



# Angriffe über die Datenautobahn

Ein detaillierter Blick auf schädlichen DNS-Traffic

# Inhaltsverzeichnis

- 2** Domain Name Server – ein Einfallstor für Angriffstraffic
- 4** Akamai-Terminologie für die Analyse des DNS-Traffics
- 6** Gefahr im Verzug: Die Durchlässigkeit für schädlichen Traffic in Unternehmen
- 25** Privatnutzer werden angegriffen
- 33** Überblick über die Phishing-Landschaft
- 35** Fazit und Empfehlungen: Moderne Angriffe mit proaktiven Maßnahmen bekämpfen
- 36** Methodik
- 37** Herausgeber- und Mitarbeiterverzeichnis

## Domain Name Server – ein Einfallstor für Angriffstraffic

---

Das Domain Name System (DNS) ist seit seinen Anfängen ein wichtiger Bestandteil der Internetinfrastruktur. Ein Großteil unserer Internetnutzung, sei es zu Hause oder am Arbeitsplatz, basiert auf dem DNS, damit wir im World Wide Web korrekt zu unserem Ziel navigieren können. Es überrascht nicht, dass Angreifer diese Infrastruktur häufig für ihre Attacken ausnutzen – sei es eine Bedrohung, die auf C2-Server (Command and Control) zugreift, um Befehle abzurufen, oder eine Remotecodeausführung, bei der eine Domain aufgerufen wird, um schädliche Dateien auf eine Maschine herunterzuladen. Aufgrund seiner Allgegenwärtigkeit ist das DNS zu einem wichtigen Bestandteil der Angriffsinfrastruktur geworden.

Als Sicherheitsunternehmen verfügt Akamai über einen Blickwinkel, der es uns ermöglicht, [Unternehmen](#) wie auch [Privatnutzer](#) zu untersuchen und vor schädlichem DNS-Traffic zu schützen, der zu Systemgefährdung und Datendiebstahl führen könnte. In diesem Bericht werden wir eine Analyse des schädlichen Traffics bereitstellen, der sich an private Nutzer und Unternehmen weltweit richtet. Eine gründliche Analyse des schädlichen DNS-Traffics, einschließlich Korrelation mit Angreifergruppen oder -tools, kann Unternehmen mit wichtigen Informationen über die häufigsten Bedrohungen versorgen. Diese Informationen können Sicherheitsexperten dabei helfen, ihre Verteidigung zu bewerten und Lücken zu analysieren, um die Techniken und Methoden abzudecken, die gegen sie eingesetzt werden. Andernfalls kann es zu Vorfällen kommen, die zum Verlust vertraulicher Daten, zu finanziellen Schäden oder zu Strafen aufgrund von Compliance-Verstößen führen. Da die [Kosten für Cyberkriminalität](#) bis 2025 auf bis zu 10,5 Billionen US-Dollar pro Jahr steigen werden, müssen Unternehmen optimal auf Angriffe vorbereitet sein.

Bei der Analyse des schädlichen DNS-Traffics von Unternehmens- und Privatnutzern konnten wir mehrere Ausbrüche und Kampagnen erkennen, wie z. B. die Verbreitung von FluBot, einer Android-basierten Malware, die sich weltweit von Land zu Land bewegt, sowie die Aktivitäten verschiedener cyberkrimineller Gruppen, die auf Unternehmen abzielen. Das vielleicht beste Beispiel ist die starke Präsenz von C2-Traffic im Zusammenhang mit Initial Access Brokern (IABs), die Unternehmensnetzwerke angreifen und den Zugriff monetarisieren, indem sie ihn an andere weiterverkaufen, wie z. B. an RaaS-Gruppen (Ransomware as a Service). Diese Aktivitäten sind für uns im DNS-Traffic ersichtlich, und wir teilen sie zum Vorteil unserer Leser.

## Zusammengefasst



Unsere Daten zeigen, dass in den Netzwerken von 10 bis 16 % der Unternehmen mindestens einmal im Quartal C2-Traffic auftritt. Das Vorhandensein von C2-Traffic weist auf die Möglichkeit eines laufenden Angriffs oder einer Sicherheitsverletzung hin. Die Bedrohungen reichen von Datendiebstahl in Botnets bis hin zu IABs.



26 % der betroffenen Geräte haben bekannte IAB-C2-Domains kontaktiert, darunter Domains mit Emotet- und Qakbot-Bezug. IABs stellen ein großes Risiko für Unternehmen dar, da sie für gewöhnlich den ersten Angriff durchführen und dann den Zugriff an Ransomware-Gruppen und andere Cyberkriminelle verkaufen.



NAS-Geräte (Network Attached Storage) sind besonders beliebte Ziele, da sie seltener gepatcht werden und viele wertvolle Daten enthalten. Unsere Daten zeigen, dass Angreifer diese Geräte über QSnatch ausnutzen. 36 % der betroffenen Geräte in Unternehmensnetzwerken greifen auf C2-Domains zu, die mit dieser Bedrohung zusammenhängen.



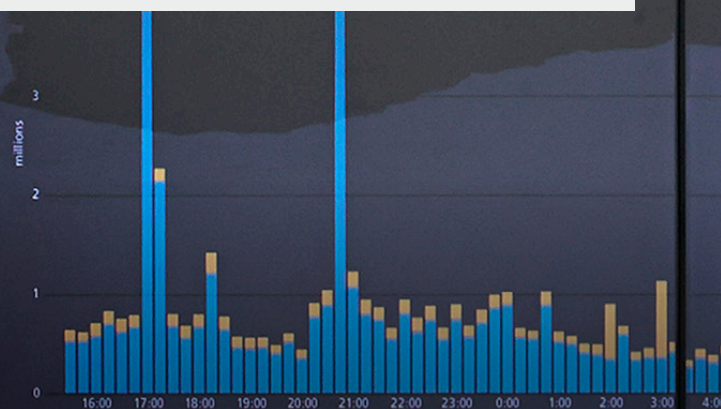
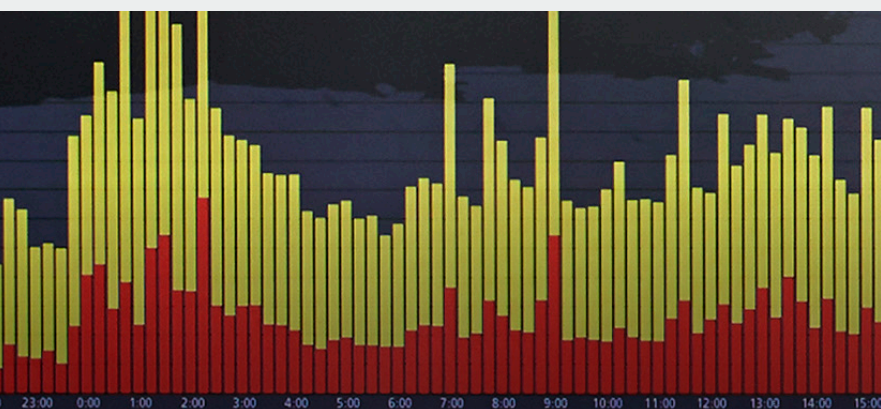
30 % der betroffenen Unternehmen sind im Fertigungssektor tätig – das sind doppelt so viele wie in der zweitgrößten Branche. Das verdeutlicht die realen Auswirkungen von Cyberangriffen wie Lieferkettenprobleme und Störungen des täglichen Lebens. Vorschriften wie [Netzwerk- und Informationssicherheit 2 \(NIS2\)](#) könnten dazu beitragen, Angriffe auf wichtige Branchen oder kritische Infrastrukturen wie die Fertigung einzudämmen.



Angriffe auf Heimnetzwerke versuchen nicht nur, herkömmliche Geräte wie Computer, sondern auch Mobiltelefone und das Internet of Things (IoT) auszunutzen. Ein beträchtlicher Teil des Angriffstraffics kann auf mobile Malware und IoT-Botnets zurückgeführt werden.



Durch unsere DNS-Datenanalyse haben wir einen wachsenden Ausbruch von FluBot-Malware in Europa, dem Nahen Osten und Afrika (EMEA), Lateinamerika (LATAM) sowie im asiatisch-pazifischen Raum und in Japan (APJ) entdeckt. Die Social-Engineering-Taktik der Malware und ihre Verwendung mehrerer Sprachen der Europäischen Union (EU) könnten einige der Faktoren sein, die zum Anstieg der Infektionen beitragen.



## Akamai-Terminologie für die Analyse des DNS-Traffics

---

Akamai [Edge DNS](#) und die [DNS-Infrastruktur](#) überwachen bis zu sieben Billionen DNS-Anfragen pro Tag. Um die Nutzer und Unternehmen von Akamai zu schützen, blockiert Akamai Anfragen an Domains, die Malware bereitstellen, oder an Websites, die Ihre Informationen stehlen könnten. Durch die Untersuchung dieser schädlichen DNS-Transaktionen können wir diese Domains in drei Kategorien einteilen – Malware, Phishing-Websites und C2 – und eine eingehende Untersuchung durchführen, um die größten Bedrohungen für Unternehmen und Privatnutzer zu ermitteln.

Aus einer sorgfältigen Datenerfassung des schädlichen DNS-Traffics können wir wichtige Schlüsse über die häufigsten Bedrohungen ziehen. Unser Schutz deckt zwei Demografien ab: Eine demografische Gruppe sind Unternehmen, bei der Akamai Unternehmensnetzwerke schützt, und die andere sind Privatnutzer, die über ihre persönlichen Netzwerke auf das Internet zugreifen und Bedrohungen wie Botnets ausgesetzt sind. Diese Bedrohungen versuchen, Nutzergeräte für schädliche Zwecke zu übernehmen, wie zum Beispiel für finanzielle Gewinne durch Cryptomining.



Zunächst wollen wir die Begriffe *Phishing-Websites*, *Malware* und *C2* definieren und erklären, wie wir sie in diesem Bericht verwenden.



**Phishing-Websites** sind Domains, die mit Phishing-Kits verknüpft sind. Sie ahmen das Erscheinungsbild von Einzelhandelsunternehmen, Banken, Hightech-Firmen und anderen Anbietern nach und klonen deren Websites, um Nutzer dazu zu bringen, Informationen wie Anmelde- oder personenbezogene Daten preiszugeben. Akamai beobachtet diesen Traffic über das DNS, um sowohl Unternehmens- als auch Privatnutzer vor Identitätsdiebstahl und Datenverlust zu schützen.



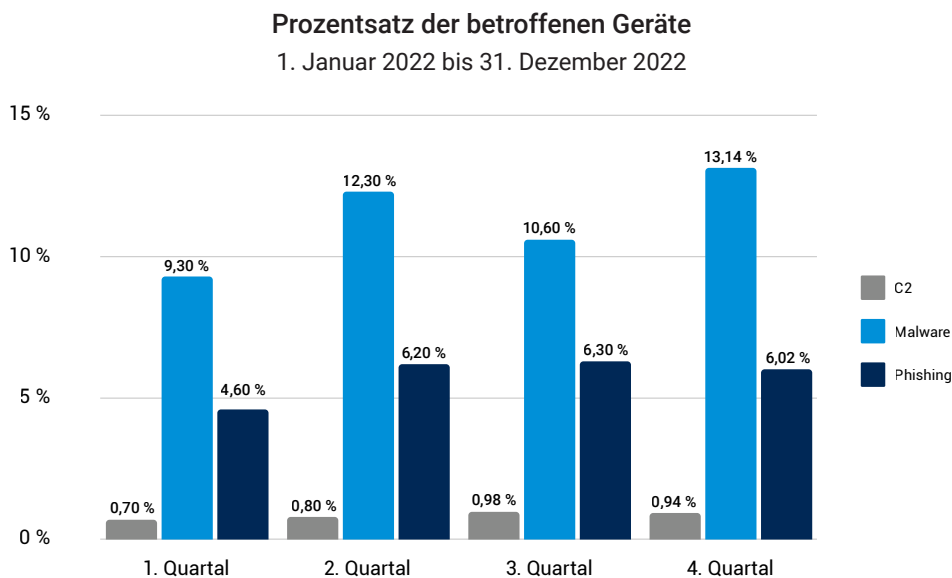
**Malware** ist eine schädliche Domain (oder Domains), die schädliche Dateien bereitstellt oder enthält. Diese Kategorie umfasst auch Websites, auf denen schädlicher JavaScript-Code gehostet wird, sowie kompromittierte Websites, die unerwünschte Anzeigen bereitstellen oder Nutzer auf eine Seite umleiten, die diese Anzeigen enthält. Bei vielen modernen Angriffen muss eine schädliche Datei von einer externen Quelle auf ein Gerät heruntergeladen werden, um die anfängliche Payload abzurufen oder die nächste Phase eines laufenden Angriffs herunterzuladen. Die Beobachtung und Blockierung dieses Traffics kann dazu beitragen, Unternehmen vor einer anfänglichen Infektion oder einem fortlaufenden Angriff zu schützen.



**C2** beschreibt im Kontext unserer DNS-Trafficanalyse eine Domain, die verwendet wird, um mit infizierten Geräten zu kommunizieren, Befehle zu senden und dann das Gerät zu steuern. Nach einem anfänglichen Angriff stellen Angreifer eine C2-Kommunikation zwischen dem infizierten System und einem von den Angreifern kontrollierten Server her, um zusätzliche Befehle zu senden und die Sicherheit des Systems oder Netzwerks weiter zu gefährden. Sie können beispielsweise andere Malware herunterladen und verbreiten, Daten extrahieren, das System herunterfahren und neu starten und vieles mehr. Die Erkennung von C2-Traffic ist von entscheidender Bedeutung, da sie einen aktiven Angriff signalisiert, der noch abgewehrt werden kann. Darüber hinaus unterbindet das Blockieren der Domains, die mit C2-Servern verknüpft sind, die Einrichtung der C2-Kommunikation und verhindert, dass die Malware weitere Anweisungen oder Befehle herunterlädt. So wird die Wahrscheinlichkeit verringert, dass Angreifer schädliche Aktivitäten in Ihrem Netzwerk ausführen.

# Gefahr im Verzug: Die Durchlässigkeit für schädlichen Traffic in Unternehmen

Basierend auf der Analyse des DNS-Traffics von Akamai konnten wir feststellen, dass 13 % der Geräte in Q4 2022 mindestens einmal versucht haben, Domains zu erreichen, die mit Malware in Verbindung standen (Abbildung 1). Darüber hinaus kommunizierten 6 % mit Domains, die Phishing betrafen. Im Bereich C2, auf den wir uns in diesem Bericht sehr stark konzentrieren werden, haben wir im Laufe des Jahres eine steigende Tendenz mit einem sehr leichten Rückgang im vierten Quartal beobachtet.



*Abb. 1: Wir beobachten einen wachsenden Trend bei geschützten Geräten, die mit schädlichen Zielen kommunizieren.*

Beachten Sie, dass sich Abbildung 1 nur auf einzelne Geräte bezieht, die versucht haben, mit schädlichen Domains zu kommunizieren. Wichtig ist hierbei die Diskrepanz zwischen Geräten, die Malware-Ziele erreichen (die von Angreifern zum Herunterladen von Malware genutzt werden können), und Geräten, die mit C2-Domains kommunizieren (die üblicherweise während eines laufenden Angriffs verwendet werden, um die Kommunikation zwischen Angreifer und Malware zu ermöglichen, und die zum Herunterladen zusätzlicher Malware verwendet werden können, um den Angriffszyklus voranzutreiben). Diese Diskrepanz kann auf die Unterschiede zwischen versuchter Netzwerkinfiltration (die beim ersten Versuch, Malware auf einen Computer herunterzuladen, blockiert werden kann) und erfolgreicher Infiltration (die in unseren Daten möglicherweise nicht über das DNS übertragen wurde) oder auf laufende Angriffe hindeuten, die sich an eine C2-Domain wenden, um die Attacke auszuführen.

Dieser Bericht konzentriert sich hauptsächlich auf C2-Traffic als potenziellen Indikator eines Falls, in dem ein Angreifer ein Gerät erfolgreich kompromittiert hat. Um die Verbreitung solcher Angriffe zu verstehen, müssen wir die Daten aus einer anderen Perspektive betrachten. Anstatt einzelne Geräte zu untersuchen, können wir die Daten nach Unternehmen aggregieren, um herauszufinden, wie häufig laufende Angriffe (angezeigt durch das Vorhandensein von C2-Traffic) innerhalb des Datensatzes auftreten.

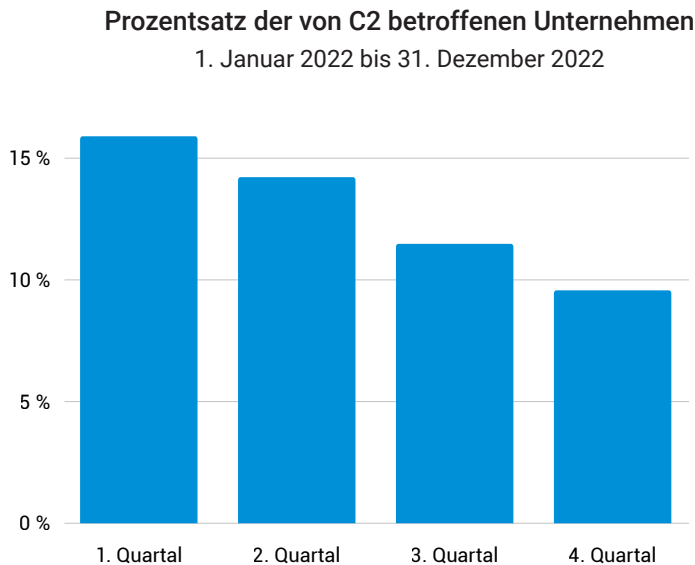


Abb. 2: Eine Analyse des schädlichen C2-Traffics zeigt den Prozentsatz der Unternehmen, in denen mindestens ein Gerät im Laufe des Jahres auf eine C2-Domain zugreift.

**Unseren DNS-Daten zufolge wurde bei 10 bis 16 % der Unternehmen beobachtet, dass mindestens einmal in jedem beliebigen Quartal C2-Traffic ihr Netzwerk verließ.**

Unseren DNS-Daten zufolge wurde bei 10 bis 16 % der Unternehmen beobachtet, dass mindestens einmal in jedem beliebigen Quartal C2-Traffic ihr Netzwerk verließ (Abbildung 2). Dies kann ein Hinweis darauf sein, dass Malware versucht, mit einem Betreiber zu kommunizieren, und ist ein Anzeichen für eine potenzielle Sicherheitsverletzung. Dieser C2-Traffic wurde von unserer Lösung daran gehindert, sein Ziel zu erreichen, aber erfolgreiche Angriffe hatten möglicherweise Datenextraktion, Ransomware-Angriffe und vieles mehr zur Folge. Im ersten Halbjahr 2022 wurden 2,3 Milliarden Malware-Varianten entdeckt, mit einem Durchschnitt von [1.501 pro Tag](#). Unsere Untersuchung zeigt, wie effektiv die Nutzung des DNS dazu beitragen kann, Schäden durch die Ausbreitung von Malware in einem Netzwerk zu verhindern.



## Initial Access Broker stellen eine weitverbreitete Bedrohung für Unternehmen dar

Mehrstufige Angriffe haben sich in der modernen Angriffslandschaft etabliert (Abbildung 3). Angreifer können ihren Erfolg steigern, wenn sie es schaffen, zusammen (oder füreinander) zu arbeiten, oder wenn es ihnen gelingt, verschiedene Tools für einen konzertierten Angriff zu kombinieren. C2 ist entscheidend für den Erfolg dieser Angriffe. Sie können nicht nur für die Kommunikation verwendet werden, sondern auch das Herunterladen einer Payload und weiterer Malware ermöglichen, um den Angriff fortzusetzen. Dies wird am besten durch die **Angriffskette** der Ransomware Emotet/TrickBot/Ryuk veranschaulicht, die in den letzten Jahren beobachtet wurde. Emotet infiltriert zunächst das Netzwerk des Opfers, und sobald der erste Zugriff eingerichtet ist, greift es auf eine Domain zu, um die TrickBot-Payload herunterzuladen und persönliche Daten, Anmeldeinformationen und vieles mehr zu stehlen. Wenn das Opfer als wertvolles Ziel für die Angreifer angesehen wird, greift die Malware dann auf die C2-Server zu und lädt die endgültige Payload herunter: die Ryuk-Ransomware.

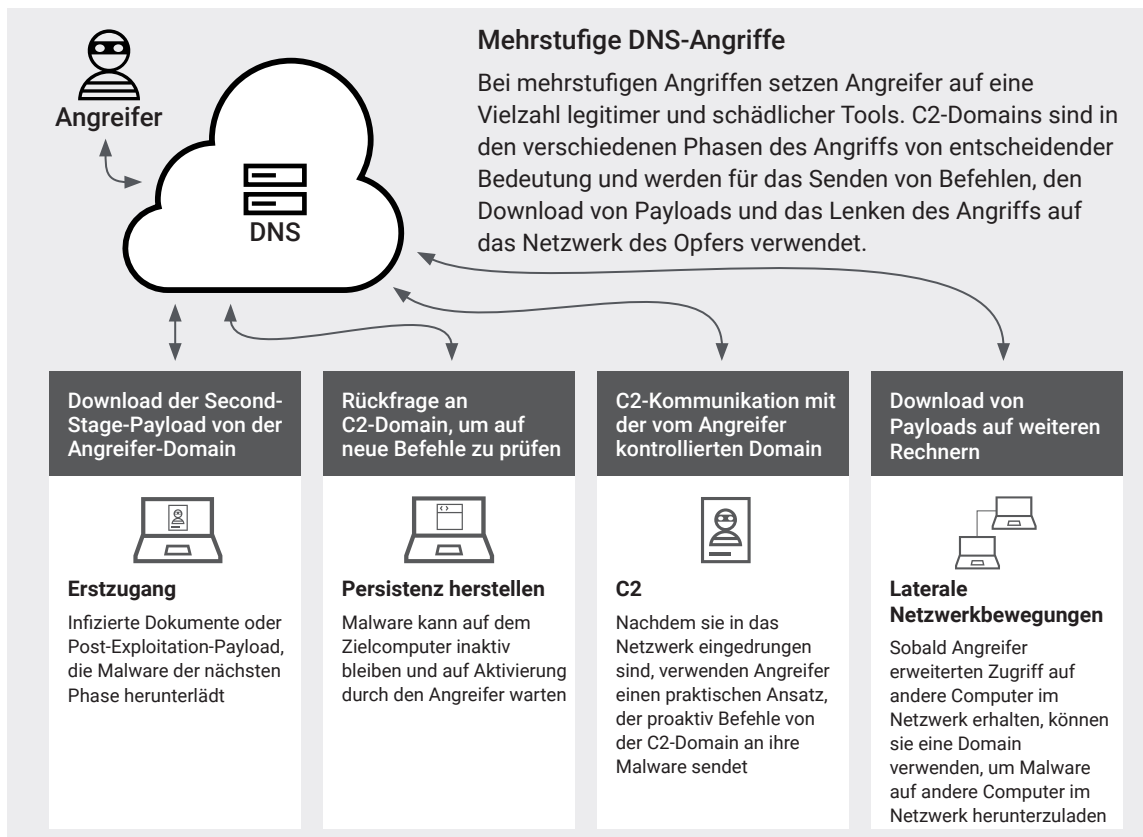
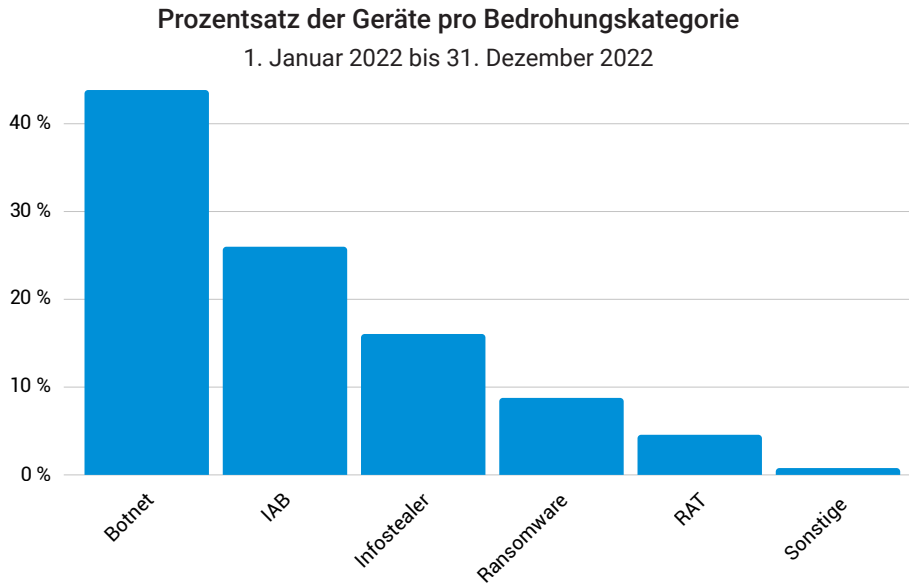


Abb. 3: Die Rolle von C2 in jeder Phase des Angriffs

Diese Ereigniskette ist bei der Bewertung der in diesem Bericht enthaltenen Informationen wichtig. C2-Kommunikation kann in verschiedenen Phasen des Angriffs erfolgen. Unsere jüngste Analyse der Methodik moderner Ransomware-Gruppen wie der **Conti-Gruppe** hat gezeigt, dass raffinierte Angreifer häufig einen Operator zuweisen, der den Angriff aktiv betreut, um ihn schnell und effizient voranzutreiben (der „Hand on Keyboard“-Ansatz). Die Möglichkeit, C2-Traffic zu erkennen und zu blockieren, kann für die Abwehr eines laufenden Angriffs von entscheidender Bedeutung sein.

Die von uns beobachteten C2-Domains können in Domains mit und ohne Zuordnung zu einer bestimmten Bedrohungsart oder Angreifergruppe kategorisiert werden. In diesem Abschnitt werden wir uns näher mit C2-Domains befassen, die mit einem Bedrohungstyp verknüpft sind, und helfen Lesern dabei, das Risikoniveau entsprechend den Fähigkeiten und Methoden jeder Gruppe zu bewerten. Beachten Sie, dass einige dieser Malware-Familien für mehrere Anwendungsfälle geeignet sein können, je nachdem, wie Angreifer sie während einer Attacke verwenden.



*Abb. 4: Unternehmen werden hauptsächlich von Botnets angegriffen, gefolgt von IABs und Infostealern.*

In Abbildung 4 werden Angreifergruppen in IABs, Botnets und RaaS-Gruppen klassifiziert. Unsere Daten zeigen, dass IABs eine der größten Bedrohungen für Unternehmensnetzwerke darstellen, ebenso wie Botnets, die auf Datenextraktion abzielen.



#### **Initial Access Broker**

IABs konzentrieren sich hauptsächlich darauf, anderen Cyberkriminellen, einschließlich Ransomware-Gruppen, einen ersten Einstiegspunkt zu bieten, um sich Zugang zu den Netzwerken von Unternehmen zu verschaffen. Persistenz, Remote-Payload-Ausführung nach dem Eindringen sowie Datenextraktion.



#### **Ransomware-as-a-Service-Gruppen**

Dies sind Gruppen, die es anderen Angreifern (selbst solchen ohne technisches Know-how) ermöglichen, Partner zu werden und ihre Ransomware gegen eine Gebühr zu nutzen.



#### **Botnets**

Angreifer können Botnets für unzählige Zwecke nutzen – von Cryptomining und DDoS-Angriffen bis hin zu Datenextraktion, Malware-Implementierung und lateraler Netzwerkbewegung.



#### **Infostealer**

Infostealer erfassen verschiedene Arten von Daten wie Nutzernamen, Passwörter, Systeminformationen, Banking-Anmeldedaten, Cookies und so weiter.

Wir beobachten auch Ransomware, Remote Access Tools (RATs) und Infostealer, die alle in verschiedenen Angriffsphasen eine entscheidende Rolle spielen. Und illegale Tools, die sowohl Neulingen unter den Angreifern als auch erfahrenen Cyberkriminellen zur Verfügung stehen und diesen ermöglichen, Netzwerke zu infiltrieren, sich dort zu verbergen und Angriffe voranzutreiben, sind eine der Ursachen dafür, dass die Anfälligkeit von Unternehmen für Cyberkriminalität immer weiter zunimmt. Bei der Betrachtung dieser Gruppierungen beschäftigen wir uns auch mit den sich ergebenden Schnittstellen, an denen Angriffe ansetzen, und den potenziellen Auswirkungen für Unternehmen.

## IAB-Gruppen

Diese spezielle Gruppe von Cyberkriminellen, die als „Initial Access Broker“ (IABs) bezeichnet wird, konzentriert sich hauptsächlich darauf, anderen Cyberkriminellen und Angreifern einen ersten Einstiegspunkt zu bieten, um in den Netzwerken von Unternehmen Fuß zu fassen. Zwar nutzen verschiedene Cyberkriminelle ähnliche Angriffsmethoden – z. B. die Ausnutzung von RDP- und VPN-Schwachstellen, Brute-Force-Angriffe, das Sammeln sogenannter Credential Dumps (Gruppen von Anmeldedaten) sowie Phishing-E-Mails mit Malware –, doch IABs sind darauf spezialisiert, Zugriff auf diese infizierten Systeme zu erlangen und diesen Zugriff an andere Gruppen zu verkaufen, anstatt den gesamten Angriff durchzuführen. Ransomware-Gruppen hinter LockBit, Darkside, Conti und BlackByte **nutzten Berichten zufolge IABs** im Rahmen ihrer Aktivitäten. In einer Studie aus dem Jahr 2023 wurde festgestellt, dass der **durchschnittliche Verkaufspreis** für den Erstzugang derzeit etwa 2.800 US-Dollar beträgt.

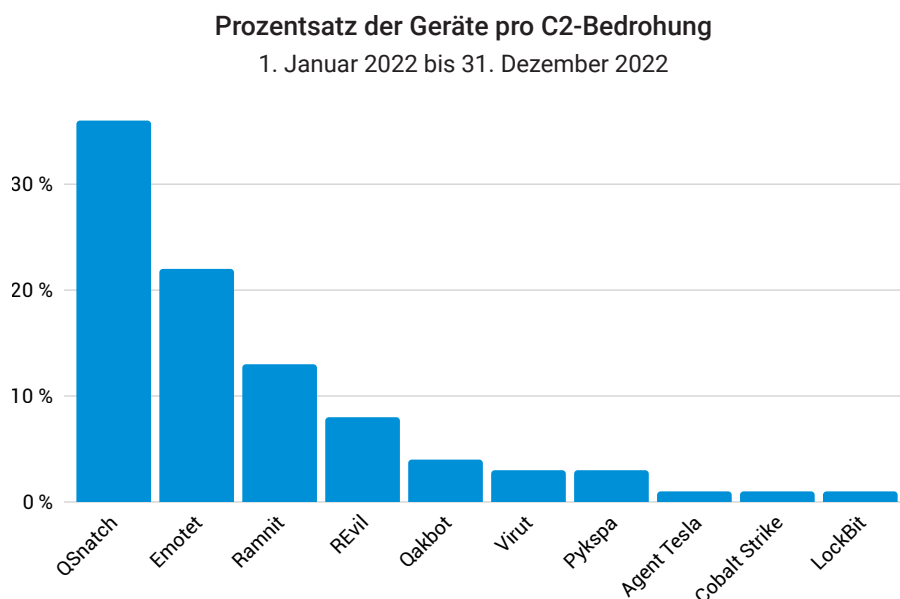
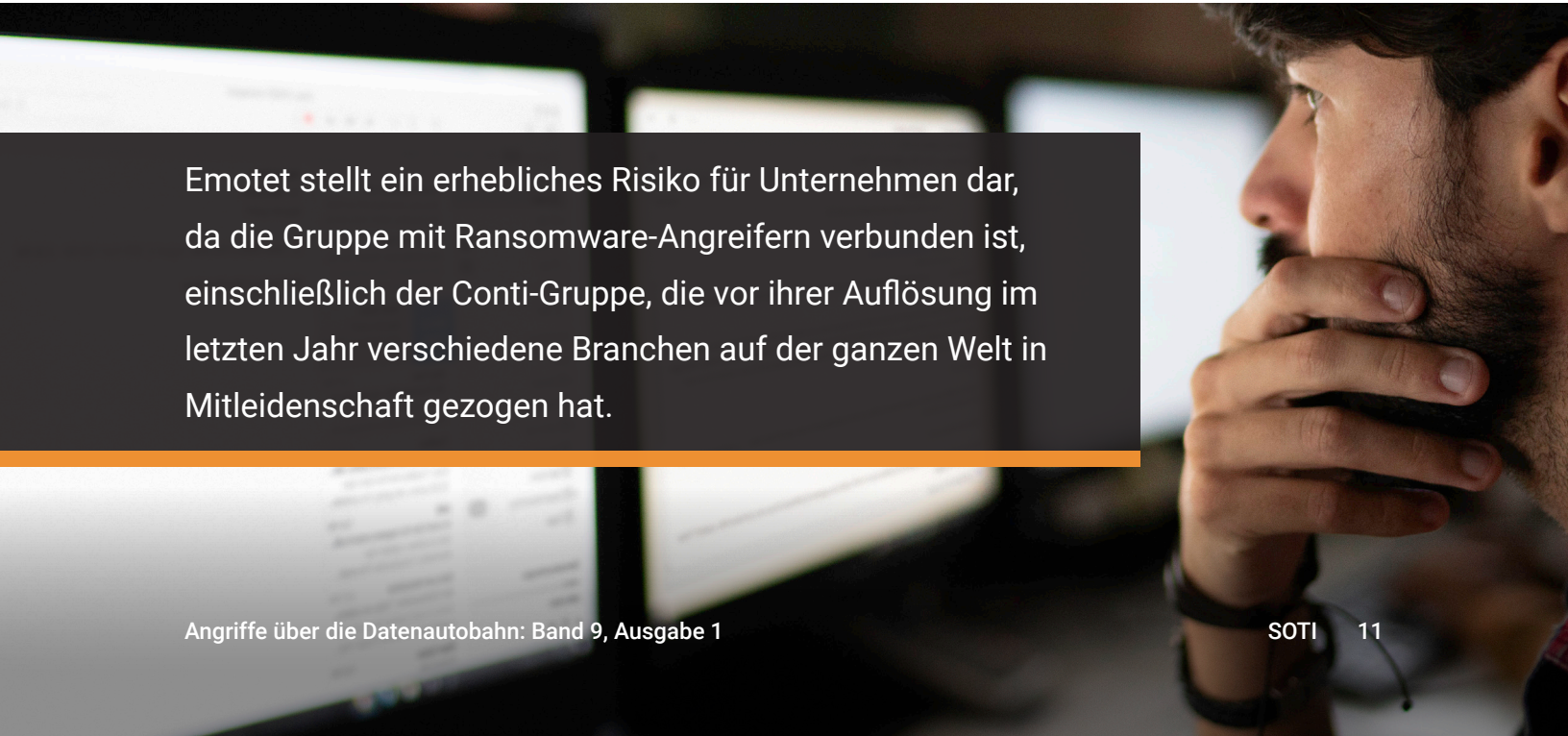


Abb. 5: QSnatch, Emotet und Ramnit sind die führenden C2-Familien im Netzwerktraffic von Unternehmen.

Laut unseren DNS-Daten (Abbildung 5) haben 26 % der infizierten Geräte mit IAB-verbundenen Domains wie [Qakbot](#) (4 % der infizierten Geräte) und [Emotet](#) (22 % der infizierten Geräte) kommuniziert. IABs spielen eine wichtige Rolle im RaaS-Geschäftsmodell und in der gesamten Landschaft der Cyberkriminalität. Ransomware-Angreifer und Cyberkriminelle benötigen Remotezugriff und Anmeldedaten nicht nur, um die Netzwerke ihrer Opfer zu infiltrieren, sondern auch, um sich unter anderem lateral im Netzwerk zu bewegen, Persistenz aufzubauen und Zugangsrechte zu erlangen. Angreifer nutzen IABs, um die zeitaufwendigen Aufgaben der Aufklärung, des potenziellen Zielscans und der Erstinfektion zu erledigen. Mit IABs, die im Untergrund leicht verfügbar sind, entfällt dieser Schritt und Angreifer benötigen weniger Fachwissen oder Zeit, um eine Attacke durchzuführen. Dieser Umstand führt zu einer Vielzahl potenzieller Angriffe auf Zielunternehmen, die Ransomware, gestohlene Anmeldedaten und vertrauliche Informationen, Spionage und Datenschutzverletzungen zur Folge haben.

Emotet erweist sich in unseren Daten als einer der bekanntesten IABs. Emotet stellt ein erhebliches Risiko für Unternehmen dar, da die Gruppe mit Ransomware-Angreifern verbunden ist, einschließlich der Conti-Gruppe, die vor [ihrer Auflösung](#) im letzten Jahr verschiedene Branchen auf der ganzen Welt in Mitleidenschaft gezogen hat. Im Laufe der Jahre fügte Emotet weitere Module hinzu, wie z. B. Funktionen für Distributed Denial of Service (DDoS) und E-Mail-Diebstahl, und erweiterte seine anvisierten Ziele. Von einem Banking-Trojaner/-Botnet mit einer Fülle von Funktionen wechselte Emotet zu einer Malware as a Service (MaaS) und verteilte Bedrohungen wie den IcedID-Banking-Trojaner, TrickBot und die UmbreCrypt-Ransomware. Die TrickBot-Gruppe nutzte Emotet auch zur Verteilung mehrerer Ransomware-Versionen, darunter Ryuk, ProLock und Conti. Ein detaillierterer Überblick über die von Emotet verwendeten Techniken finden Sie im [MITRE ATT&CK-Framework](#) zu diesem Thema.



Emotet stellt ein erhebliches Risiko für Unternehmen dar, da die Gruppe mit Ransomware-Angreifern verbunden ist, einschließlich der Conti-Gruppe, die vor ihrer Auflösung im letzten Jahr verschiedene Branchen auf der ganzen Welt in Mitleidenschaft gezogen hat.

Der zweithäufigste IAB in den Daten ist Qakbot. Diese Gruppe hat bekanntermaßen mit der Ransomware-Gruppe „Black Basta“ zusammengearbeitet, die [Berichten zufolge](#) mindestens 50 Organisationen aus verschiedenen Teilen der Welt betroffen hat. Das Qakbot-Team ist bekannt für seine Funktionen zum Datendiebstahl und für die Bereitstellung von Second-Stage-Malware, um die Systemsicherheit weiter zu beeinträchtigen. Laut Forschungsergebnissen [nutzt Qakbot Cobalt Strike](#), ein legitimes Tool für Penetrationstests, das von Red Teams eingesetzt und von Angreifern ausgenutzt wird, um nach dem Eindringen eine Reihe schädlicher Aktivitäten durchzuführen und eine Backdoor in die Umgebung des Opfers zu öffnen. Diese Technik wird in den letzten Jahren zunehmend [von IABs verwendet](#). Das MITRE ATT&CK-Framework kann zusätzliche Informationen zu [den Techniken](#) liefern, die Qakbot während seines Angriffs einsetzt.

## Botnet-Gruppen

In unserer Analyse stellen Botnets mit 44 % des analysierten C2-Traffics die größte Gruppe von Bedrohungstypen dar. In dieser Gruppe sind zahlreiche Angreifer vertreten. Hierbei ist es wichtig, daran zu denken, dass nicht alle Botnets gleich sind. Weniger schädliche Varianten könnten Cryptominer einsetzen oder die Maschine des Opfers für DDoS-Angriffe ausnutzen. Zwar können auch diese Versionen Kosten verursachen, doch in Unternehmen finden sich auch Botnets, die für Datenextraktion und mehrstufige Angriffe verwendet werden – was ein höheres Risiko darstellen kann. Botnets können sich lateral im Netzwerk verbreiten und zur Bereitstellung von Ransomware verwendet werden, wie im Fall von TrickBot. Oder sie konzentrieren sich speziell auf den Diebstahl von Informationen und das Sammeln von Anmeldedaten.

Wir haben festgestellt, dass [QSnatch](#), das größte Botnet in Unternehmensumgebungen, genau das tut: die Datenextraktion von Netzwerkgeräten. Unseren Daten zufolge machte QSnatch 36 % der infizierten Geräte aus. Diese Malware richtet sich gezielt an QNAP, eine Art NAS-Gerät, das von Unternehmen für Sicherungen oder Dateispeicherung verwendet wird. Obwohl die Infektionsmethode noch immer unbekannt ist, gehen Forscher davon aus, dass QSnatch Geräte durch Ausnutzung von Firmware-Schwachstellen oder Brute-Force-Angriffe auf Geräte mit Standard-Nutzernamen/-Passwörtern infizieren könnte. Es wird dringend empfohlen, dass Unternehmen, die QNAP verwenden, ihre Firmware auf dem neuesten Stand halten (nach einer Infektion würde [QSnatch die Installation von Patches verhindern](#), ebenso wie die Deaktivierung von Sicherheitsprodukten) und die Standardpasswörter sofort ändern. QSnatch wird von Angreifern zum Scraping von Anmeldedaten, zur Passwortprotokollierung, für Remotezugriff sowie zur Datenextraktion verwendet, um nur einige zu nennen. Angreifer können es auf Speichergeräte abgesehen haben, da diese eine Fülle an wertvollen Informationen enthalten. Wenn diese Geräte infiziert werden, haben Unternehmen im Falle von Ransomware-Angriffen keine Backups mehr. Einzelheiten zu Taktiken und Gegenmaßnahmen werden in dieser [CISA-Warnung](#) vorgestellt.

## Ransomware-as-a-Service-Gruppe

In unserer Analyse des DNS-Traffics haben 9 % der infizierten Geräte, die mit C2-Familien kommuniziert haben, auf Domains zugegriffen, die mit RaaS-Gruppen verbunden sind. Diese Art von Cyberkriminellen ermöglicht es anderen Angreifern (auch ohne technisches Know-how), Partner zu werden und ihre Ransomware gegen eine Gebühr zu nutzen. Unternehmen, die von Ransomware betroffen sind, sehen sich mit unzähligen Konsequenzen konfrontiert, die nicht auf den Verlust vertraulicher Unternehmensdaten beschränkt sind. Sie könnten außerdem mit Wiederherstellungskosten, Anwaltsgebühren, Bußgeldern, Ausfallzeiten, die zu Produktivitätseinbußen führen, sowie Marken- und Reputationsschäden zu kämpfen haben. Cybersecurity Ventures prognostizierte, dass die [Kosten für Ransomware-Angriffe](#) bis 2031 etwa 265 Milliarden US-Dollar jährlich betragen werden. Der [globale Ransomware-Bericht](#) von Akamai beleuchtet auch die lähmenden Auswirkungen von Ransomware, die über finanzielle Verluste hinausgehen, wie z. B. Unterbrechungen der Lieferkette – in einigen Fällen kann Ransomware sogar [eine Frage von Leben und Tod](#) sein.

Eine produktive RaaS-Gruppe ist die REvil-Gruppe, die durch die Attacke auf einen [IT-Management-Anbieter](#) im Rahmen eines Lieferkettenangriffs, von dem mehr als 1.500 Managed Service Provider betroffen waren, zweifelhafte Berühmtheit erlangte. Ihr Betrieb wurde eingestellt, nachdem mehrere [Mitglieder von der russischen Regierung festgenommen worden waren](#). Einige Monate nach der Auflösung stellten Sicherheitsforscher jedoch fest, dass die Leak-Website von REvil wieder aktiv war und Informationen über die jüngsten Opfer enthielt, darunter einige Universitäten in den Vereinigten Staaten. Forscher spekulierten, dass es sich hierbei [nicht um dieselbe REvil-Gruppe handelte](#), die diese Kampagne leitete, und haben davor gewarnt, dass Nationalstaaten die REvil-Gruppe ausnutzen könnten, um ihre Spuren zu verwischen. Was die Taktik angeht, so ist [REvil dafür bekannt, den Angriffsfluss an die beabsichtigten Opfer anzupassen](#), was veranschaulicht, wie gut die Gruppe über ihre Ziele Bescheid weiß. Weitere Informationen zu Taktiken, Techniken und Verfahren im Zusammenhang mit REvil finden Sie im [Beitrag von MITRE](#).

**Angreifer können es auf Speichergeräte abgesehen haben, da diese eine Fülle an wertvollen Informationen enthalten. Wenn diese Geräte infiziert werden, haben Unternehmen im Falle von Ransomware-Angriffen keine Backups mehr.**

Eine weitere RaaS-Gruppe, die wir bei unserer Untersuchung des DNS-Traffics entdeckt haben, ist LockBit. Nach dem „Verschwinden“ von Conti wurde die LockBit-Gruppe zu einem der aktivsten RaaS-Anbieter. Zuvor (von November 2019 bis März 2022) war es laut diesem [Bericht](#) die RaaS mit der höchsten Anzahl getroffener Organisationen nach Conti.

Die LockBit-Gang ist stolz darauf, dass sie über einen [schnelleren Verschlüsselungsmechanismus](#) verfügt als andere RaaS-Gruppen, und [behauptete](#), mit ihrem LockBit 2.0 mehr als 12.000 Unternehmen getroffen zu haben. Im Juni 2022 veröffentlichte die Gruppe LockBit 3.0 mit zusätzlichen Funktionen, einschließlich eines Bug-Bounty-Programms. Berichten zufolge [nutzt die Gruppe auch die Log4j-Schwachstelle](#), um anfänglichen Zugriff auf seine Ziele zu erhalten, was die Bedeutung von Patching unterstreicht. Unternehmen, die solche Sicherheitslücken nicht behoben haben, sind möglicherweise einem erhöhten Risiko ausgesetzt, mit LockBit infiziert zu werden. LockBit erfindet sich immer wieder neu – eine der jüngsten Erpressungstaktiken ist die [dreifache Erpressungstaktik](#), bei der Dateien verschlüsselt, auf Leak-Websites veröffentlicht und DDoS-Angriffe gestartet werden, wenn Opfer sich weigern, das Lösegeld zu zahlen.

## Tools der Branche

Die in diesem Abschnitt genannten Tools können eine bestimmte Rolle bei einem Angriff spielen, sei es die Systeminfiltration, das Einholen von Informationen oder die Eskalation von Berechtigungen. Das Arsenal, das wir von verschiedenen Angreifergruppen gesehen haben, erfordert häufig Kommunikation, um wie Infostealer und RATs zu agieren. Wenn Sie diese Tools und die Taktiken von Angreifergruppen kennen, können Sicherheitsexperten besser verstehen, wie Angriffe ablaufen, und entsprechend planen.

### Infostealer

Infostealer wurden für den Zugriff auf verschiedene Datentypen entwickelt, wie z. B. Nutzernamen, Passwörter, Systeminformationen, Banking-Anmeldedaten und Cookies. Sie sind nach wie vor eines der MaaS-Angebote, die häufig bei Angriffen eingesetzt werden. Angreifer, die möglicherweise nicht über das technische Wissen und/oder die nötigen Fähigkeiten verfügen, können sich einfach zu relativ niedrigen Kosten Infostealer beschaffen und ihre eigenen Angriffe starten.

In der Liste von C2-Malwarefamilien haben wir beobachtet, dass 16 % der Geräte, die auf bekannte C2-Ressourcen zugegriffen haben, Infostealer nutzten. [Ramnit](#) (13 % der infizierten Geräte) ist nicht nur ein gewöhnlicher Infostealer. Seine Stärke liegt in der hohen Modularität, die es Angreifern ermöglicht, seine verschiedenen Funktionen zu nutzen, wie z. B. den Diebstahl anderer sensibler Daten und das Herunterladen/Bereitstellen anderer Malware, um ihr Endziel zu erreichen oder den Angriff voranzutreiben. Im Jahr 2021 galt Ramnit als der führende [Banking-Trojaner](#). In den jüngsten Nachrichten wurde berichtet, dass eine andere Malware einen [ähnlichen Code](#) nutzte wie Ramnit.





Die Präsenz von Infostealern in Ihrem Netzwerk ist ein deutliches Zeichen dafür, dass die Anmeldedaten eines Nutzers gefährdet sein könnten. Die gesammelten gestohlenen Informationen könnten in Untergrundmärkten verkauft und ausgenutzt werden, um anderen Angreifern den ersten Zugriff zu verschaffen. Ransomware-Gruppen können Infostealer über Phishing oder Botnets bereitstellen, um gültige Anmeldedaten zu erhalten, können in einem Schwarzmarktforum, das MaaS anbietet, [Zugriffslizenzen für einen Infostealer vermieten](#) oder Netzwerkzugriff über IABs erwerben. In einigen Fällen können Infostealer-Betreiber zu IABs werden und wertvolle Anmeldedaten (wie VPN- oder RDP-Zugriff) an die Höchstbietenden oder andere Cyberkriminelle verkaufen, die einen weitaus komplexeren Angriff starten könnten.

### Tools für Remotezugriff

Cobalt Strike wurde von mehreren Angreiferguppen im Rahmen ihrer Attacken ausgenutzt. Es gibt verschiedene Bereiche, für die dieser leistungsstarke RAT von Angreifern genutzt wird, darunter Aufklärung, Berechtigungseskalation, laterale Netzwerkbewegung, das Erreichen von Persistenz, Remote-Payload-Ausführung nach dem Eindringen (z. B. Ransomware) sowie Datenextraktion. Obwohl das Tool hauptsächlich für laterale Netzwerkbewegung und Exfiltration nach dem Eindringen verwendet wird, kann es auch als erster Zugangsvektor dienen, da es über ein [Spear-Phishing-Modul](#) verfügt. Gruppen, von denen bekannt ist, dass sie dieses Tool verwenden, sind [Conti](#), [Qakbot](#), [TrickBot](#) und [Emotet](#), um nur einige zu nennen. Um die Erkennung von Cobalt Strike in einer Umgebung zu erleichtern, wurden diese [YARA-Regeln](#) erstellt, um die schädliche Verwendung des Tools zu ermitteln.

Unsere Daten zeigen auch das Vorhandensein von C2-Traffic für [Agent Tesla](#). Dieser RAT wird [auf dem Untergrundmarkt verkauft](#), und sein erschwinglicher Preis und die Nutzerfreundlichkeit machen dieses Tool für Cyberkriminelle äußerst attraktiv. Angreifer können dieses Tool verwenden, um Anmeldedaten von verschiedenen Browsern zu sammeln, Tastenanschläge zu erfassen (Keylogging) und Screenshots aufzunehmen. Eine der bemerkenswerten Taktiken des Unternehmens ist das „Form Grabbing“ (Formularerfassung), das es Angreifern ermöglicht, personenbezogene Daten und andere vertrauliche Informationen zu stehlen. Diese gestohlenen Informationen können dann für Identitätsdiebstahl oder Betrug verwendet werden. PCrisk hat [weitere Details](#) zu den Techniken von Agent Tesla und den Auswirkungen für betroffene Nutzer veröffentlicht.



## Aktivitätslandschaft zeigt sporadische Malware-Kampagnen im Laufe des Jahres

Im Laufe eines Jahres haben wir Schwankungen bei den Aktivitäten von C2-Malware beobachtet (Abbildung 6). Hierzu ein Beispiel: Nach seinem [Wiederaufflammen im November 2021](#) war Emotet im Januar und Februar 2022 besonders aktiv. Dieser Anstieg der Aktivität deutet auf eine beeindruckende Kampagne hin, die der Gruppe helfen soll, nach Monaten der Inaktivität ihren alten Status zurückzuerlangen. In den Monaten nach seinem Comeback verbesserte Emotet seine Taktik, indem es Möglichkeiten hinzufügte, die von Microsoft vorgenommene Deaktivierung von Anwendungsmakros in Visual Basic zu umgehen. Einige [Berichte](#) deuten darauf hin, dass Emotet zwischen Juli und November 2022 wieder inaktiv wurde. Unsere Datenbeobachtungen zeigen einen Rückgang des C2-Traffics im Juli, wie an dem geringeren Prozentsatz infizierter Geräte zu erkennen ist, die mit Emotet-Domains kommunizieren. Dies kann darauf hinweisen, dass die Gruppe das ganze Jahr über aktiv war, oder es könnte sich um installierte Malware handeln, die noch immer mit einer veralteten Infrastruktur kommuniziert. Die Beobachtungen im Jahr 2023 könnten uns helfen festzustellen, ob die Emotet-Gruppe tatsächlich inaktiv geworden ist.

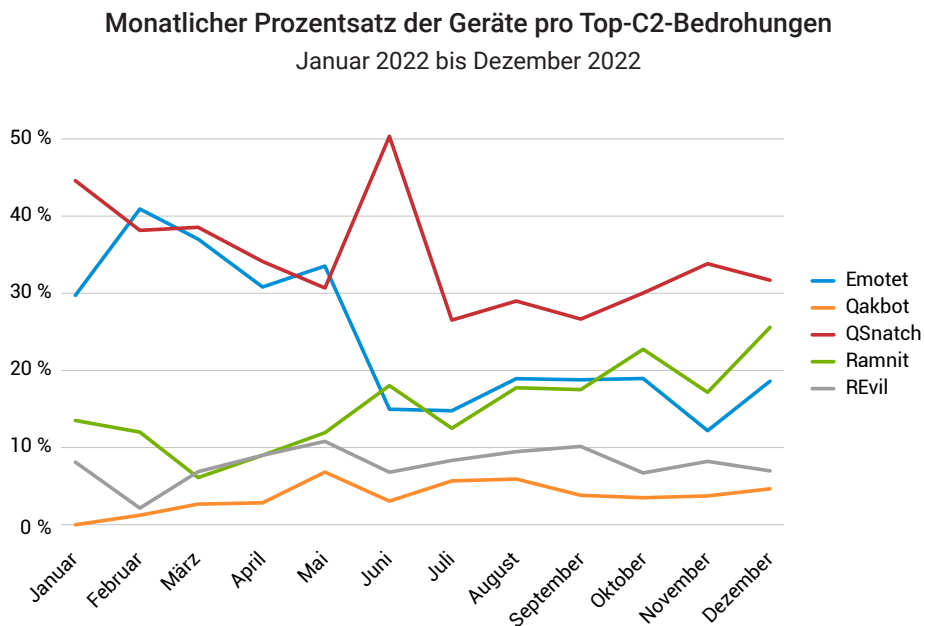


Abb. 6: Das monatliche Trenddiagramm zeigt, dass QSnatch 2022 durchgehend aktiv war.

**Nach seinem Wiederaufflammen im November 2021 war Emotet im Januar und Februar 2022 besonders aktiv. Dieser Anstieg der Aktivität deutet auf eine beeindruckende Kampagne hin, die der Gruppe helfen soll, nach Monaten der Inaktivität ihren alten Status zurückzuerlangen.**

QSnatch war das ganze Jahr über aktiv und erreichte seinen Höchststand im Juni. Das zeigt, wie beharrlich diese Bedrohung ist. NAS-Server sind aus mehreren Gründen beliebte Ziele unter Angreifern: Erstens enthalten sie sensible Daten, zweitens ist die Wahrscheinlichkeit, dass NAS-Server gepatcht werden, geringer, und drittens sind diese Geräte im Unternehmensnetzwerk potenziell leichter zugänglich und könnten als Ausgangspunkt für laterale Netzwerkbewegung dienen. Zwar gab es in den letzten Jahren Veränderungen, wie die Einführung integrierter Sicherheitslösungen, doch Cyberkriminelle konnten diese umgehen, indem sie installierte Sicherheitsprodukte deaktiviert und/oder Geräte daran gehindert haben, mit neuen Fixes aktualisiert zu werden. Daher sind diese Geräte weiterhin anfällig für neue Arten dieser Malware.

Wir sehen auch, dass Ramnit von August bis Dezember in immer mehr Unternehmensnetzwerken zu finden war. Das ist besorgniserregend, da diese Malware eine Vielzahl vertraulicher Informationen stehlen könnte, die Angreifer später an andere Kriminelle für zukünftige Angriffe verkaufen könnten.

### QSnatch und Emotet: Häufige Bedrohungen in allen Regionen

Um die verbreiteten Bedrohungen pro Region zu ermitteln, haben wir den Anteil der Geräte in der jeweiligen Region untersucht, die mit C2-Domains kommunizieren (Abbildung 7). Jeder Prozentsatz ist relativ zur Anzahl der betroffenen Geräte pro Region, die ebenfalls je nach Region unterschiedlich ist. Interessanterweise sehen wir ähnliche Angriffstrends in allen Regionen, wenn auch mit sehr wenigen Ausreißern. Wir empfehlen daher, dass jede Region die Empfehlungen im Abschnitt „Fazit und Empfehlungen“ bzw. unter jeder Malware-Gruppe in den obigen Abschnitten befolgt.

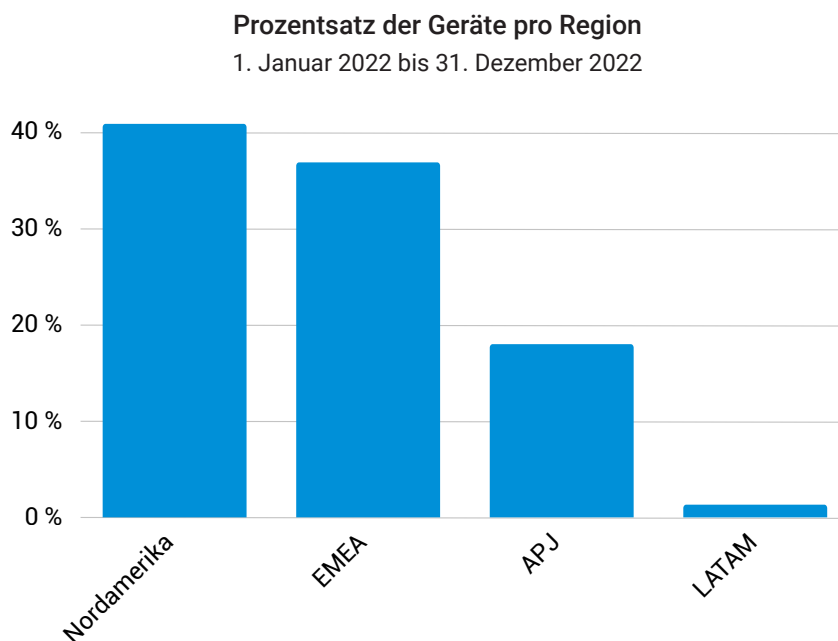


Abb. 7: Nordamerika liegt mit 41 % an der Spitze, wenn es um die Anzahl der betroffenen Geräte pro Region geht, gefolgt von EMEA (37 %) und APJ (18 %).

## Nordamerika

Die meisten Unternehmen weltweit litten unter diesen beiden größten Bedrohungen: QSnatch und Emotet. In Nordamerika enthielten etwa 29 % der betroffenen Geräte in der Region Emotet, während 33 % von QSnatch betroffen waren (Abbildung 8). Laut einem [Bericht](#) von Dark Reading ergab eine Suche nach Shodan, dass 300.000 QNAP-Geräte mit dem Internet verbunden sind, was es zu einem attraktiven Ziel macht. Darüber hinaus könnten NAS-Geräte wie QNAP als Backup verwendet werden und als Medien- oder Fileserver dienen.

Weitere nennenswerte Bedrohungen in Nordamerika sind Ramnit, Qakbot und REvil. Das ist interessant, wenn man bedenkt, wie IABs wie Emotet den Weg für andere Infektionen geebnet haben, unter anderem für Ransomware.

Prozentsatz der Geräte pro Top-C2-Bedrohung in Nordamerika

1. Januar 2022 bis 31. Dezember 2022

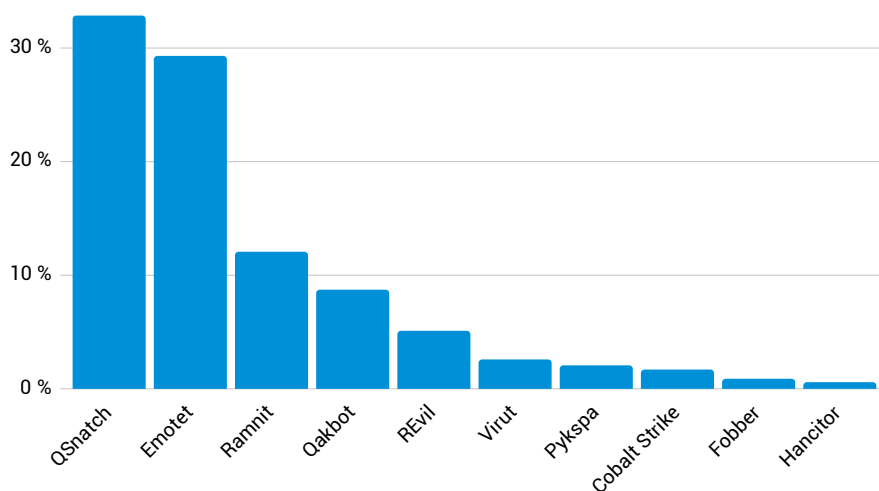


Abb. 8: Die Mehrzahl der betroffenen Geräte in nordamerikanischen Unternehmen griff mindestens einmal auf Domains zu, die mit QSnatch, Emotet und Ramnit zusammenhingen.



## Europa, Naher Osten und Afrika

EMEA weist neben Nordamerika den höchsten Prozentsatz betroffener Geräte auf. Die größten Bedrohungen, die wir in der Region erfasst haben (Abbildung 9), waren QSnatch (28 %) und Ramnit (21 %). Es überrascht nicht, dass Ramnit in der Region aufgestiegen ist, da seine Betreiber in der Vergangenheit [Banken-/Finanzinstitute in Italien, dem Vereinigten Königreich und Frankreich ins Visier nahmen](#). In einer seiner Iterationen enthielt Ramnit als Hauptziele EU-Länder. Wenn man die Anzahl der weltweit von Ramnit betroffenen Geräte vergleicht, macht EMEA nach wie vor die meisten Ramnit-Infektionen aus. Darüber hinaus gab es mit 19 % ebenfalls viele Geräte mit Emotet-Infektion in der Region.

### Prozentsatz der Bedrohungen pro Top-C2-Bedrohung in EMEA

1. Januar 2022 bis 31. Dezember 2022

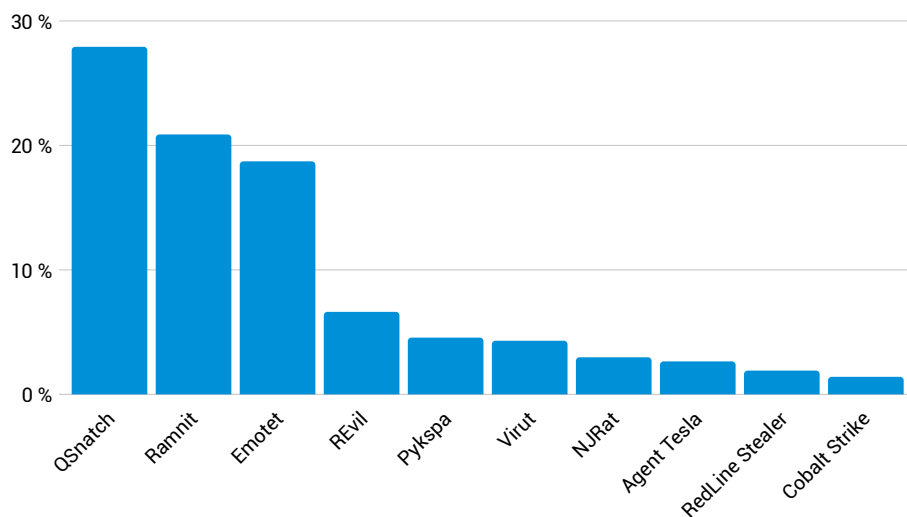


Abb. 9: In der EMEA-Region erreichten mehr Geräte Ramnit-C2-Domains als in anderen Regionen, was das Risiko für Unternehmen in der Region deutlich erhöhte.

## Asiatisch-pazifischer Raum und Japan

In APJ haben wir festgestellt, dass QSnatch-Infektionen die Region signifikant beeinflussen (Abbildung 10). Wenn wir die Zahlen hinter jeder Region vergleichen, liegt APJ in Bezug auf Geräte mit QSnatch-Infektionen hinter Nordamerika an zweiter Stelle. Andererseits sollten Verantwortliche in APJ auch auf die Ransomware-Versionen REvil und LockBit achten, da sie zu den fünf häufigsten Bedrohungen auf betroffenen Geräten in der Region gehörten. Obwohl Mitglieder der [REvil-Gruppe letztes Jahr verhaftet wurden](#), wurde diese Malware einige Monate später wieder in freier Wildbahn gesehen. Es ist möglich, dass alte Mitglieder, die Zugang zu dem Code haben, versucht haben, REvil wiederzubeleben. Es ist nicht überraschend, Ransomware-Bedrohungen (die größtenteils finanziell motiviert sind) wie LockBit und REvil zu begegnen. Und da RaaS-Betreiber weiterhin IABs wie Emotet nutzen, bleibt Ransomware für Unternehmen in allen Branchen und Regionen eine entscheidende Sicherheitsherausforderung.

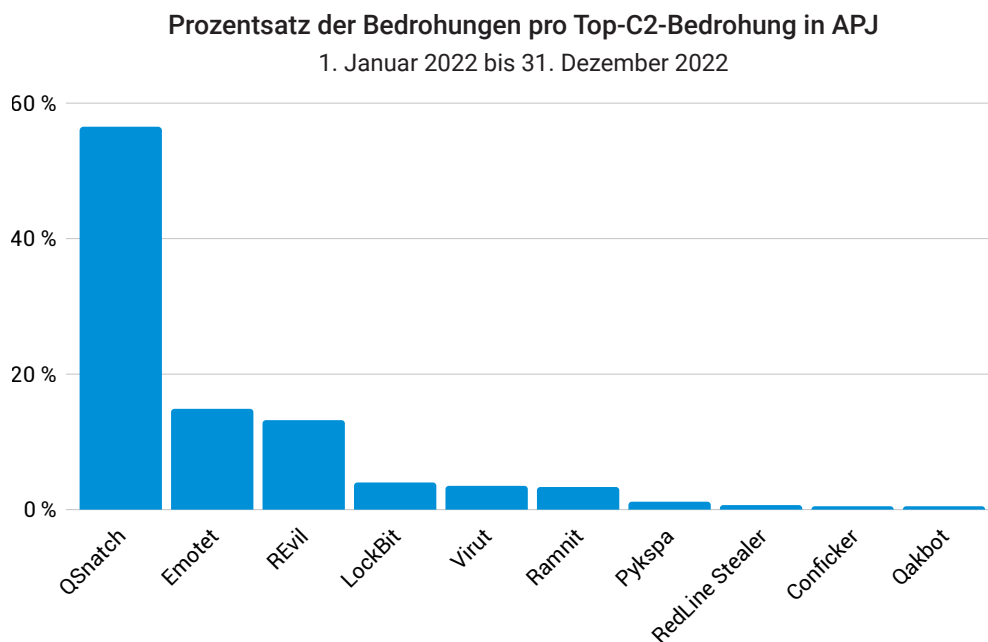
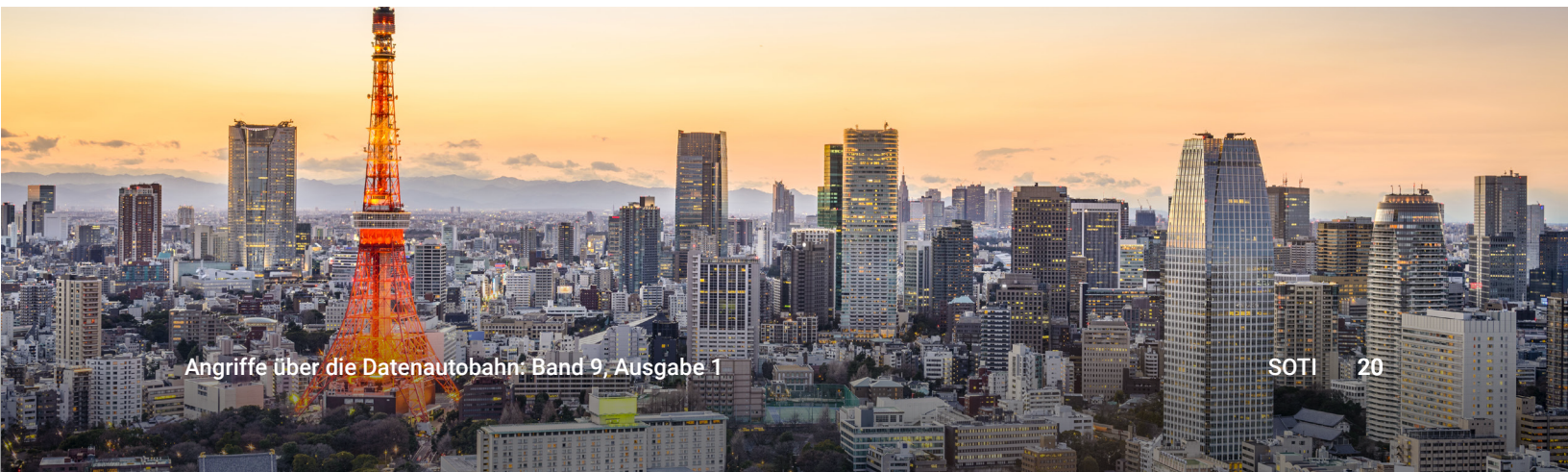


Abb. 10: Akamai beobachtete eine erhebliche Anzahl von QSnatch-Infektionen in der Region.



## Lateinamerika

Lassen Sie uns nun die Trends in LATAM untersuchen. Obwohl diese Region über die geringste Anzahl betroffener Geräte verfügt, bedeutet das nicht unbedingt, dass sie weniger angegriffen wird oder dass sie weniger unter den Folgen von Angriffen zu leiden hat. Ähnlich wie die globalen Trends wurde auch diese Region von QSnatch und Emotet getroffen (Abbildung 11). Allein die Untersuchung dieser einzelnen Region zeigt, dass Agent Tesla, Virut und Ramnit stark vertreten sind.

### Prozentsatz der Bedrohungen pro Top-C2-Bedrohung in LATAM

1. Januar 2022 bis 31. Dezember 2022

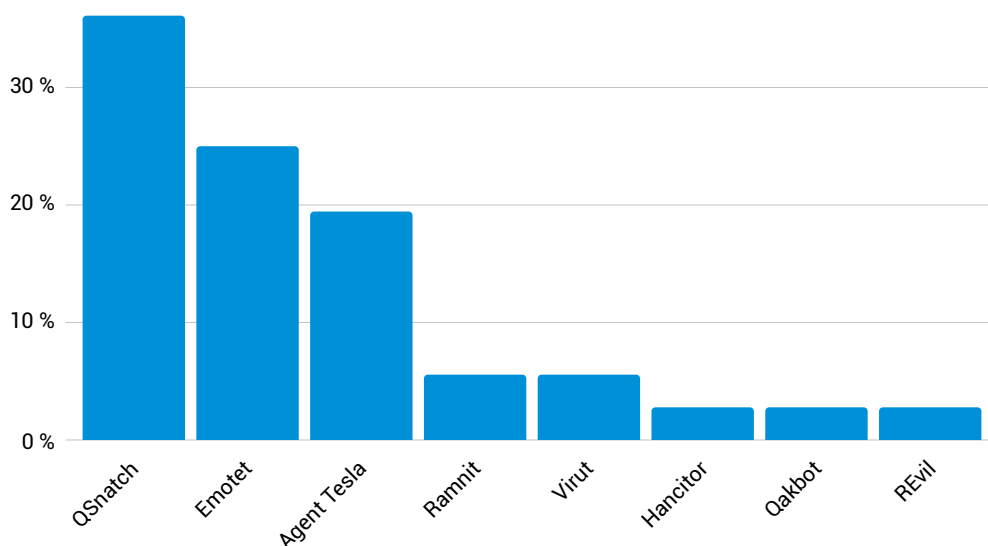


Abb. 11: Globale Trends finden sich auch in der Bedrohungslandschaft von LATAM.

Regionale Aufschlüsselungen sind nicht nur wichtig, um Gemeinsamkeiten zu erkennen, sondern auch um zu ermitteln, welche spezifischen Bedrohungen für jede Region einzigartig sind. Obwohl QSnatch immer die führende Bedrohungsfamilie ist, ändern sich die nächsten vier größten Bedrohungen je nach Region – mit einer Mischung aus Emotet, REvil, Ramnit und Agent Tesla. Regionale Bedrohungen spielen eine wichtige Rolle, wenn Sie entscheiden, worauf sich Ihre Schwachstellenmanagement- und Pentest-Teams konzentrieren sollten.

## Branchentrends: Fertigung stark von Initial Access Brokern und Botnets betroffen

Anhand einer Analyse von Branchentrends können wir das Risikoniveau jedes einzelnen Sektors und seine Lage im Vergleich zu anderen Branchen einschätzen. Anstatt die Anzahl der betroffenen Geräte zu untersuchen, haben wir die Geräte nach Kunden zusammengefasst, um zu ermitteln, wie viele Unternehmen pro Branche betroffen sind (Abbildung 12). Basierend auf unseren DNS-Daten haben wir festgestellt, dass mehr als 30 % der analysierten Unternehmen mit schädlichem C2-Traffic im Fertigungssektor angesiedelt sind. Darüber hinaus waren Unternehmen in den Branchen Business Services (15 %), Hightech (14 %) und Handel (12 %) betroffen. Die beiden wichtigsten Branchen in unseren DNS-Daten – Produktion und Business Services – finden sich ebenfalls in den Top-Branchen, die von der Conti-Ransomware betroffen sind (die wir in unserem [globalen Ransomware-Bericht](#) behandelt haben). In diesem Bericht haben wir uns intensiv mit den Opfern der Conti-Ransomware befasst und sie nach Branchen, Umsatz und Region geordnet, was die Angriffstrends dieser produktiven Bedrohung veranschaulichte.

**Basierend auf unseren DNS-Daten haben wir festgestellt, dass mehr als 30 % der analysierten Unternehmen mit schädlichem C2-Traffic im Fertigungssektor angesiedelt sind. Darüber hinaus waren Unternehmen in den Branchen Business Services (15 %), Hightech (14 %) und Handel (12 %) ähnlich stark betroffen.**

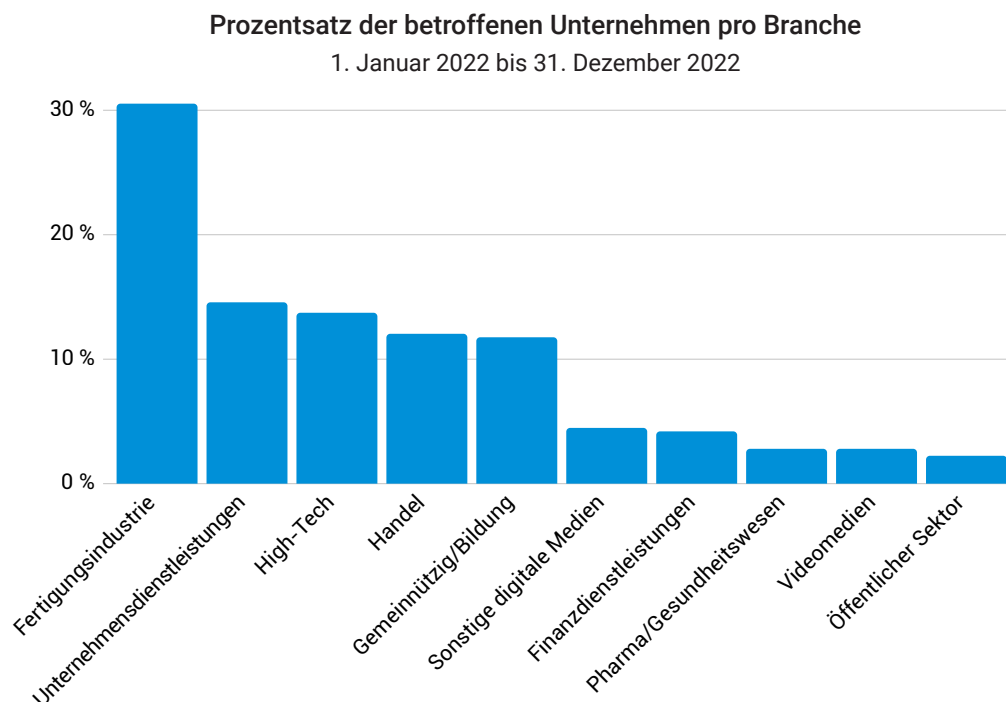


Abb. 12: Fertigung, Business Services und Hightech sind die Branchen, die am stärksten von C2-Infektionen betroffen sind.



Die Tatsache, dass das Fertigungsgewerbe von verschiedenen C2-Angriffen stark betroffen ist, ist besorgniserregend, da es als kritische Infrastruktur gilt und erfolgreiche Angriffe auf diese Branche reale Auswirkungen wie Lieferkettenstörungen haben können. Die Daten zeigen keine spezifischen Gründe dafür, warum die Fertigung die am stärksten betroffene Branche ist, doch eine genauere Untersuchung der Bedrohungsarten in dieser Branche könnte etwas Licht ins Dunkel bringen.

In einigen Ländern werden Vorschriften zur Erhöhung der Sicherheit in kritischen Sektoren wie der Fertigung angewendet. Die EU-weite Gesetzgebung mit der Bezeichnung „NIS2“ hat Cybersicherheitsstandards und -anforderungen erhöht, darunter Risikoanalysen und Sicherheitsstrategien für Informationssysteme, die Sicherheit der Lieferkette sowie Vorfallsbearbeitung für systemrelevante Einrichtungen (z. B. Energie, Verkehr, Banken). Außerdem wurde der Umfang der betroffenen Branchen erweitert.

### Prozentsatz der Bedrohungen pro Top-C2-Bedrohung in Fertigung

1. Januar 2022 bis 31. Dezember 2022

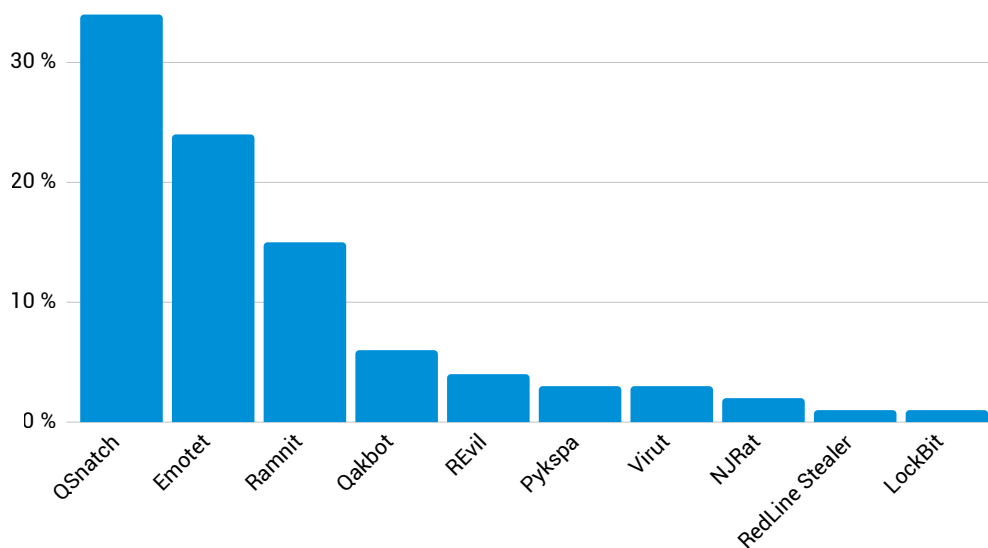


Abb. 13: Die größten C2-Bedrohungsfamilien in der Fertigungsbranche sind QSnatch, Emotet und Ramnit.



Ein ausführlicher Blick auf die Fertigungsbranche zeigt, dass QSnatch, IABs und Ramnit zu den am häufigsten verwendeten C2-Domains gehören, auf die Unternehmen in dieser Branche zugegriffen haben (Abbildung 13). Das Vorhandensein von IABs in ihrem Netzwerk könnte darauf hindeuten, dass Angreifer Informationen über ihre potenziellen Ziele sammeln. Und sobald sie Zugriff auf kompromittierte Computer haben, können sie diese Daten an andere Cyberkriminelle wie RaaS-Gruppen verkaufen. Außerdem sehen wir in der Liste der C2-Malware, die diese Branche bedroht, auch Infostealer. Eine nennenswerte Bedrohung ist [Redline Stealer](#), das Browserinformationen wie Anmelde- und Kreditkartendaten sammeln kann und derzeit als MaaS verkauft wird – im Rahmen eines monatlichen Abonnements zwischen 100 und 150 US-Dollar. Laut einer [Studie von Group-IB](#) hat dieser Infostealer zwischen H2 2021 und H1 2022 schätzungsweise 35.585.412 Protokolle gesammelt, die möglicherweise SSO-Konten (Single Sign-on) enthalten. Darüber hinaus haben die mit diesem Infostealer verbundenen C2-Domains allein in Q3 2022 [um 409 % zugenommen](#).

Branchentrends sind immer interessant nachzuverfolgen. Was in einer Branche geschieht, ist oft nur der Ausgangspunkt, da sich Cyberkriminelle durch die gesamte Landschaft und alle Branchen arbeiten. Manchmal erleben wir, dass sich Angreifer auf eine bestimmte Technologie konzentrieren, die in der jeweiligen Branche eine wichtige Rolle spielt. In anderen Fällen zielen sie auf diejenigen ab, die am wahrscheinlichsten oder am meisten zahlen. Wir haben auch erlebt, wie sie sich auf Branchen konzentrieren, die traditionell nicht so viel in Cybersicherheit investieren. Das Fazit lautet: Wenn es im Nachbarhaus brennt, ist es eine gute Idee, seine eigenen Brandschutzmaßnahmen zu überprüfen.



## Privatnutzer werden angegriffen

---

Angreifer richten ihr Augenmerk auf Unternehmen, da sich ein erfolgreicher Angriff auf ihre Netzwerke stärker auszahlt. Sie nutzen eine Vielzahl von Tools und Taktiken, um in das Unternehmensnetzwerk einzudringen, Persistenz zu schaffen und in einigen Fällen vertrauliche Informationen zu extrahieren. Dementsprechend sehen wir Bedrohungen wie Infostealer und IABs in Unternehmensnetzwerken, wie im vorherigen Abschnitt erläutert. In Heimnetzwerken findet sich jedoch ein anderes Szenario, was die Bedrohungen und ihren Zweck angeht.

Privatnutzer sind eine Zielgruppe, die im Vergleich zu Unternehmensumgebungen weniger gesichert, jedoch auch weniger einträglich ist. Angreifer wissen das und suchen daher nach Möglichkeiten, Profit daraus zu schlagen, dass Heimgeräte einfacher infiziert werden können. So werden beispielsweise große Kampagnen gestartet, bei denen mit einer Dauerfeuertaktik so viele Geräte wie möglich kompromittiert werden sollen, während Angriffe auf Unternehmen viel zielgerichteter ablaufen. Sobald diese Heimgeräte Teil eines massiven Botnets werden, können Angreifer diese Zombie-Geräte mobilisieren, um ohne Wissen des Nutzers unzählige cyberkriminelle Aktivitäten durchzuführen, wie Spamming und DDoS-Angriffe auf Unternehmen. Damit Botnets erfolgreich sind oder Cyberkriminelle ihre Botnets vermieten können, müssen sie so viele Geräte wie möglich infizieren. Eine weitere Möglichkeit für Angreifer, finanziell von Attacken auf Privatnutzer zu profitieren, ist die Nutzung der Computerressourcen infizierter Geräte für Cryptomining.

**Sobald diese Geräte Teil eines massiven Botnets werden, können Angreifer diese Zombie-Geräte mobilisieren, um ohne Wissen des Nutzers unzählige cyberkriminelle Aktivitäten durchzuführen, wie Spamming und DDoS-Angriffe auf Unternehmen.**

## Heimnetzwerke sind stark durch von Botnets verursachten Traffic betroffen

Mit Blick auf Privatnutzer untersuchen wir den schädlichen DNS-Traffic von Heimnetzwerken, indem wir eine anonymisierte Stichprobe der Millionen als bösartig gekennzeichneten Abfragen aus den letzten sechs Monaten analysieren und anhand dieser veranschaulichen, welche Bedrohungen für die Nutzer Anlass zu echter Sorge sein sollten. Auf den ersten Blick beziehen sich die größten Bedrohungen auf Botnets. Das könnte erklären, wie Angreifer IoT-Geräte für verschiedene Zwecke nutzen, auf die wir in den nachfolgenden Abschnitten näher eingehen werden.

## Anzahl der Abfragen pro Top-C2-Bedrohung

Juli 2022 bis Januar 2023

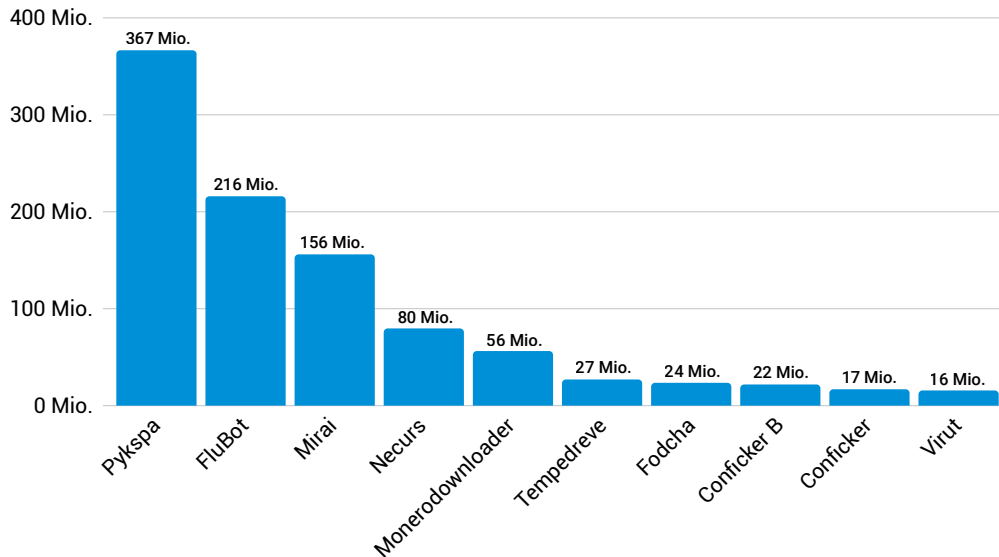


Abb. 14: Pykspa, FluBot und Mirai sind die drei wichtigsten Botnets im DNS-Traffic von Heimnetzwerken.

### Pykspa: Verbreitung über soziale Medien

Auf Grundlage unserer Datenergebnisse war Pykspa für weltweit 367 Millionen DNS-Abfragen verantwortlich (Abbildung 14). Diese Bedrohung verbreitet sich über Skype, indem sie schädliche Links an die Kontakte der betroffenen Nutzer sendet. In bestimmten Fällen, in denen Twitter auf einem Browsertab geöffnet ist, wird außerdem ein Tweet mit einem Download-Link zur Malware veröffentlicht. Darüber hinaus verwendet Pykspa einen Domain Generation Algorithm (DGA), um die C2-Kommunikation herzustellen. In der Vergangenheit verwendete v2 der Bedrohung eine [Teilmenge ihrer DGA](#), um zu verhindern, dass sie erkannt wurde, und verblieb so länger im Netzwerk.

Die [Backdoor-Funktionen ermöglichen es Angreifern](#), eine Verbindung zu einem Remotesystem herzustellen und unter anderem beliebige Befehle auszuführen, wie das Herunterladen von Dateien, das Beenden von Prozessen und die Verbreitung über verschiedene Mittel (z. B. zugeordnete Laufwerke, Netzwerkfreigaben). Pykspa fragt außerdem die Skype-Konfiguration ab, um persönliche Informationen über die betroffenen Nutzer zu sammeln. Darüber hinaus wird der Zugriff auf bestimmte Websites verhindert, insbesondere wenn diese bestimmte Zeichenfolgen enthalten, die auf Anti-Malware-Lösungen hindeuten. Interessant dabei ist, dass Pykspa die Spracheinstellungen des betroffenen Nutzers für Skype überprüft. Wenn es sich um eine der zahlreichen überwachten Sprachen (einschließlich Deutsch, Englisch, Italienisch, Französisch und Spanisch) handelt, wird die Spam-Nachricht in Skype von der Malware entsprechend angepasst.

## FluBot: Android-basiertes Malware-Botnet

Nach Pykspa ist die FluBot-Malware die führende C2-Malwarefamilie. Android-Smartphones werden hauptsächlich per Textnachrichten infiziert, in denen Nutzer dazu verleitet werden, auf einen schädlichen Link zu klicken, der dann zum Download der Malware führt. Im Rahmen ihrer [Verbreitungstaktik](#) lädt die FluBot-Malware die Kontaktlisten der betroffenen Nutzer auf den C2-Server hoch und sendet den gleichen Social-Engineering-Köder an die Kontakte der Opfer. Für Nutzer bedeutet FluBot auf ihrem Gerät ein Risiko für ihre Banking- und Finanzdaten, da diese Malware eine gefälschte Seite überlagern kann, wenn Nutzer auf legitime Banking-Apps zugreifen. Daher können diese Anmeldedaten für Identitätsdiebstahl oder betrügerische Transaktionen verwendet werden.

Diese Malware verwendet verschiedene Social-Engineering-Köder. Beispielsweise kann sie Nutzer dazu bringen, auf einen Link zu klicken, um den Status ihrer Paketzustellung zu überprüfen. In anderen Fällen kann sie Nutzer dazu verleiten, eine falsche Voicemail-App herunterzuladen, indem sie ihnen mitteilt, dass eine Mailbox-Nachricht auf sie wartet. Sie kann auch [vorgeben, ein Sicherheitsupdate zu sein](#), und Nutzer dazu auffordern, auf den Link zu klicken. Sobald Nutzer auf den Link klicken, werden sie aufgefordert, eine App herunterzuladen. Diese App fordert wiederum die Berechtigung an, auf Kontaktlisten zuzugreifen, Anrufe zu tätigen usw. Was diese Bedrohung so gefährlich macht, ist, dass sie auch [eine Berechtigung für Barrierefreiheitsdienste anfordert](#). Hiermit können Angreifer Touch-Eingaben vornehmen, was potenziell zur Installation weiterer Apps führt. Nutzer sollten [ihre Geräte auf die Werkseinstellungen zurücksetzen](#), um diese Malware zu entfernen.

## Mirai: Nutzung der Macht des Internet of Things, um weitreichende Störungen zu verursachen

In unserer Forschung folgte Mirai eng auf die FluBot-Malware – mit 156 Millionen identifizierten DNS-Abfragen. Mirai ist bekannt dafür, dass es auf IoT-Geräte mit offenen Telnet-Ports abzielt, und wurde durch den [DDoS-Angriff](#) auf einen der größten DNS-Anbieter berühmt. Dieser sich selbst verbreitende Wurm sucht nach anfälligen Geräten, die die Standardkombinationen aus Nutzernamen und Passwörtern verwenden. Zu einem bestimmten Zeitpunkt sammelten die Angreifer mehr als [100.000 Zombie-Geräte](#) an, die sie bei DDoS-Angriffen auf hochkarätige Ziele nutzten. Bei einem der früheren Angriffe [nutzte Mirai 145.000 Geräte](#) für einen Angriff auf ein Technologieunternehmen aus. Das ist ein Beispiel dafür, wie unsichere Geräte zu Cyberangriffen und weitreichenden Unterbrechungen für Unternehmen führen können.

Im Jahr 2016 [veröffentlichte die Gruppe hinter Mirai ihren Quellcode](#), möglicherweise um zu verhindern, dass Strafverfolgungsbehörden ihn bis zu den ursprünglichen Autoren zurückverfolgen, und damit einer Verhaftung zu entgehen. Doch nun begannen andere Gruppen, den Code von Mirai zu verwenden und ihn [mit weiteren Funktionen zu modifizieren und zu erweitern](#), z. B. um Systeme infizieren zu können. Eine der Auswirkungen der Codeveröffentlichung ist, dass wir neue Varianten gefunden haben, wie Okiru, Satori, Masuta und PureMasuta – allesamt ebenfalls mit dem Ziel, DDoS-Angriffe zu starten. Obwohl ein Neustart des infizierten Geräts hilfreich ist, da die Malware ständig nach Geräten sucht, besteht eine hohe Wahrscheinlichkeit, erneut infiziert zu werden, wenn Nutzer nicht ihr Passwort ändern.

## Necurs: Malware-Distributor und Zugriffsverkäufer

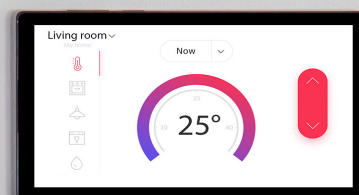
Das Botnet von Necurs, das 2012 erstmals entdeckt wurde, machte in den letzten sechs Monaten 80 Millionen der als schädlich identifizierten Anfragen aus. Es stellt ein ernstes Risiko für Privatnutzer und Unternehmen dar, da es [andere Malware-Payloads](#) wie Dridex, TrickBot und Locky bereitstellen kann. Ein bemerkenswerter Faktor ist, dass dieses Botnet im Rahmen seiner „Botnet for Hire“-Angebote (Botnet zu vermieten) auch [Zugriff auf infizierte Computer an andere Gruppen verkauft](#). Wie die meisten Botnets verwendet auch dieses einen DGA, um mehrere Domains für seine C2-Server durchlaufen und den Betrieb trotz blockierter Domains fortsetzen zu können.

Neben der Verteilung von Ransomware und Banking-Trojanern wird Necurs auch zur Verbreitung verschiedener Spam-Angriffe verwendet, wie russischer Dating-Betrug, pharmazeutischer Betrug usw. Während einer Untersuchung überwachte Microsoft die Aktivitäten dieses Botnets und stellte fest, dass es innerhalb von nur 58 Tagen rund 3,8 Millionen Spam-E-Mails verschickt hatte. Im Jahr 2020 [wurde der Betrieb des Necurs-Botnets unterbrochen](#), und zwar durch die Zusammenarbeit von Strafverfolgungsbehörden und der Sicherheitscommunity.

## Monerodownloader: Mining-Botnet

Eine der vielen Möglichkeiten, mit denen Angreifer Profit erzielen, besteht darin, kompromittierte Computer für Cryptomining auszunutzen. Die zunehmende Beliebtheit der Kryptowährung Monero bei Cyberkriminellen ist ein Grund dafür, dass Botnets speziell für das Mining dieser Währung entwickelt werden. Angreifer bevorzugen diese Kryptowährung, da die Blockchain nicht so offen ist und daher mehr Anonymität bietet. So lässt sich die Währung nicht zu ihnen zurückverfolgen. Zwar ist über den Monerodownloader wenig bekannt, doch eine seiner Taktiken besteht darin, Informationen zu sammeln und Verbindungen zu C2-Servern herzustellen, um die eigentliche Payload herunterzuladen.

Wenn Systeme nicht gepatcht werden, ebnet dies den Weg für Bedrohungen wie Monero-Cryptominer. Andere ähnliche Monero-Coinminer nutzen Schwachstellen aus, geben sich als kostenlose Software aus, um Nutzer zum Herunterladen des Miners zu bewegen, und können sich lateral durch das Netzwerk bewegen und andere Geräte infizieren, um so viel Umsatz wie möglich zu erzielen. Zwar betrifft diese laterale Netzwerkbewegung eher Unternehmen als Privatnutzer, doch wir erhalten hierdurch einen Einblick, wie Cryptominer die Infektion maximieren.



## Größte Bedrohungen pro Region: Botnets dominieren nach wie vor in Heimnetzwerken

Schauen wir uns unsere regionalen Daten genauer an, um anhand des DNS-Traffics von Heimnetzwerken herauszufinden, welche spezifischen Botnets in den einzelnen Regionen dominieren, und um einige mögliche Faktoren zu untersuchen, die zu einem solchen Trend beitragen.

### Nordamerika

#### Anzahl der Abfragen pro Top-C2-Bedrohung in Nordamerika

Juli 2022 bis Januar 2023

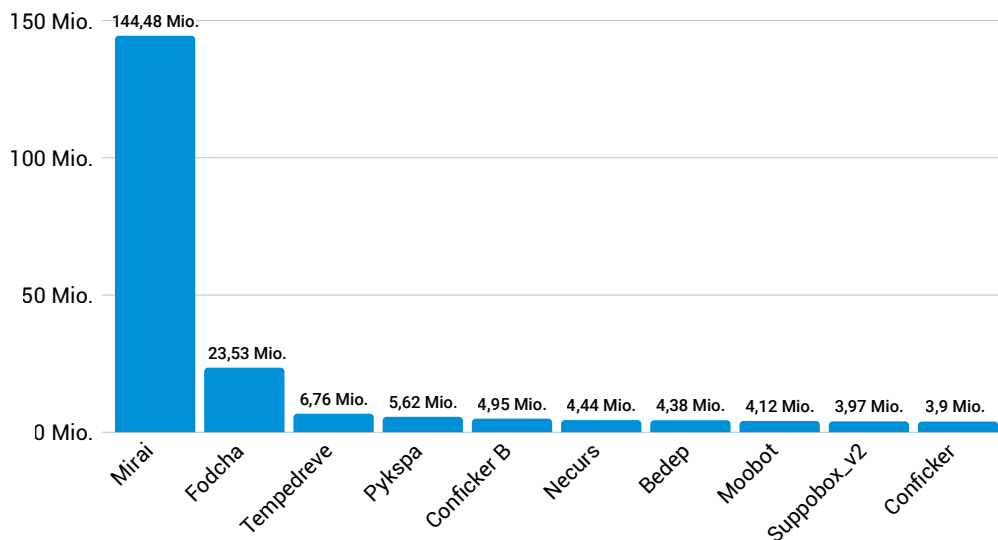


Abb. 15: Mirai schlägt in Nordamerika weiterhin Wellen, möglicherweise aufgrund unsicherer IoT-Geräte.

In Nordamerika wurden mehr als 144 Millionen Abfragen im Zusammenhang mit dem Mirai-Botnet in Heimnetzwerken verzeichnet (Abbildung 15). Dieses Botnet zielt auf anfällige IoT-Geräte ab, die weiterhin Standard-Nutzernamen und -Passwörter verwenden. Die hohe Anzahl von Anfragen in dieser Region könnte auf die Beliebtheit oder hohe Nutzung von IoT-Geräten in entsprechenden Haushalten zurückzuführen sein. Allein im Jahr 2022 verfügen US-Haushalte [Berichten zufolge](#) über durchschnittlich 22 vernetzte Geräte, was gegenüber 25 im Vorjahr einen leichten Rückgang darstellte. Und da IoT-Verbindungen in Nordamerika [voraussichtlich zunehmen werden](#) (5,4 Milliarden Dollar bis 2025), besteht eine hohe Wahrscheinlichkeit, dass weitere Bedrohungen wie Mirai oder ähnliche Varianten unsichere IoT-Geräte ausnutzen.

Für Privatnutzer bedeutet eine solche Bedrohung, dass Cyberkriminelle ihre Geräte ohne ihr Wissen ausnutzen können, um Verbrechen zu begehen. Aber auch Unternehmen leiden unter den Auswirkungen von DDoS-Angriffen oder auch von schädlichen Spam-Kampagnen, die von Botnets wie Mirai gestartet werden. Als Best Practice empfiehlt es sich, den Standard-Nutzernamen und das -Passwort Ihrer Geräte zu ändern, um sie vor Mirai und anderen ähnlichen Angriffen zu schützen.

## Europa, Naher Osten und Afrika

Anzahl der Abfragen pro Top-C2-Bedrohung in EMEA  
Juli 2022 bis Januar 2023

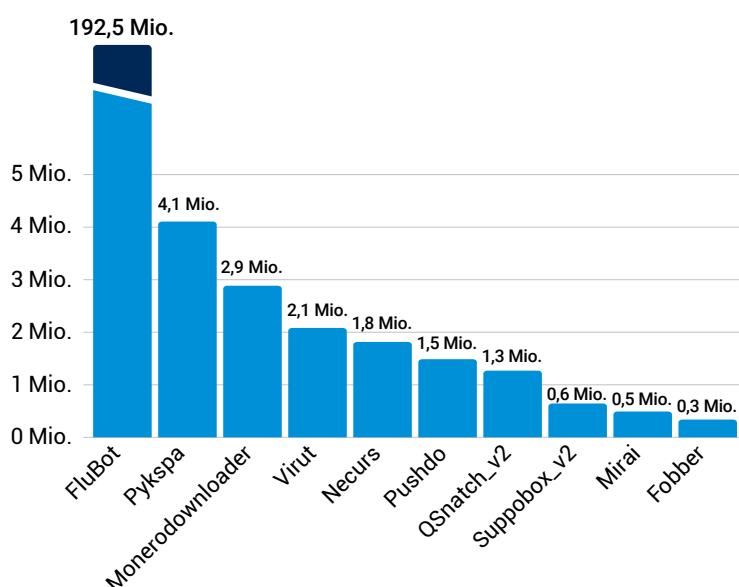


Abb. 16: Wir haben einen Ausbruch von FluBot-Malware in der EMEA-Region beobachtet, möglicherweise aufgrund ihrer Verbreitungstaktik und der Verwendung mehrerer europäischer Sprachen als Teil des Social-Engineering-Köders.

Zu behaupten, dass sich FluBot-Malware in EMEA wie ein Lauffeuer ausbreitet, wäre eine Untertreibung. Bemerkenswert ist das enorme Volumen der DNS-Abfragen, die in dieser Region beobachtet wurden (ca. 193 Millionen). Durch die Untersuchung des DNS-Traffics konnte Akamai diese Infektionen in EMEA beobachten (Abbildung 16). Ein Faktor, der dazu beiträgt, ist die Verbreitungstaktik des Smishings – eine Form von Phishing, bei der der Angreifer SMS-Nachrichten an die Kontaktliste des Opfers sendet. Darüber hinaus werden Nutzer dazu verleitet, eine App herunterzuladen – angeblich in Bezug auf eine Paketzustellung oder eine Voicemail –, bei der es sich jedoch tatsächlich um Malware handelt. Darüber hinaus fordert FluBot zusätzliche Berechtigungen an und protokolliert heimlich die Banking-/Finanzdaten der Nutzer. Die Malware zielt [Berichten zufolge](#) unter anderem auf Nutzer in Deutschland, Finnland, Spanien und dem Vereinigten Königreich ab. Die SMS wird auch in mehreren anderen EU-Sprachen geschrieben, wie Deutsch und Ungarisch, was einer der vielen Faktoren sein könnte, die diese Malware in Europa in die Höhe getrieben hat.



## Lateinamerika

### Anzahl der Abfragen pro Top-C2-Bedrohung in LATAM

Juli 2022 bis Januar 2023

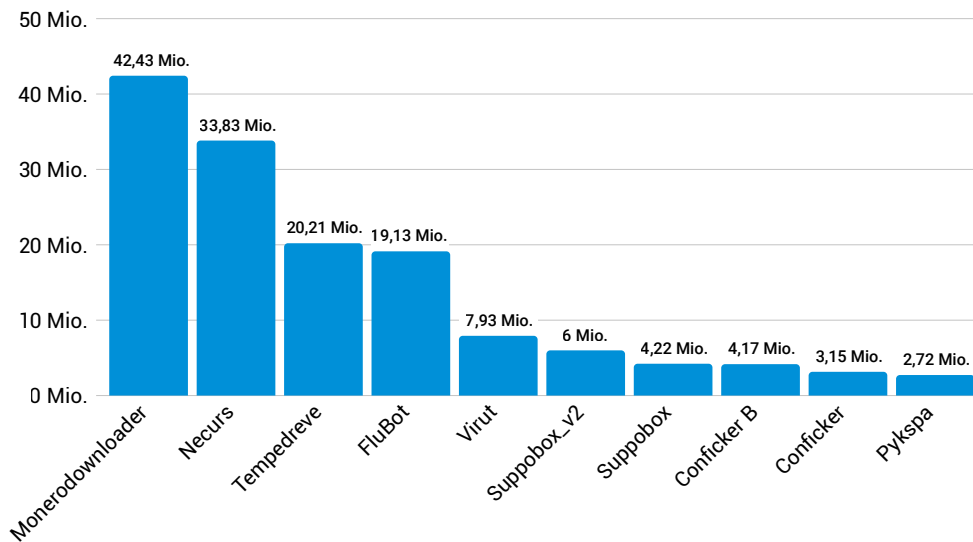


Abb. 17: Das Cryptomining-Botnet „Monerodownloader“ wurde zur größten Bedrohung in Lateinamerika, möglicherweise aufgrund der starken Nutzung von Kryptowährungen in der Region.

Im Gegensatz zu Nordamerika und EMEA weist die Region LATAM eine vielfältigere Verteilung von Botnets auf (Abbildung 17). Monerodownloader, ein Cryptomining-Botnet, führt die Liste der aktiven Botnet-Gruppen mit 42 Millionen identifizierten Abfragen an, gefolgt von Necurs (34 Millionen) und Tempedreva (20 Millionen). Die starke [Verbreitung von Kryptowährungen](#) in der Region – angetrieben durch hohe Inflation und Geldsendungen – könnte erklären, warum Botnets wie Monerodownloader an der Spitze der Liste standen. Ohne das Wissen des Nutzers könnten Cyberkriminelle die Ressourcen der Nutzergeräte für Mining-Zwecke und für ihren eigenen finanziellen Gewinn ausnutzen. An dieser Stelle möchten wir darauf hinweisen, dass FluBot eine der größten Bedrohungen im DNS-Traffic ist, was die Verbreitung des Botnets auch außerhalb der EMEA-Region zeigt: Auch hier war ein hohes Trafficvolumen zu verzeichnen.



## Asiatisch-pazifischer Raum und Japan

Anzahl der Abfragen pro Top-C2-Bedrohung in APJ  
Juli 2022 bis Januar 2023

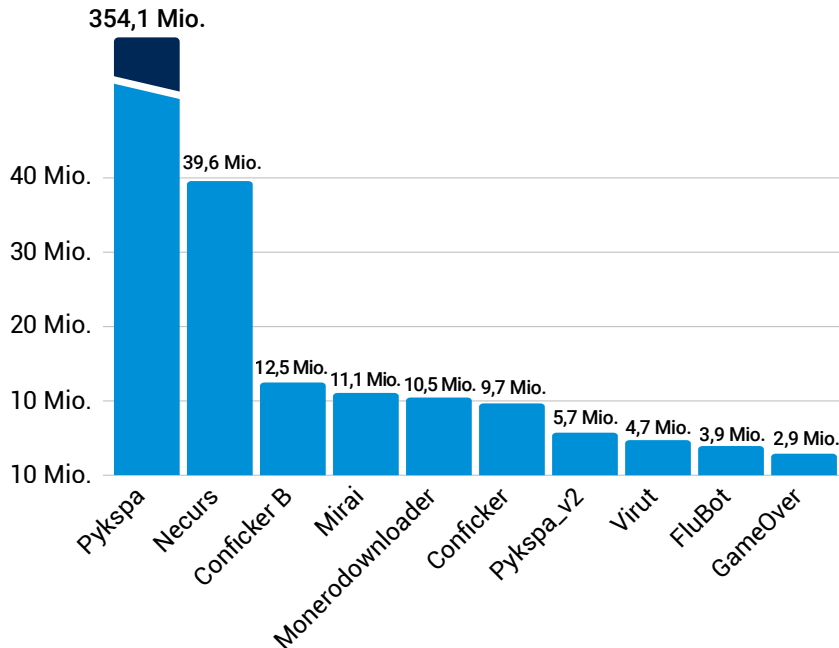


Abb. 18: Zu den vorherrschenden Bedrohungen in APJ gehören Pykspa und Necurs.

In APJ wurden mehr als 350 Millionen Anfragen im Zusammenhang mit Pykspa beobachtet (Abbildung 18). In einem [Blogbeitrag](#) von 2019 stellten wir fest, dass Pykspa einen selektiven DGA-Mechanismus einsetzte, um über einen langen Zeitraum unter dem Radar zu bleiben. Die in diesem Bericht hervorgehobenen Domains wurden größtenteils in Ostasien gefunden. Wir beobachteten auch Abfragen im Zusammenhang mit Botnets wie Necurs, einem starken Indikator dafür, dass Systeme mit anderer Malware infiziert sind.



## Überblick über die Phishing-Landschaft

Im letzten Teil unserer DNS-Trafficanalyse haben wir Phishing-Kits und ihre entscheidende Rolle für den Erfolg von Phishing-Kampagnen untersucht. Phishing ist immer noch relevant – mehr denn je – und zwar aufgrund der sich ständig weiterentwickelnden Taktiken von Gegnern und der zunehmenden Menge an persönlichen Informationen, die online verfügbar sind. Angreifer nutzen Social Engineering, um ihre Phishing-Versuche legitim erscheinen zu lassen, und es gibt Hinweise darauf, dass die Erfolgsrate dieser Angriffe weiterhin hoch ist. Die Forschungen von Akamai zu [urlaubsbezogenem Phishing-Betrug](#) haben gezeigt, dass Angreifer neue Techniken und Taktiken einsetzen, um weiterhin unter dem Radar zu bleiben. Zu diesen neuen Taktiken gehören der Einsatz gefälschter Nutzerrezensionen als Teil des Betrugs sowie die neu entdeckte Technik, mithilfe von HTML-Ankern sicherzustellen, dass nur gültige Nutzer auf betrügerischen Websites landen.

Die Zunahme der Remotearbeit aufgrund der Coronapandemie hat die Erkennung und Verhinderung von Phishing-Angriffen zusätzlich erschwert. Deshalb ist es für Einzelpersonen und Organisationen wichtiger denn je, wachsam zu bleiben und Maßnahmen zu ergreifen, um sich selbst zu schützen. Darüber hinaus haben der Aufstieg der sozialen Medien und die zunehmende Zahl internetverbundener Geräte mehr Chancen für Angreifer geschaffen.

### Phishing-Kampagnen treffen Finanzdienstleister

Bei der Untersuchung, welche Marken durch Phishing-Betrug ausgenutzt und nachgeahmt werden, gibt es verschiedene Möglichkeiten zur Datenerfassung. Wir haben die Gesamtzahl der Kampagnen mit der Anzahl der Opfer verglichen. So können wir die Erfolgsrate einer bestimmten Kampagne bewerten und sehen, welche Rate in den einzelnen Branchen anvisiert wird.

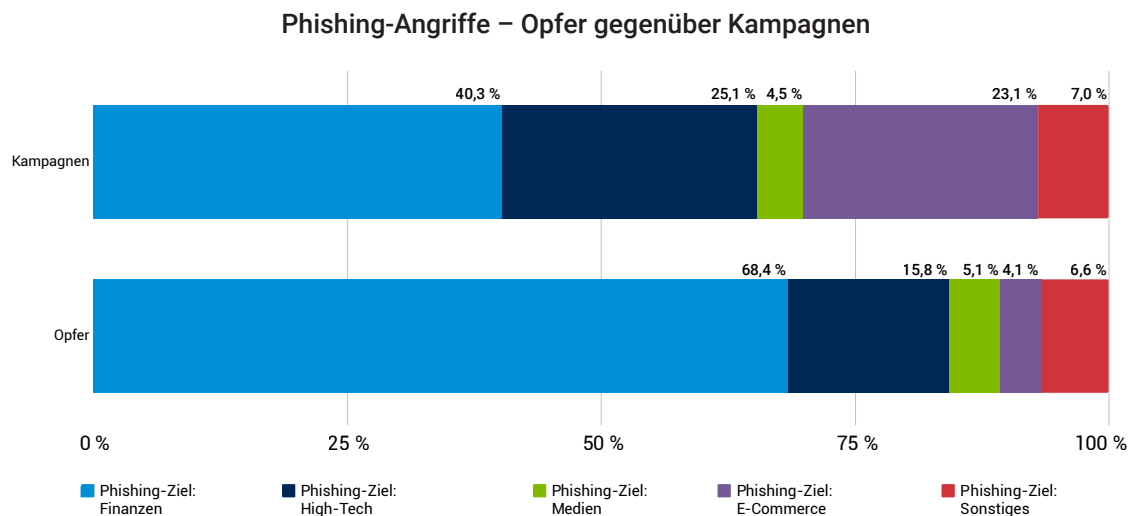


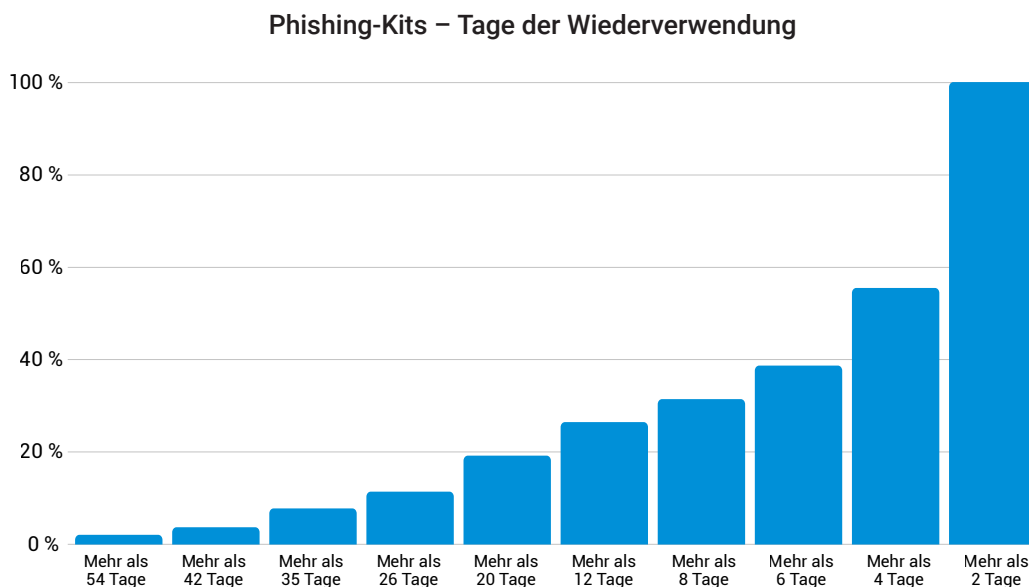
Abb. 19: Die meisten Phishing-Kampagnen zielten auf die Finanzdienstleistungsbranche ab (Q4 2022).

Unsere Untersuchungen haben ergeben, dass Finanz- und Hightech-Marken sowohl bei der Anzahl der Kampagnen als auch bei der Zahl der Opfer führend waren (Abbildung 19). Außerdem richteten sich 40,3 % der Kampagnen gegen Kunden im Finanzdienstleistungssektor, was 68,4 % der Opfer ausmachte. Das deutet darauf hin, dass Angriffe im Finanzdienstleistungssektor in Q4 2022 sehr effektiv waren. In unserem Bericht zu Finanzdienstleistungen, [Der Feind vor den Toren: Analyse von Angriffen auf die Finanzdienstleistungsbranche](#) haben wir unterstrichen, dass Phishing-Angriffe finanziell motiviert sind und hauptsächlich auf Finanzdienstleister und ihre Kunden abzielen. Zu den möglichen Auswirkungen solcher Angriffe gehören die Schädigung der Marke und des Rufs sowie der Verlust des Kundenvertrauens. Phishing kann das jeweilige Unternehmen außerdem Ressourcen kosten, um das Problem zu beheben.

Im Q4 2022 richteten sich 23 % der Phishing-Kampagnen auf die E-Commerce-Branche. Obwohl wir mehr Kampagnen verzeichnet haben als tatsächliche Opfer, ist es wichtig, darauf hinzuweisen, dass Angreifer diese Branche angreifen und Nutzer wachsam bleiben müssen, da Cyberkriminelle möglicherweise ihre persönlichen Informationen oder Banking-Daten stehlen wollen.

### Phishing-Toolkits: Auslöser für Phishing-Betrug

Das überwältigende Ausmaß und die Tragweite der Phishing-Landschaft wird erst durch die Existenz von Phishing-Toolkits ermöglicht. Phishing-Toolkits unterstützen die Bereitstellung und Verwaltung von Phishing-Websites und ermöglichen es selbst technisch unerfahrenen Betrügern, Teil der Phishing-Bedrohungslandschaft zu werden und Phishing-Betrug auszuführen.



*Abb. 20: Phishing-Toolkits nach Anzahl der Tage, an denen sie wiederverwendet wurden (Q4 2022)*

Unseren Untersuchungen zufolge, bei denen mehr als 300 verschiedene Phishing-Toolkits verfolgt wurden, die in freier Wildbahn für neue Angriffskampagnen verwendet werden, wurden 2,04 % der erfassten Kits in Q4 2022 an mindestens 54 verschiedenen Tagen wiederverwendet (Abbildung 20). Darüber hinaus wurden 55,5 % der Kits an mindestens fünf Tagen wiederverwendet, um eine neue Angriffskampagne zu starten, und 100 % der nachverfolgten Kits wurden in Q4 2022 an mindestens drei Tagen wiederverwendet.

## Fazit und Empfehlungen: Moderne Angriffe mit proaktiven Maßnahmen bekämpfen

---

Nachdem wir uns nun mit Bedrohungsgruppen und Angriffsmethoden befasst haben, wollen wir darüber sprechen, wie wir all diese Informationen nutzen können. Wir beginnen mit der Verwaltung des DNS – intern oder an Dritte ausgelagert. Für größere oder komplexere Unternehmen ist es sinnvoll, einen Anbieter einzusetzen, der sich auf die Verwaltung von DNS spezialisiert hat. Stellen Sie in jedem Fall sicher, dass Sie die Performance und den Schutz Ihres DNS überwachen. Betrachten Sie als Nächstes die verschiedenen Kontrollen, die Sie benötigen. DDoS, Malware-Angriffe und Scraping, laterale Netzwerkbewegung und Exfiltration sind die wichtigsten Bereiche, vor denen Sie sich schützen müssen. Die Verfolgung dieser Datenreise und die Suche nach allen kritischen Schwachstellen, die Sie bei jedem Schritt beheben können, ist ein Cybersicherheitsmodell, das oft als „Cyber Kill Chain“ bezeichnet wird.

Erwägen Sie die Erstellung von Playbooks für die Angriffstechniken, die in diesem Bericht behandelt werden. Erkundigen Sie sich bei Ihrem Pentest- oder Red Team, ob es dieselben Tools und Techniken verwendet wie IABs wie Qakbot und Emotet, Bots wie QSnatch, Ransomware wie LockBit (in der Laborumgebung) und Tools wie Cobalt Strike. Es ist wichtig, dass Ihre Sicherheitskontrollen effektiv vor dieser Art von Angriffen warnen, sie effektiv aufhalten und dass Ihre Teams entsprechend geschult sind.

Wenn Cobalt Strike in Ihrem Netzwerk erkannt wird, ist es ratsam, sofort einen Vorfallbericht zu erstellen und ihn zu untersuchen. Obwohl das Tool von Ihrem Red Team eingesetzt werden könnte (in diesem Fall sollte es dennoch untersucht und gemeldet werden), sollte das Vorhandensein eines solchen Traffics den Alarm auslösen, da dies auf einen Angriff durch andere RaaS-Angreifergruppen oder -Akteure hinweisen und einen fortlaufenden Angriff signalisieren könnte, der vielleicht noch abgewehrt werden kann.

Denken Sie darüber nach, wie Ihr Security Operations Center funktioniert, und bestimmen Sie, wie Sie Prozesse (wie Bits, Wget oder cURL) verfolgen, die möglicherweise darauf hindeuten könnten, dass derzeit eine IAB-bezogene Bedrohung Aufklärung in Ihrem Netzwerk betreibt. Am wichtigsten ist es, herauszufinden, was heruntergeladen wurde, und den Vorgang zu stoppen, wenn er noch läuft. Untersuchen Sie dann, was der IAB ausgelöst hat: War es eine LNK-Datei, ein Makro oder ein VScript? Untersuchen Sie dann von dort aus, wie der Angriff begonnen hat.

Bleiben Sie auf dem Laufenden über unsere neuesten Forschungsergebnisse, indem Sie unseren [Security Research Hub](#) besuchen.

# Methodik

---

## Command-and-Control-Angriffstraffic

Die Daten in diesem Bericht werden von unserem SIA-Produkt (Secure Internet Access) generiert und beschreiben den C2-Angriffstraffic (Command and Control). SIA ist ein cloudbasiertes Secure Web Gateway, mit dem Nutzer ihre Geräte einfach und sicher mit dem Internet verbinden können. Die beiden unterschiedlichen Datensätze, die in diesem Bericht verwendet werden, spiegeln getrennt die Sicherheitswarnungen von Unternehmen (mit einer großen Anzahl von Nutzern) und Internetanbietern (mit einzelnen Privatanutzern) wider. Diese Daten wurden anhand der Anzahl betroffener Geräte bzw. der Anzahl von Abfragen gemessen. Ein „betroffenes Gerät“ wurde als Gerät definiert, das mindestens einmal eine Verbindung zu einer bekannten und identifizierten C2-Domain hergestellt hat. Auf ähnliche Weise wurde eine „C2-Abfrage“ als eine Abfrage definiert, die eine bekannte und identifizierte C2-Domain erreicht hat. Unsere Sicherheitsteams verwenden diese Daten intern, um Angriffe zu untersuchen, schädliches Verhalten zu kennzeichnen, Kunden zu benachrichtigen und zusätzliche Informationen in die Sicherheitslösungen von Akamai einzuspeisen.

## Mitwirkende

### Redaktion und Text

Or Katz

Eliad Kimhy

Badette Tribbey

### Prüfung und Fachleute

Tanya Belousov

Stiv Kupchik

Shiran Guez

Grace Wang

Ophir Harpaz

Steve Winterfeld

### Datenanalyse

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

### Marketing und Veröffentlichung

Georgina Morales Hampe

Shivangi Sahu



Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Akamai Connected Cloud, eine stark verteilte Edge- und Cloud-Plattform, bringt Anwendungen und Erlebnisse näher an die Nutzer und hält Bedrohungen fern. Möchten Sie mehr über die Cloud-Computing-, Sicherheits-, und Inhaltsbereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter [akamai.com](https://akamai.com) und [akamai.com/blog](https://akamai.com/blog) oder folgen Sie Akamai Technologies auf [Twitter](https://twitter.com/Akamai) und [LinkedIn](https://www.linkedin.com/company/akamai). Veröffentlicht: 03/23

## Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai.

[akamai.com/soti](https://akamai.com/soti)

## Weitere Informationen zur Bedrohungsforschung bei Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden.

[akamai.com/security-research](https://akamai.com/security-research)

## Greifen Sie auf Daten aus diesem Bericht zu

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, auf die in diesem Bericht verwiesen wird. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten.

[akamai.com/sotidata](https://akamai.com/sotidata)

## Weitere Informationen zu Akamai-Lösungen

Weitere Informationen über Akamai-Lösungen zum Schutz vor Bedrohungen, die auf Unternehmen abzielen, finden Sie auf unserer Seite zu [Secure Internet Access Enterprise](#). Serviceanbieter, die auf Verbraucher- und KMU-Märkte abzielen, können die Seite zu [Secure Internet Access Services für Internetanbieter](#) besuchen.