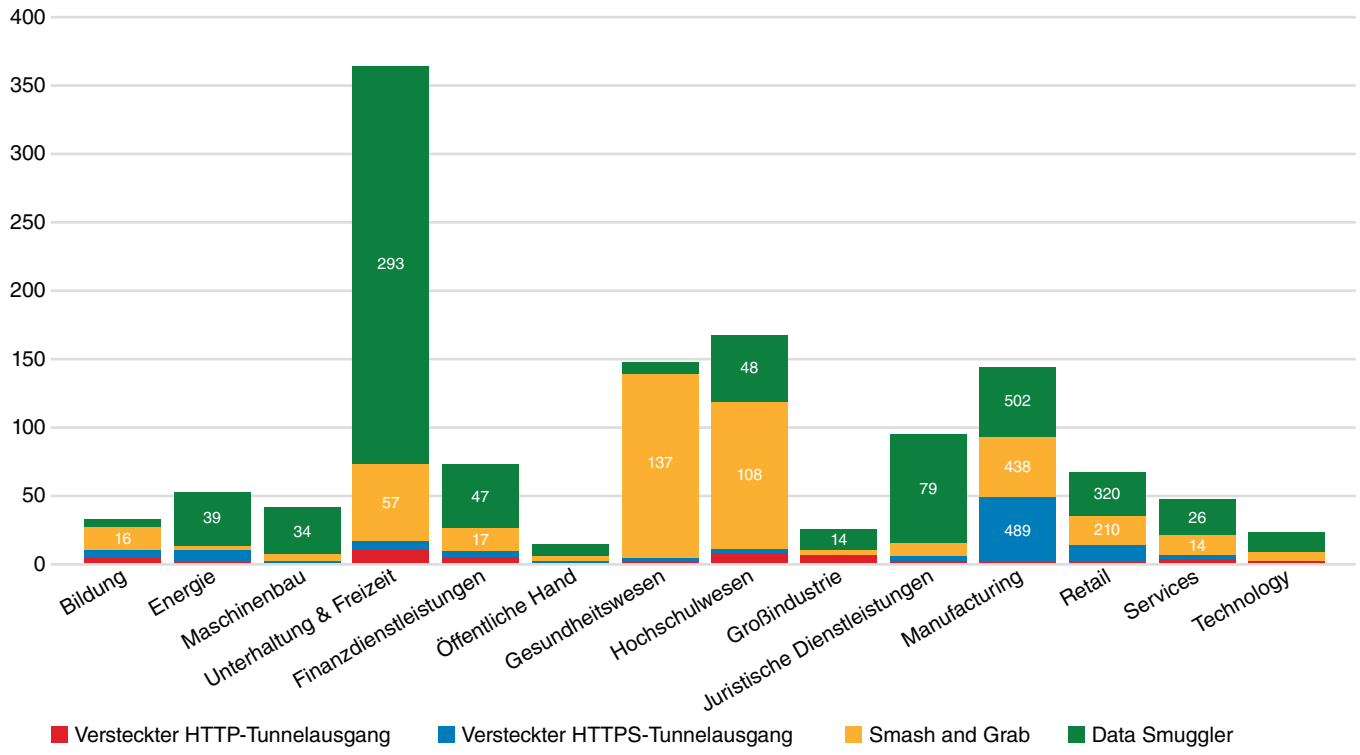
In der Dienstleistungsbranche deckte Cognito eine hohe Zahl an SMB-Brute-Force-Aktivitäten auf. Diese deuten darauf hin, dass ein Gerät – ausgehend von denselben Konten – eine Vielzahl von Anmeldeversuchen unternimmt, um auf einen Server zuzugreifen.



## Exfiltration nach Branchen

Smash-and-Grab ist in allen Branchen das häufigste Exfiltrationsverhalten. Es fällt auf, wenn ein Gerät ungewöhnlich große Datenmengen an Ziele sendet, die für die Umgebung nicht als normal gelten.

Die zweithäufigste Erscheinungsform der Exfiltration ist Data Smuggling. Dieses Verhalten trat vorwiegend in der Unterhaltungs- und Freizeitbranche auf. Es lässt sich daran erkennen, dass ein interner Host in großem Umfang Daten von einem oder mehreren Servern sammelt und dann ein signifikantes Datenvolumen zu einem externen System überträgt.




## Fazit

Für diese Ausgabe des Attacker Behavior Industrie Reports hat Vectra die Untersuchungsbasis auf mehr und im Durchschnitt größere Organisationen ausgeweitet. Einbezogen wurden mehr als 4,6 Millionen Geräte, mehr als doppelt so viele wie im vorhergehenden Report.

Vectra möchte sich an dieser Stelle bei den Organisationen bedanken, die sich dafür entschieden haben, Metadaten für die Studie zur Verfügung zu stellen. Insgesamt zeigen die Trends einen Anstieg bei den erkannten Bedrohungen und bei den identifizierten Verhaltensweisen von Angreifern, was Grund zur Sorge gibt.

Weil professionell vorgehende Cyberkriminelle auf Automatisierung setzen und die Effizienz ihrer eigenen Technologie steigern, gibt es einen dringenden Bedarf, im Gegenzug Werkzeuge für Informationssicherheit im Bereich Erkennung und Response zu automatisieren, um Bedrohungen schneller zu stoppen.

Gleichzeitig verhindert nach wie vor der globale Mangel an gut ausgebildeten Cybersecurity-Fachleuten, dass Bedrohungserkennung und Response-Maßnahmen in einem angemessenen Zeitrahmen bewältigt werden können. Vor diesem Hintergrund ist der Einsatz künstlicher Intelligenz unverzichtbar, um vorhandene Cybersecurity-Teams so zu unterstützen, dass sie Bedrohungen schneller erkennen und auf sie reagieren können. So sind sie den Angreifern stets einen Schritt voraus.

*Ich bin eine künstliche Intelligenz.*
*Die treibende Kraft hinter der Jagd auf Cyber-Angreifer.*
*Ich bin Cognito.*

VECTRA
Security that thinks®

**Email** info_DACH@vectra.ai **Tel.** +41 43 810 47 52 / +49 69 202 328 10 https://vectra.ai/dach