ZAHLEN UND FAKTEN

# SECURITY REPORT 2018/19




AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

# Der AV-TEST Sicherheitsreport

Mit der Erfassung des neunhundertmillionsten Malware-Samples durchbrach die Entwicklung von Schadprogrammen Mitte Mai 2019 eine Schallmauer. Bei Abschluss des Jahres 2018 lag die Anzahl der durch die Analysesysteme von AV-TEST erfassten Schadprogramme noch bei 856,62 Millionen. Damit kehrt sich der seit 2015 feststellbare Trend rückläufiger Malware-Entwicklung in 2018 um, wie bereits in der Analyse des letzten Sicherheitsreports prognostiziert.

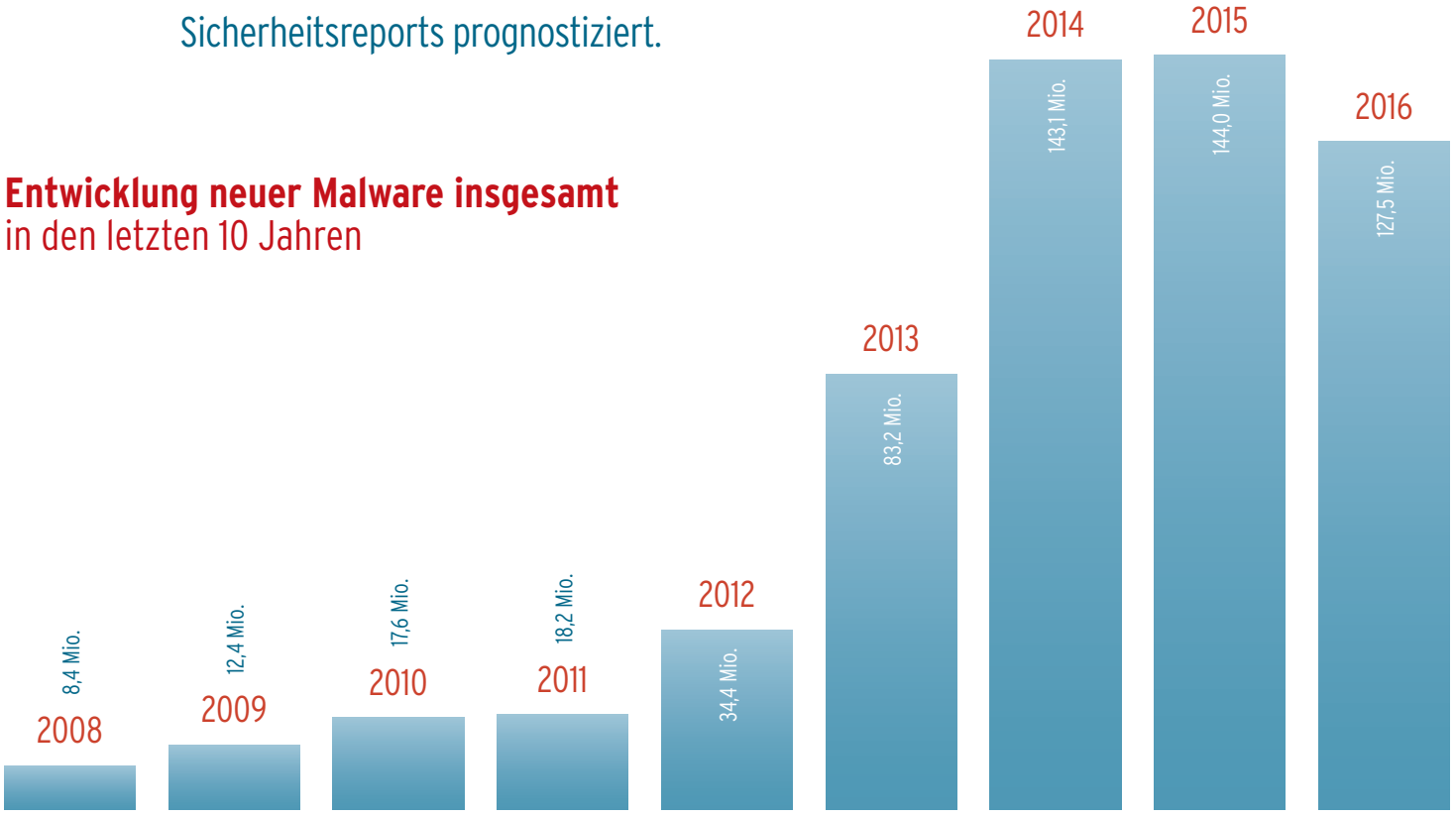
## Mehr Angriffe auf macOS und IoT

Während Windows-Systeme weiterhin im Fokus industriell organisierter Krimineller stehen, verdreifachte sich die Anzahl von Schadprogrammen für Apples Betriebssystem macOS nahezu. Abseits der massenhaften Malware-Verbreitung zeichnen sich bei Analyse der Zahlen des vergangenen Jahres sowie des ersten Quartals 2019 weitere besorgniserregende Trends ab. So bietet etwa die Digitalisierung industrieller Operational Technology (OT)- und IoT-Anlagen ohne ausreichenden Schutz stark wachsendes Potential für gezielte Angriffe und eine weit offene Flanke, wie der vorliegende Sicherheitsreport ab Seite 19 aufzeigt.

## Steigende Malware-Rate und Höchststand an Sicherheitslücken

Mit der Zunahme der Malware-Neuentwicklungen 2018 steigerte sich die quantitative Bedrohungslage: Mussten Schutzprogramme 2017 im Durchschnitt noch 3,9 Schadprogramme pro Sekunde abwehren, waren es 2018 bereits 4,4 pro Sekunde und damit 376.639 neue Schädlinge pro Tag!

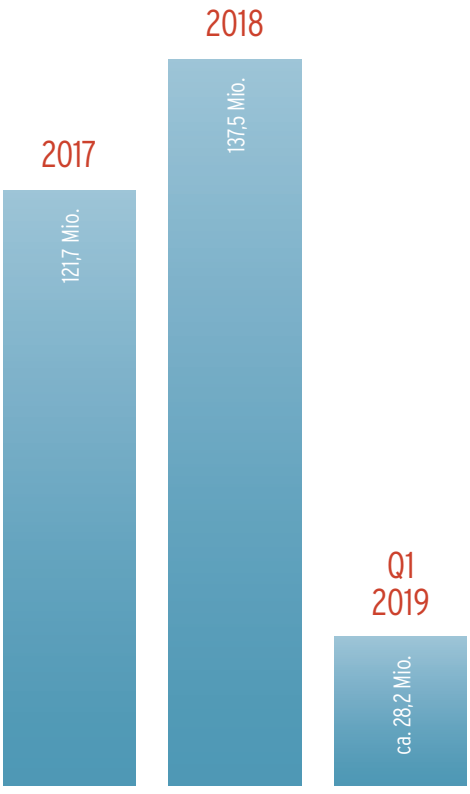
**Entwicklung neuer Malware insgesamt**
in den letzten 10 Jahren



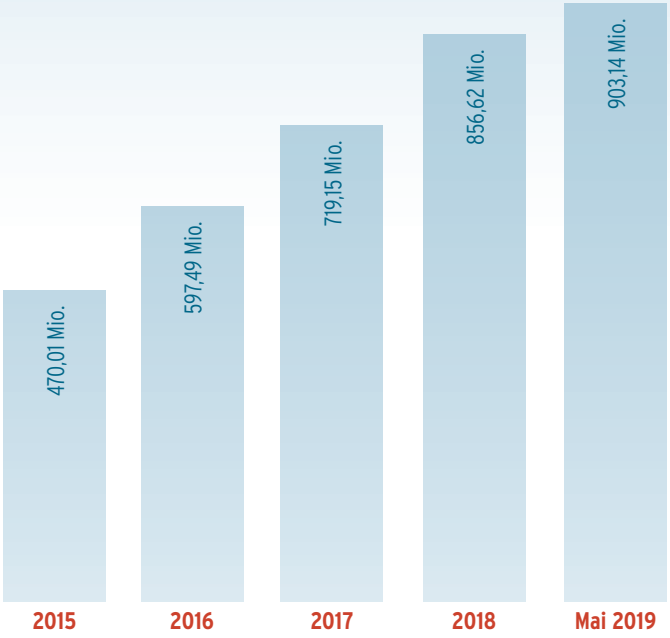
## Der Hardware-Super-GAU: Meltdown und Spectre

Zu den gravierendsten Sicherheitslecks dürften die gleich Anfang Januar veröffentlichten Hardware-Lecks „Meltdown" (CVE-2017-5754) und „Spectre" (CVE-2017-5715 ff) zählen, die die Sicherheitsarchitektur von Mikroprozessoren auf Hardware-Ebene aushebelten. So war es Angreifern möglich, sensible Speicherinhalte auszulesen, und damit etwa an Passwörter und andere brisante Inhalte aus eigentlich nicht zugänglichen Speicherbereichen von Programmen und Betriebssystemen zu gelangen. Betroffen waren alle Geräte, die CPUs der Hersteller Intel, ARM und AMD verbaut hatten – also nahezu alle PCs, Server und Smartphones, vernetzte Endanwenderprodukte bis hin zu Industrieanlagen.

Kurz nach Veröffentlichung beider Hardware-Lecks Anfang Januar stellten die Analysesysteme des AV-TEST Instituts einen starken Anstieg möglichen Schadcodes für die Lücken fest. Diese Malware-Samples basierten auf dem bekannten Proof-of-Concept-Code und zielten hauptsächlich auf Windows, macOS und Linux ab. Meist handelte es sich allerdings um Test-Samples, die Hersteller betroffener Produkte und Anbieter von Sicherheitslösungen zur Überprüfung der Produktsicherheit beziehungsweise zum Patchen ihrer Systeme einsetzten.




## Malware insgesamt
2015 bis Mai 2019



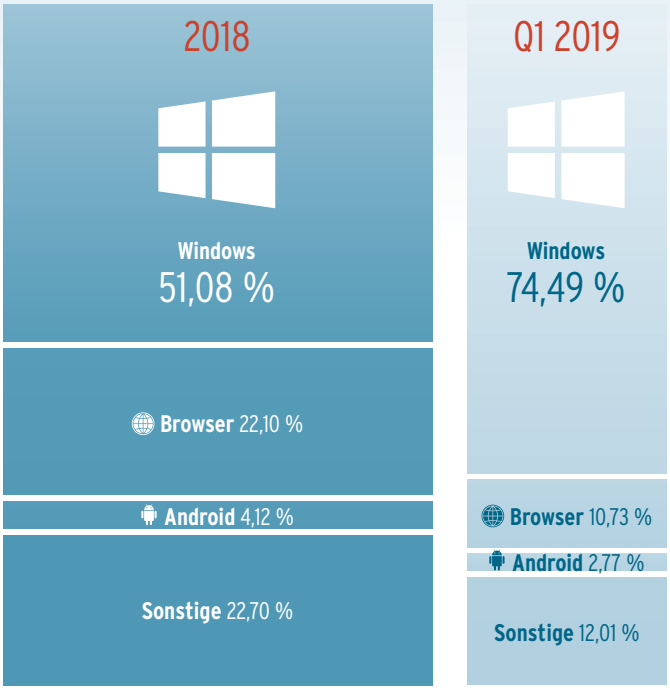

Da Chip- und Geräte- als auch Software-Hersteller bereits im Juni 2017 bei Entdeckung der Lücken informiert wurden, standen zumindest von namenhaften Herstellern bereits Richtung Februar 2018 entsprechend umfangreiche Patch-Bibliotheken zur Verfügung. Das galt allerdings nach wie vor nicht für alle angreifbaren Geräte. Und da die Verfügbarkeit von Sicherheitsupdates nicht automatisch bedeutet, dass diese auch installiert werden, dürften sich die Meltdown- und Spectre-Lücken weiterhin von einer großen Anzahl von Systemen zur Verbreitung von Schadcode nutzen lassen.

Zu den gravierenden Hardware-Lücken gesellte sich in 2018 „Foreshadow" (CVE-2018-3620 ff), die ebenfalls Prozessoren von Intel und AMD betraf und das Einschleusen von Schadcode ermöglichte. Und auch 2019 werden mögliche Attacken auf Hardware-Lücken wie „ZombieLoad" (CVE-2018-12130) Hersteller, Kriminelle und Sicherheitsexperten weiter in Atem halten.

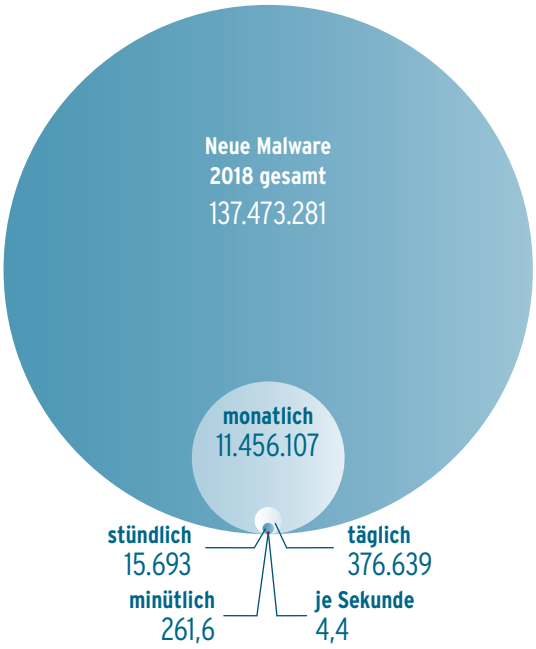
## Windows weiterhin Hauptangriffsziel

Im Vergleich zum Vorjahr konzentrierte sich die konventionelle Malware-Industrie weiterhin auf Windows-Systeme. Über die Hälfte (51,08 Prozent) aller neu entwickelten Schadprogramme zielten 2018 auf das weltweit meist genutzte Betriebssystem aus Redmond. Aufgrund der ständig steigenden Abwehrleistung von Schutzprogrammen, sowohl für Privatnutzer als auch im Unternehmensbereich, sahen sich Cyberkriminelle offensichtlich gezwungen, auch die Schlagzahl neuer Schadcodes zu erhöhen. Die in den regelmäßigen Tests des AV-TEST Instituts nachgewiesene, deutlich verbesserte Erkennungsleistung des Windows-eigenen Sicherheitsmoduls Microsoft Defender trug ebenfalls zu dieser Entwicklung bei. Aus der Notwendigkeit heraus, mit Windows-Malware weiterhin wirtschaftlich erfolgreich zu sein, musste die Malware-Industrie ihre Produkte notgedrungen ständig optimieren – ein weiterer Anhaltspunkt zur Erklärung der steigenden Malware-Rate. Detaillierte Auswertungen zu Windows-Malware enthält dieser Report ab Seite 6.

## Malware-Erkennung nach Plattform




## Durchschnittliche Bedrohungslage durch neue Malware 2018



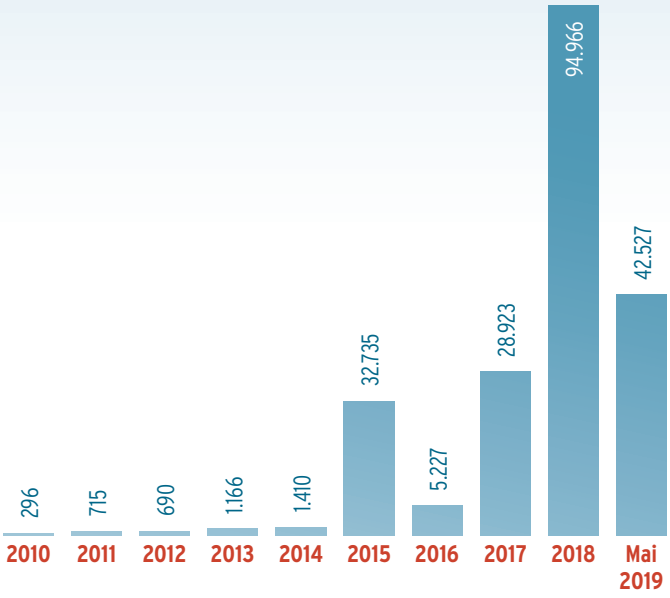

## AV-TEST optimiert Malware-Auswertung

Im Verhältnis zur Malware-Auswertung in bisherigen Sicherheitsreports erfasst das AV-TEST Institut die Verteilung von Malware auf unterschiedliche Plattformen und Betriebssysteme jetzt noch dezidierter, und das sogar rückwirkend. Aufgrund der exakteren Erfassung kommt es insbesondere bei den Malware-Zahlen für Windows-Systeme zu Abweichungen gegenüber vorherigen Sicherheitsreports. Das liegt etwa an der Erfassung von Browser-Malware, die bisher hauptsächlich den Windows-Systemen oder der Kategorie „Sonstige“ zugerechnet wurde.

Dezidierte Informationen zur sich leicht entspannenden Entwicklung der Malware-Situation für das weltweit meistgenutzte Betriebssystem für Mobilgeräte Android gibt dieser Report ab Seite 12.

## Malware-Entwicklung unter Android
2010 - Mai 2019


## Malware-Entwicklung unter macOS
2010 - Mai 2019




## macOS-Malware fast verdreifacht

Während die Rate der Malware-Neuentwicklungen für das größte Mobilbetriebssystem 2018 im Vergleich zum Vorjahr leicht abflaute, verdreifachte sich die Sample-Zahl neuer Malware für macOS nahezu. Prozentual erscheint der Anteil von Mac-Malware mit 0,15 Prozent der Gesamtsumme neu entwickelter Schadprogramme zwar verschwindend gering. Allerdings darf nicht vergessen werden, dass den insgesamt 94.966 im Jahr 2018 neu entwickelten Schädlingen massenhaft Apple-Geräte ohne ausreichenden Virenschutz gegenüberstehen. Denn genau wie bei Mobilgeräten unter Android gibt es auch hinsichtlich der Installationsrate wirkungsvoller Schutzprogramme bei Apple-Rechnern nach wie vor Luft nach oben. Genauere Informationen zur Malware-Situation für Apple-Geräte sind ab Seite 16 zu finden.

## Kriminelle Geschäftsmodelle: Crypto-Miner contra Ransomware

Neben dem klassischen Malware-Erfolgsmodell bestehend aus dem Diebstahl sensibler Daten sowie Abfangen und Missbrauch von Bank- und Kontoinformationen setzten Cyberkriminelle auf neue Geschäftsfelder: Erpressung durch Verschlüsseln relevanter Daten und Systeme der Opfer durch Ransomware sowie das Schürfen von Kryptowährung durch heimliches Ausnutzen fremder Rechenleistung und IT-Infrastruktur durch Crypto-Miner. Während die von AV-TEST erfasste Sample-Zahl von Ransomware rückläufig war, galt für Crypto-Miner im vergangenen Jahr das Gegenteil. Wie diese Zahlen genau aussehen und was daraus zu schließen ist, beleuchtet dieser Report ab Seite 24.

# Sicherheitsstatus WINDOWS

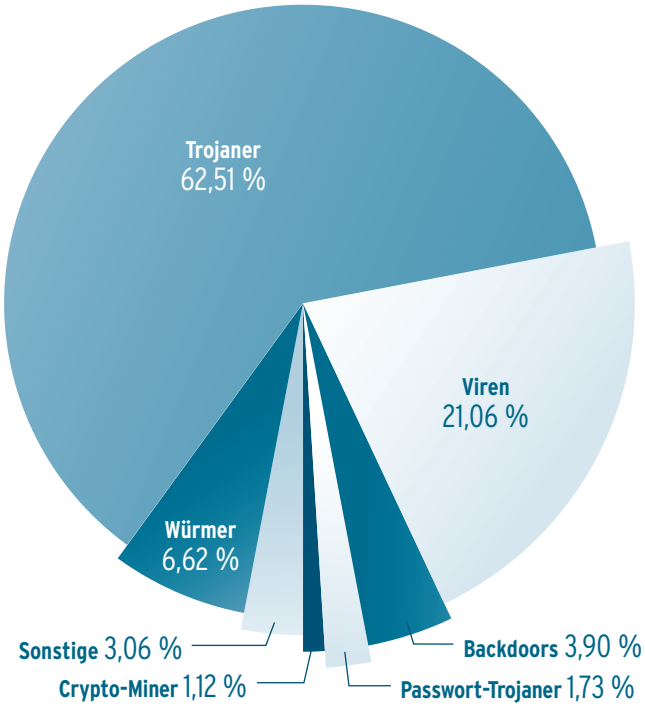
Monokulturen leiden oft unter verstärktem Schädlingsbefall. Und so verwundert es nicht, dass Windows als weltweit meistgenutztes Betriebssystem seit jeher mit Abstand die meisten Malware-Attacken auf sich zieht. Die Aussicht, mit Windows-Malware Kasse zu machen, ist aufgrund des hohen Verbreitungsgrades ungleich höher als bei Attacken auf andere Betriebssysteme. Und so zielten 2018 über die Hälfte aller Schadprogramme, exakt 51,08 Prozent, auf die Basis-Software der meisten Privat-PCs und Business-Rechner.

## Malware-Entwicklung insgesamt moderat

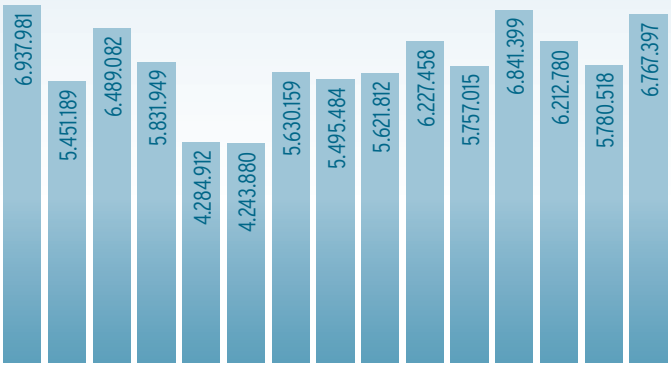
Gleich zu Beginn des Jahres, genau genommen im Januar, vermeldeten die Erfassungssysteme des AV-TEST Instituts den Höchststand neu entwickelter Windows-Malware für das Jahr 2018. Mit knapp sieben Millionen neuen Schadprogrammen allein in jenem Monat startete das letzte Jahr also alles andere als beruhigend für Nutzer von Windows-Systemen. Eine noch größere Malware-Flut, deutlich über 10 Millionen neuer Malware in einem Monat, verzeichneten die AV-TEST Systeme zuletzt im Juni 2015.

Doch die Entwicklung neuer Windows-Malware zeigte sich auch 2018 starken Schwankungen unterworfen. Und so ebbte die Neuentwicklungsrate neuer Windows-Schädlinge gegen Mitte des Jahres stark ab. In den Monaten Mai und Juni verringerten sich die Erfassungswerte drastisch auf nur noch knapp über vier Millionen neuer Samples pro Monat. Allerdings nur, um von da an wieder kontinuierlich anzusteigen.

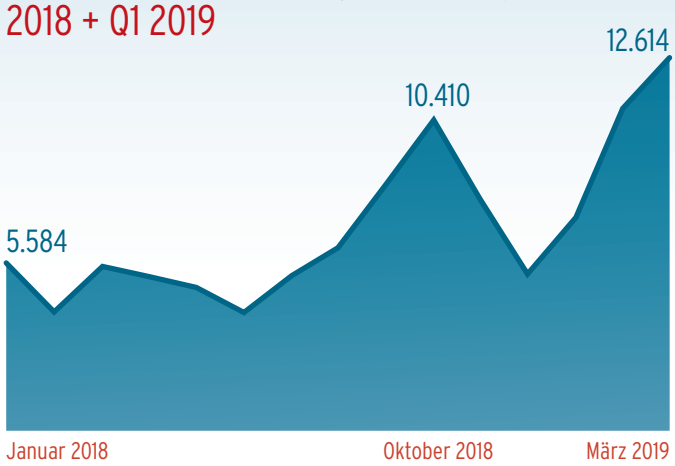
## Malware-Verteilung unter Windows 2018



## Windows: Entwicklung neuer Malware
2018 + Q1 2019




## Windows: Entwicklung neuer Exploits
2018 + Q1 2019




## Massive Zunahme ausnutzbarer Windows-Lücken

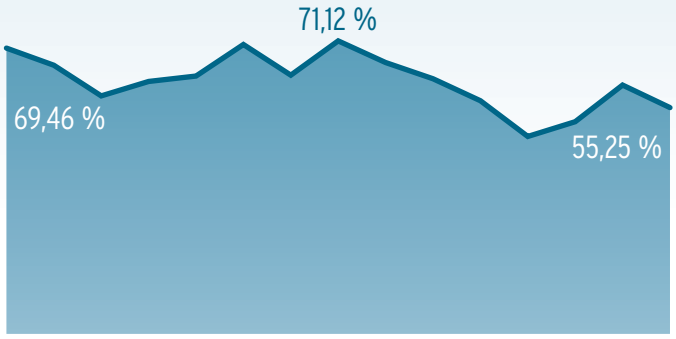
Setzt man die über 2018 zwar konstant, insgesamt aber doch moderat steigende Anzahl von Windows-Schädlingen in Relation zu den verfügbaren ausnutzbaren Schwachstellen in Windows-Programmen, ergibt sich ein anderes Bild. Denn gegenüber den Vorjahren stieg die Anzahl an Windows-Exploits sprunghaft an. Besonders von Mitte bis Ende des vergangenen Jahres verlief deren Steigerungsrate fast exponentiell. Im Oktober 2018 erreichte die Anzahl von Exploits für Windows-Systeme einen kritischen Höchstwert von 10.000 Samples pro Monat, fiel aber bis Jahresende wieder auf fast die Hälfte zurück. Hinsichtlich der massiven Zunahme ausnutzbarer Exploits wirkte der Entwicklungstrend neuer Malware über das gesamte Jahr 2018 daher insgesamt eher verhalten.

## Trojaner bleiben Bedrohung Nr. 1

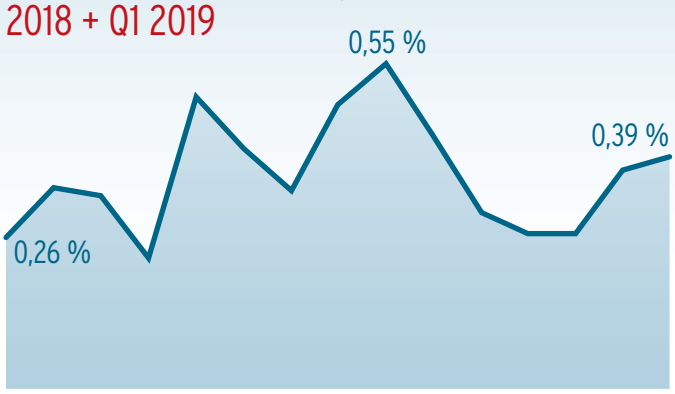
Als erstes Mittel der Wahl von Cyberkriminellen bewiesen sich auch 2018 mit großem Abstand vor allen anderen Schädlingsgattungen Trojaner. Kein Wunder, denn Trojaner sind sowohl an Funktionsvielfalt als auch an Möglichkeiten, sie zu verbreiten, von keiner anderen Schädlingsgattung zu übertreffen. Im vergangenen Jahr machten diese Universal-Werkzeuge von Cyberkriminellen fast zwei Drittel aller für Windows neu entwickelten Schadprogramme aus (62,51 %). Mit weitem Abstand folgten darauf klassische Computerviren (21,06 %) und deutlich abgeschlagen auf Platz 3 Internet-würmer (6,62 %).

Den weitaus größten Anteil der Trojaner-Flut verbuchten die Analysesysteme von AV-TEST als Schadcode der Kennung „Agent". Dabei handelt es sich trotz ähnlicher Schädlingskennung um eine größere Varianz klassischer Trojaner mit unterschiedlichem Funktionsumfang. Die Gattungskennung „Agent" fasst also generische Trojaner-Erkennungen zusammen, ohne sie einer bestimmten Trojaner-Familie zuzuordnen. Meist handelt es sich um Standard-Trojaner mit der Aufgabe, ein System auf unterschiedlichen Wegen zu infizieren und im Anschluss vom Angreifer ausgewählten Schadcode nachzuladen. So lassen sich gekaperte Systeme langfristig auf unterschiedliche Weise missbrauchen.

## Windows: Entwicklung neuer Trojaner
2018 + Q1 2019




## Windows: Entwicklung neuer Ransomware
2018 + Q1 2019




Anfang des Jahres 2018 handelte es sich bei von Trojanern nachgeladenem Schadcode mit großer Sicherheit um Passwort-Trojaner, Ransomware und Crypto-Miner. Denn alle drei unter Trojanern subsumierbare Schädlingsgattungen fielen zu Beginn des Jahres durch überdurchschnittliche Verbreitungszahlen auf. Im gleichen Zeitraum ließen sich umfassende Kampagnen zum Massenversand infizierter Spam-Mails rund um den Globus nachweisen. Ausgangspunkt waren dabei meist große Botnetze wie „SmokeLoader". Dessen verseuchte Spam-Sendungen enthielten im betreffenden Zeitraum häufig infizierte Microsoft Word-Dokumente mit manipulierten Makros, welche Angreifern das Fernsteuern infizierter Systeme sowie das Nachladen diverser Schadfunktionen erlaubten. Nahezu zeitgleich gelang es den kriminellen Betreiber das Botnets „SmokeLoader", ihr Netzwerk an gekaperten Rechnern durch unterschiedliche durchdachte Maßnahmen stark auszubauen. Eine dieser Maßnahmen nutzte psychologisch geschickt das Bekanntwerden der Hardware-Lecks Meltdown und Spectre. Über in Suchmaschinen gut platzierte Websites boten die Kriminellen unter anderem gefälschte Sicherheits-Updates zum Download an, deren Installation die Rechner besorgter Nutzer dann wiederum in ihre Gewalt brachten.

## 2018: Verdrängen Crypto-Miner Ransomware?

Im letzten Sicherheitsreport kündigte AV-TEST nicht zuletzt aufgrund der Messwerte des ersten Quartals für 2018 das „Zeitalter der Crypto-Miner" an und lag damit richtig. Auch die Prognosen anhand der Ransomware-Messungen des ersten Quartals bewahrheiteten sich. Und so ist die digitale Erpressung durch Ransomware, so die gute Nachricht für 2018, seit Beginn des Jahres auf dem absteigenden Ast. Einerseits beschert die Anonymität digitaler Währungen Kriminellen hohe Sicherheit beim Abkassieren ihrer Opfer, und der Einsatz von Ransomware erfordert deutlich weniger Aufwand im Vergleich zum Geschäft mit anderen Schadprogrammen. Andererseits steht und fällt das Geschäftsmodell mit der Zahlungsbereitschaft der unfreiwilligen Kunden. Und genau diese scheint zumindest in Privathaushalten zu sinken. Demzufolge ist eine stagnierende Neuentwicklungsrate von Ransomware-Samples zu konstatieren, die sich bei circa 20.000 Samples pro Monat einpendelt.

## Windows: Entwicklung neuer Crypto-Miner
2018 + Q1 2019

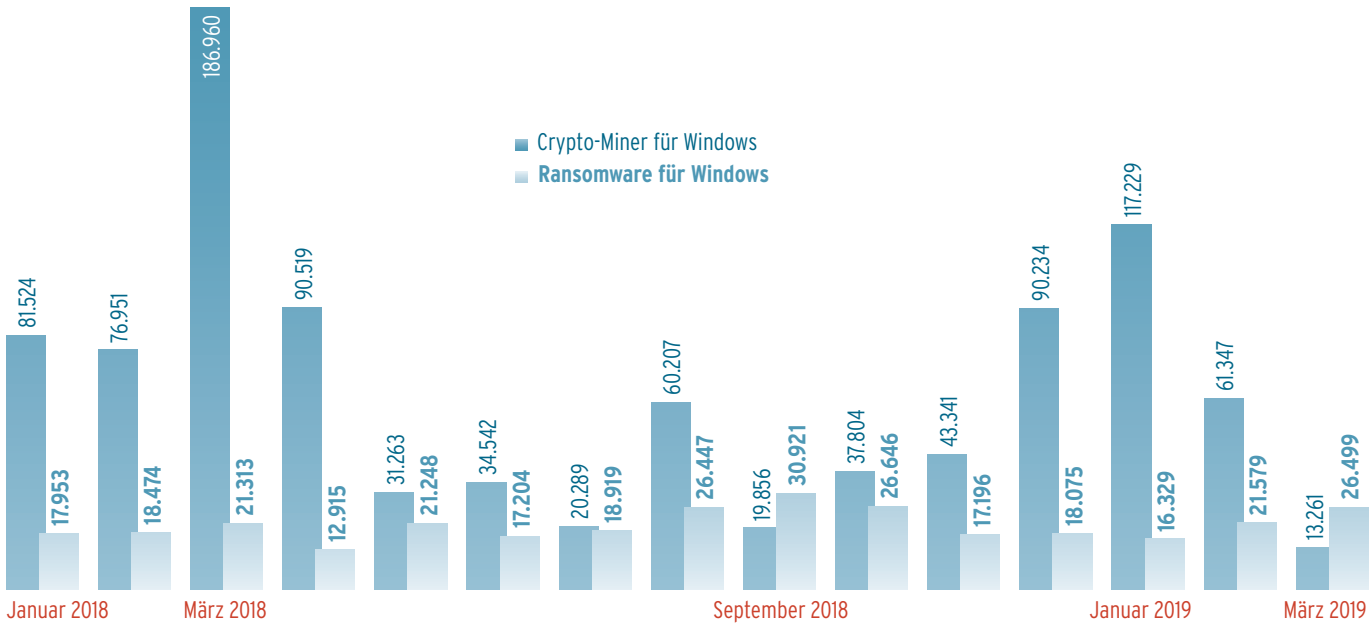

Neben der Erfassung von Ransomware-Samples sowie deren Verbreitungswege über infizierte Websites oder verseuchte E-Mails, setzt das AV-TEST Institut zur Analyse der Effektivität von Cyber-Erpressung ein selbstentwickeltes Tool ein. Es monitort die in Erpresser-E-Mails als auch in Ransomware genannten Bitcoin-Wallets. Das erlaubt den Experten aus Magdeburg nicht nur den Überblick über aktuell laufende sowie bereits erfolgte Erpressungskampagnen, sondern auch den Nachweis eingehender Zahlungen auf die von Cyberkriminellen genutzten Bitcoin-Konten.

## Crypto-Miner in der Entwicklungsphase

Konträr zur Ransomware-Entwicklung stieg die Nutzung von Crypto-Minern 2018 wie erwartet stark an, unterlang dabei jedoch heftigen Schwankungen. Ihren Höhepunkt fand die Verbreitung neuer Malware-Samples zum Schürfen digitaler Währungen im ersten Quartal des vergangenen Jahres. Über 1 80.000 Samples erfassten die Erkennungssysteme von AV-TEST im März. Von diesem Zeitpunkt an bis in den Juli brachen die erfassten Sample-Zahlen dagegen stark ein. Insgesamt zeigt die Rückschau auf 2018 drei Peaks in der Verbreitung neuer Crypto-Miner-Samples. Denn im August sowie im Dezember schnellten die Messungen erneut in die Höhe, wenn auch nicht so gewaltig, wie zuvor im Januar. Im August ließen sich immerhin exakt 60.207 Samples messen. Im Dezember schnellte die Zahl auf 90.234 erkannte Samples.

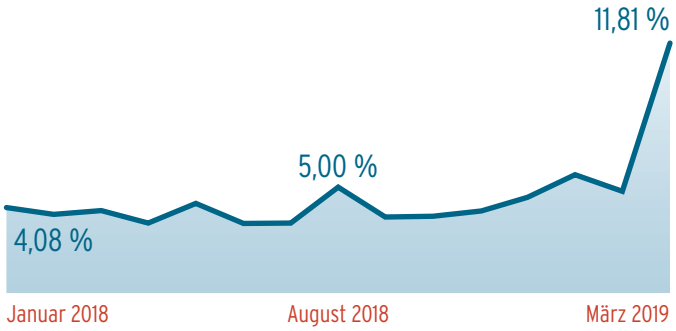
Das sprunghafte Erscheinen von Crypto-Miner-Samples lässt vermuten, dass die Entwickler ihre Produkte noch austesten beziehungsweise in Zeiten der Anstiege der Sample-Zahlen auf neue Bedingungen, etwa durch die erhöhte Erkennung durch Sicherheitsprogramme, reagieren mussten. Das Geschäft mit Crypto-Minern lohnt sich für Kriminelle nur, wenn durch eine möglichst große Anzahl infizierter Systeme möglichst lange ausreichend Rechenleistung zur Arbeit in der Blockchain zur Verfügung steht. Dementsprechend

## Windows: Vergleich Entwicklung neuer Crypto-Miner/Ransomware
2018 + Q1 2019



## Windows: Entwicklung neuer Passwort-Trojaner 2018 + Q1 2019


## Windows: Entwicklung neuer Backdoors 2018 + Q1 2019




lautet das Ziel der Angreifer, möglichst lange unauffällig die Ressourcen fremder Systeme nutzen zu können. Mit Samples der ersten Generation dürfte es kaum noch möglich sein, den Scans aktueller Sicherheitsprogramme zu entgehen. Dementsprechend müssen Kriminelle ihre Crypto-Miner ständig weiterentwickeln, wollen sie langfristig mit dieser Malware erfolgreich sein. Die drei im letzten Jahr signifikanten Ausschläge in den Erfassungszahlen könnten auf solche Entwicklungsstadien hindeuten. Der Entwicklung von Crypto-Minern widmet dieser Report ab Seite 24 ein eigenes Kapitel.

## Passwort-Trojaner im Sinkflug

Mit Passwort-Trojanern griffen Kriminelle 2018 vermehrt im ersten Quartal Zugangsdaten zu Onlinekonten ihrer Opfer ab. Von Januar bis April blieben die hohen Verbreitungswerte dieser Trojaner-Familie mit Werten weit über 130.000 neuer Samples pro Monat recht konstant. Doch in Richtung Jahresmitte halbierten sich die Werte nahezu. Und im August erreichten sie mit exakt 58.304 unterschiedlichen Samples ihren Tiefststand. Seither wurden keine Sample-Raten jenseits der signifikanten 100.000er-Marke mehr erreicht und es bleibt abzuwarten, ob Cybergangster derzeit eher auf andere Malware setzen, die mehr Erfolg mit weniger Aufwand verspricht.

Der Missbrauch fremder Kontodaten setzt im Gegensatz zur Ransomware-Erpressung und zum vergleichsweise eleganten Missbrauch fremder Rechenleistung durch Crypto-Miner einiges an Logistik und Arbeitsteilung voraus. Dementsprechend hoch ist über die Erstellung und Verbreitung der Malware hinaus auch der Aufwand beim Sammeln, Auswerten und Umsetzen der erbeuteten Kontoinformationen. Zudem reagieren Banken und andere Finanzdienstleister mittlerweile deutlich schneller auf auffällige Kontobewegungen. Damit steigt auf Seiten der Kriminellen der Aufwand, während die Margen sinken. Es bleibt abzuwarten, ob das Geschäft mit fremden Onlinedaten für Kriminelle lukrativ bleibt.

## TOP 10 Windows-Malware 2018

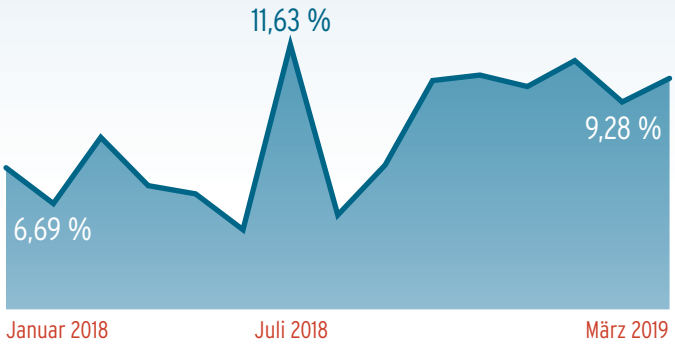
| | | |
|---|---|---|
| 1 | AGENT | 11,21 % |
| 2 | SIVIS | 5,05 % |
| 3 | KRYPTIK | 4,84 % |
| 4 | VIRLOCK | 4,57 % |
| 5 | LUDBARUMA | 3,78 % |
| 6 | VIRUT | 3,59 % |
| 7 | RAMNIT | 2,79 % |
| 8 | ADLOAD | 2,63 % |
| 9 | UPATRE | 2,16 % |
| 10 | LAMER | 2,00 % |

## Andere Malware-Gattungen und PUA

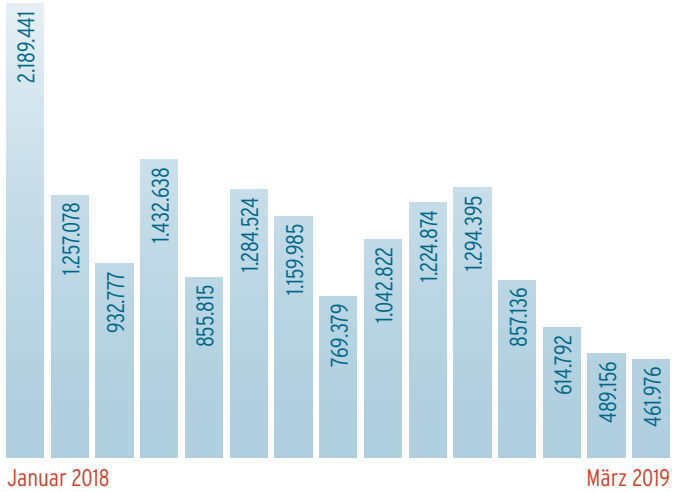
Während Schutzprogramme für Windows 2018 vorwiegend mit der weiter steigenden Flut von Trojanern zu kämpfen hatten, zeigten sich die Neuentwicklungsraten anderer klassischer Malware-Gattungen im Abwärtstrend oder stagnierten im Vergleich mit den Vorjahreswerten aus 2017. Das galt sowohl für Internet-Würmer, die 2018 die Grenze von 100.000 Neu-Samples pro Monat nicht überschritten, als auch für schädliche Skripte, die nur noch 0,15 Prozent der gesamten Malware-Erfassung ausmachten. Dialer und Rootkits wurden von den Erkennungssystemen des AV-TEST Instituts zwar erfasst, spielten 2018 zumindest statistisch aufgrund zu geringer Sample-Zahlen keine relevante Rolle.

Eine weitere gute Nachricht ist die rückläufige Entwicklung von Tracking-Tools zur Überwachung des Nutzerverhaltens sowie anderer unerwünschter Programme (PUA). Diese im rechtlichen Graubereich agierende Software, die etwa das Surfverhalten von Nutzern erfasst und an Unternehmen weiterleitet, scheint sich zumindest unter Windows nicht mehr zu lohnen und ist daher stark rückläufig. Dies kann unter anderem als Erfolg von Herstellern von Antiviren-Software für Windows gesehen werden, die PUA trotz erheblicher Widerstände der Industrie als Bedrohung an die Nutzer ihrer Schutzprogramme meldeten.

## Windows: Entwicklung neuer Würmer
2018 + Q1 2019




## Windows: Entwicklung neuer PUA
2018 + Q1 2019




# Trend 2019

**Die Erfassungsdaten des ersten Quartals 2019 bestätigen im Wesentlichen die Entwicklung des vorangegangenen Jahres. Einer stark steigenden Zahl an Windows-Exploits folgen die Entwicklungszahlen von Trojanern, die weiterhin den Großteil der für Windows neu entwickelten Malware stellen. Der Anteil spezialisierter Trojaner, darunter Crypto-Miner, nimmt zu. Auch für Ransomware zeigen die AV-TEST Systeme im ersten Quartal entgegen den Zahlen des Vorjahres einen leicht steigenden Trend. Die Entwicklungszahlen neuer Passwort-Trojaner sinken dagegen beständig bis zu unter einem Prozent des Malware-Gesamtaufkommens.**

**Die AV-TEST GmbH überprüft im Zweimonatsturnus regelmäßig alle auf dem Markt relevanten Anti-Viren-Lösungen für Windows. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/privat-windows/ abgerufen werden.**

# Sicherheitsstatus ANDROID

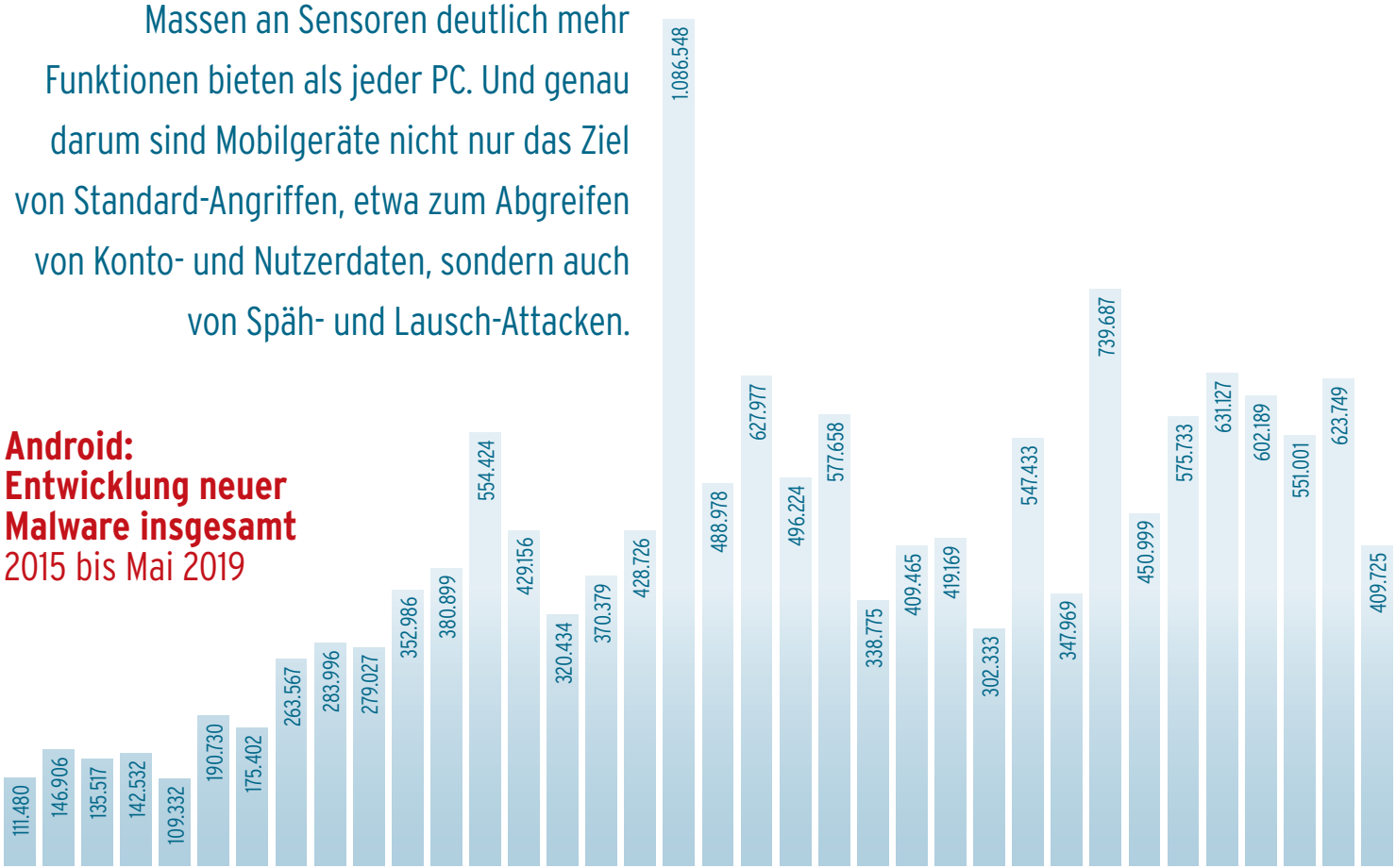
Smart wurden Mobiltelefone 2007 mit der Einführung von Apps. Mit der Möglichkeit, selbstentwickelte Applikationen für fremde Nutzer online anzubieten, wurden leider auch die Angriffsmethoden Cyberkrimineller pfiffiger. Und seither entwickeln sie ständig neue Malware für Geräte, die Nutzer permanent bei sich tragen und die dank Massen an Sensoren deutlich mehr Funktionen bieten als jeder PC. Und genau darum sind Mobilgeräte nicht nur das Ziel von Standard-Angriffen, etwa zum Abgreifen von Konto- und Nutzerdaten, sondern auch von Späh- und Lausch-Attacken.

## Sinkende Rate neu entwickelter Malware

Im Vergleich zum bisherigen Höchststand der Malware-Neuentwicklungsrate im Juni 2016 lesen sich die Entwicklungszahlen des vergangenen Jahrs geradezu entspannt: Im Vergleich hat sich die Anzahl neuer Schadprogramme für Android-Systeme nämlich fast halbiert. Im Durchschnitt verbreiteten Kriminelle im vergangenen Jahr pro Monat 616.459 schädliche Applikationen für das weltweit meistgenutzte Mobilbetriebssystem. Dementsprechend fällt zumindest die rein quantitative Betrachtung positiv aus.

Allerdings, und das ist die Kehrseite der Medaille, nahm der Spezialisierungsgrad der Malware deutlich zu. Und so sind die sinkenden Malware-Zahlen leider alles andere als ein Grund, Entwarnung zu geben. Vornehmlich beruht die quantitative Entspannung auf dem Rückgang klassischer Trojaner. Die machen mit über 90 Prozent aller Neuentwicklungen nach wie vor den Großteil aller Schädlinge für Android aus. Allerdings legen Schadprogramme mit hohem Spezialisierungsgrad und zielgerichteter Schadwirkung stark zu, darunter Crypto-Miner, Passwort-Trojaner und Ransomware. Dementsprechend ist ein Trend zu Malware erkennbar, mit der Kriminelle direkt und ohne große Umwege Geld verdienen können.

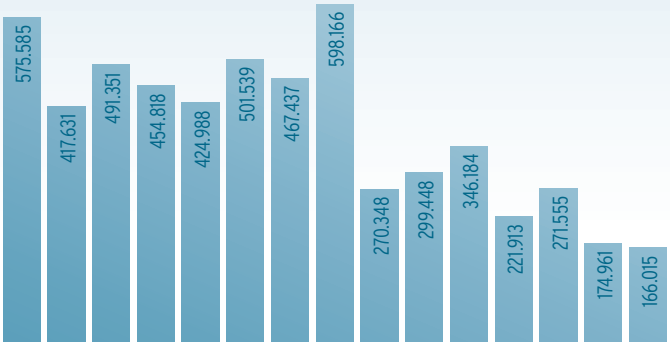
**Android: Entwicklung neuer Malware insgesamt**
2015 bis Mai 2019



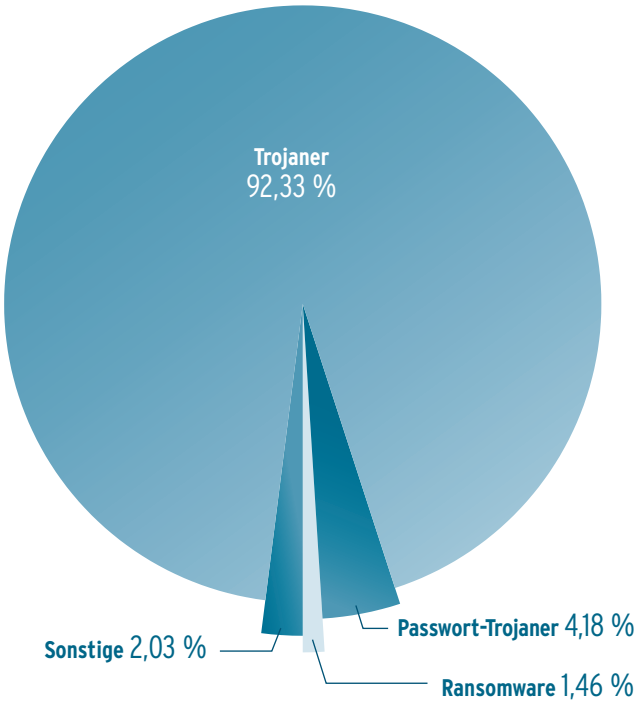
## Banking-Malware wird Hightech

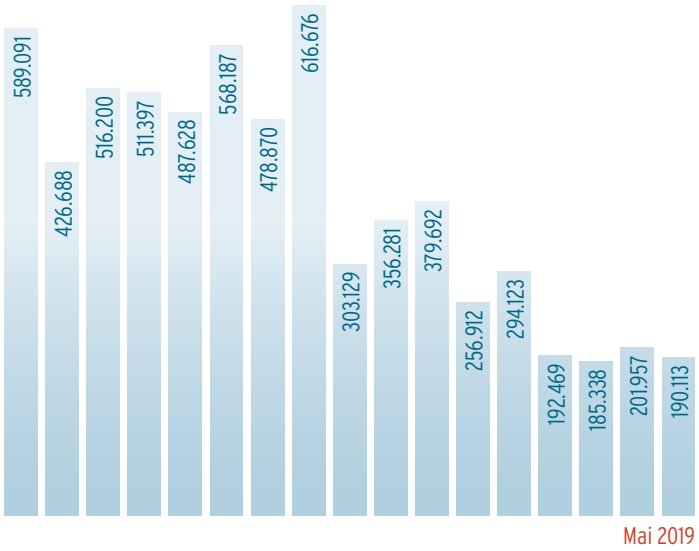
Die zunehmende Verbreitung und Akzeptanz von Banking-Apps ist schließlich auch Cyberkriminellen nicht entgangen. Weltweit gibt es kaum noch ein Bankhaus, das keine eigene App anbietet. Und solche Banking-Apps werden zunehmend nicht nur zur Zwei-Faktor-Authentifizierung beim Banking über den PC genutzt, sondern immer mehr Kontozugriffe werden direkt über das Mobilgerät vorgenommen. Neben etablierten Banken boten 2018 auch immer mehr Finanzdienstleister, sogenannte Fintechs, Apps für Mobile-Banking auf Android-Basis. Und bei solchen Geldhäusern gibt es gar keinen anderen Zugang zum eigenen Konto, als über die jeweilige App. Dementsprechend wandelte sich die Entwicklung von Schadprogrammen, die per Phishing Anmeldeinformationen von Onlinekonten ergaunern, hin zu Hightech-Malware. Ein Beispiel dafür ist die Entwicklung, die der Banking-Trojaner „Anubis", im Laufe des Jahres zeigte. Die Malware zum Abgreifen von Kontozugangsdaten bekam über das Jahr Modifikationen, die seine Erkennung durch Sicherheits-Apps verhindern sollen. Der Schädling, der etwa als Batterie-App getarnt aufs Gerät kommt, verschafft sich Zugriff auf die Bewegungssensoren infizierter Mobilgeräte. Vermelden die Sensordaten keine Bewegung, geht der Schädling von einer Sandbox zur Erkennung von Schadsoftware aus und stellt sich tot.

## Android: Entwicklung neuer Trojaner
2018 + Q1 2019

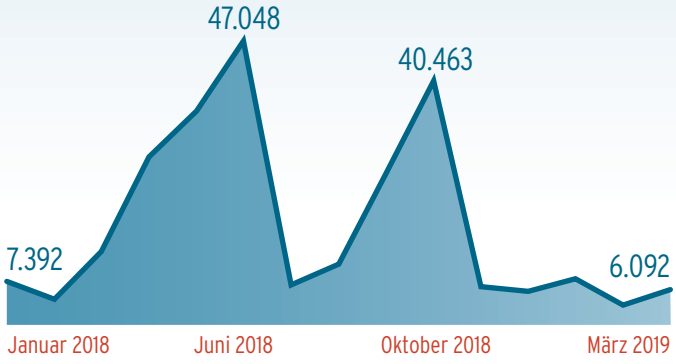



## Android: Malware-Verteilung 2018

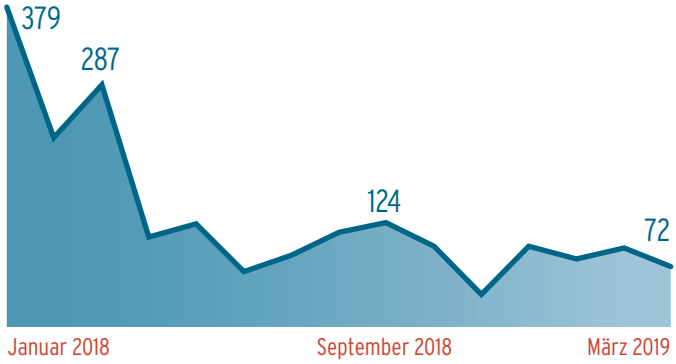


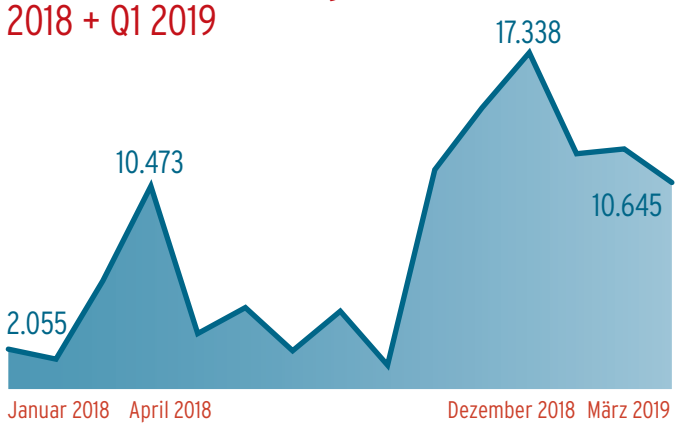
## Android: Entwicklung neuer Passwort-Trojaner 2018 + Q1 2019




## Android: Entwicklung neuer Crypto-Miner 2018 + Q1 2019




## Android: Entwicklung neuer Ransomware 2018 + Q1 2019




Letzter Stand der Technik dürfte der im ersten Quartal 2019 geortete Banking-Trojaner „Gustuff" sein. Dieser Hightech-Schädling kann nicht nur Anmeldedaten von über 100 Banking- sowie mehr als 30 Kryptowährungs-Apps stehlen, sondern mit diesen Daten auch automatisch Transaktionen ausführen. Dazu startet Gustuff im Hintergrund selbstständig entsprechende Apps und leitet über abgefangene Kontodaten eigenständig Transaktionen auf voreingestellte Konten ein.

## „Schnelles Geld" mit Android

Im ersten Quartal des vergangenen Jahres starteten zudem Crypto-Miner auf Android-Basis ihren Höhenflug, der allerdings seither abebbt und im ersten Quartal 2019 bei Entwicklungsraten von unter hundert neuen Samples pro Monat stagniert. Es ist allerdings davon auszugehen, dass Kriminelle die ständig steigende Rechenleistung mobiler Endgeräte dauerhaft anzapfen werden, sobald die technische Entwicklung ihrer Malware einen langfristigen unentdeckten Verbleib auf den Endgeräten ermöglicht. Dies setzt voraus, dass die Crypto-Miner so entwickelt werden, dass ihre Ortung nicht bereits durch den stark zunehmenden Akkuverbrauch erfolgt.

Eine andere Masche zum direkten „Abkassieren" der Nutzer von Mobilgeräten sind Erpresser-Trojaner. Und gerade gegen Ende des Jahres 2018 legte die Entwicklung neuer Ransomware-Samples für Googles Betriebssystem stark zu. Im Dezember erreichte die Jahresrate mit 17.338 neu entwickelten Ransomware-Samples ihren Höchststand. Setzt man die nach wie vor zu geringe Verbreitung von Schutz-Apps für Android-Geräte sowie die Nachlässigkeit beim Erstellen von Backups in Relation zu all den Daten, die Nutzer auf ihren Geräten mit sich herumtragen, scheint es sich bei Ransomware für Android um ein zukunftsträchtiges Geschäftsmodell zu handeln.

## TOP 10
## Android-Malware 2018

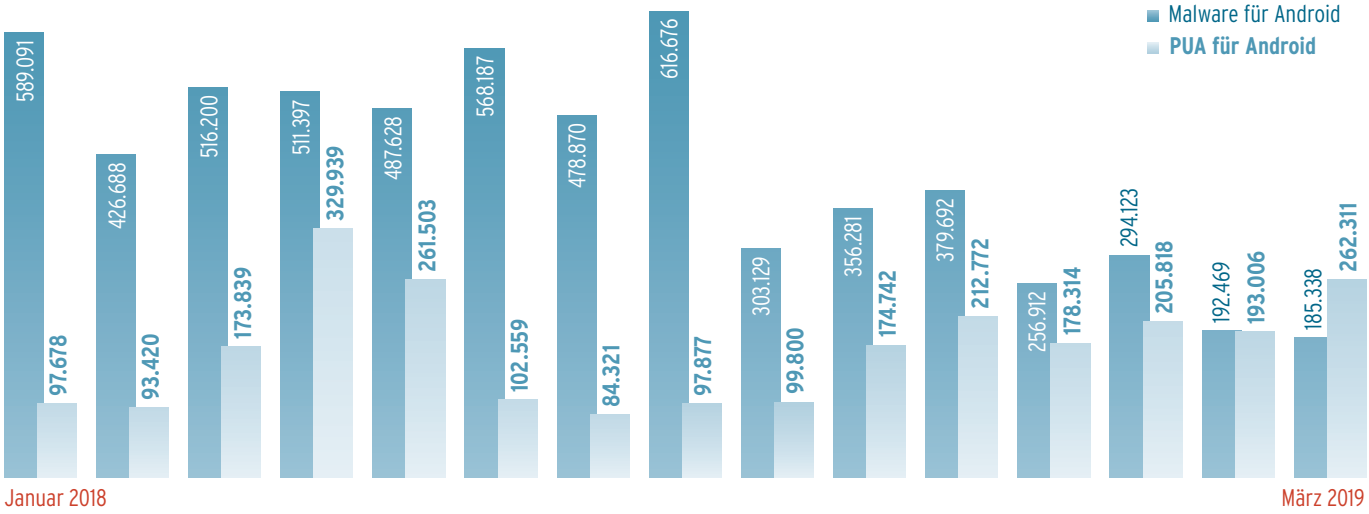
| | | |
|---|---|---|
| 1 | SMSREG | 23,81 % |
| 2 | SHEDUN | 19,94 % |
| 3 | AGENT | 15,44 % |
| 4 | SMSPAY | 6,92 % |
| 5 | SMS | 5,30 % |
| 6 | HIDDENAPP | 3,00 % |
| 7 | HIDDAD | 1,89 % |
| 8 | CLICKER | 1,86 % |
| 9 | SMSAGENT | 1,57 % |
| 10 | FAKEAPP | 1,23 % |

# Trend 2019

**Die Gesamtrate von Android-Schadprogrammen zeigt sich im ersten Quartal 2019 weiter rückläufig. Dieser Trend kommt im Wesentlichen durch sinkende Sample-Zahlen bei klassischen Trojanern zustande. Ihm folgen auch die Raten hochspezialisierter Malware, wie Ransomware, Crypto-Miner und Banking-Trojaner. Allerdings geben diese Raten lediglich die quantitative Malware-Entwicklung wider und die Analyse von Hightech-Malware wie „Gustuff" lässt vermuten, dass der Trend eher zu qualitativ hochwertigen Schädlingen geht und die Bedrohungslage trotz sinkender Sample-Zahlen steigt.**

**Bei Android-Mobilgeräten kommt ein negativer Trend hinzu: Während bei den meisten anderen Betriebssystemen die Entwicklung unerwünschter Software (PUA) rückläufig ist, nimmt die Spionage des Nutzungsverhaltens bei Android-Geräten zu. So übersteigt die Zahl von PUA-Samples im März erstmals die Anzahl neu entwickelter Schadprogramme.**

## Android: Entwicklung Malware zu PUA
2018 + Q1 2019

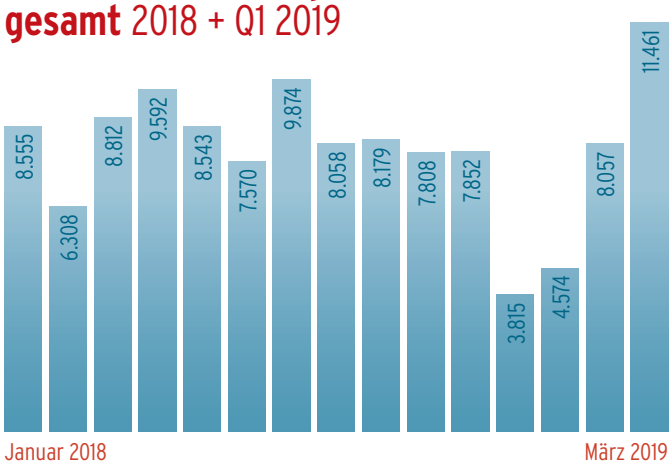



AV-TEST GmbH überprüft im Zweimonatsturnus regelmäßig alle marktrelevanten Schutzlösungen für Android-Mobilgeräte. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/mobilgeraete/ abgerufen werden.

# Sicherheitsstatus macOS

Seit der Integration des Malware-Scanners Xprotect in Mac OS X 10.6 (Snow Leopard) gibt Apple de facto zu, dass die Malware-Bedrohung auch für ihre Rechner existiert. Dennoch hält sich nicht nur unter Apple-Fans hartnäckig das Gerücht, macOS-Nutzer bräuchten keinen zusätzlichen Virenschutz. Das AV-TEST Institut steuert der oft emotional geführten Diskussion mit aktuellen Messungen zu Mac-Malware entscheidende Fakten bei.

**macOS: Entwicklung neuer Malware gesamt** 2018 + Q1 2019




## Macs Malware-Kurve steigt beständig

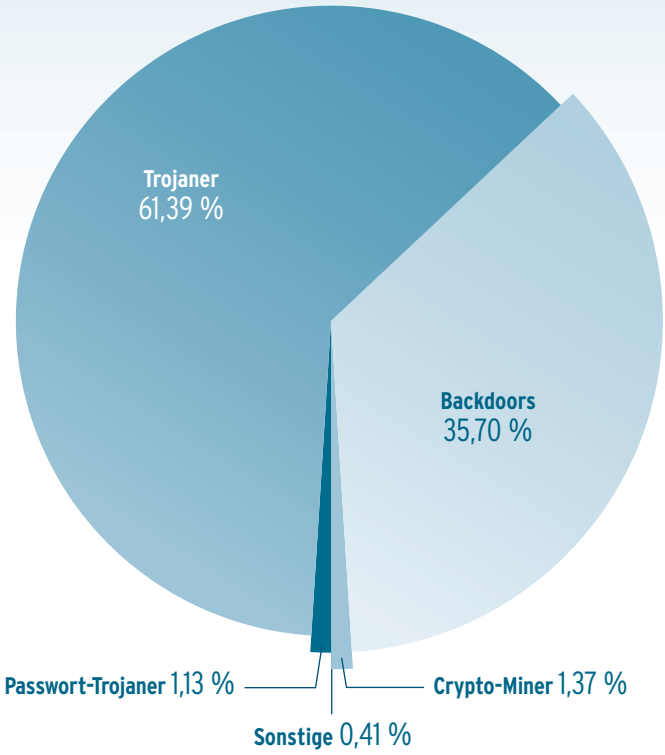
Richtig ist, dass die quantitative Bedrohungslage für Apple-Nutzer gemessen am reinen Vorkommen neu entwickelter Malware-Samples deutlich geringer ausfällt, als bei anderen gängigen Betriebssystemen. Pro Monat entdeckten die Erfassungssysteme des AV-TEST Instituts in 2018 im Durchschnitt 7.913 neue Malware-Samples für Apples Betriebssystem. In Summe kamen im vergangenen Jahr somit genau 94.966 Mac-Schädlinge zusammen. Dieser Malware-Rate sehen sich Windows-Systeme annähernd pro Stunde ausgesetzt. Allerdings schützen auch deutlich mehr Windows-Nutzer ihre Systeme mit einer Viren-Abwehr-Software. Und im Vergleich zu den „glücklichen Jahren" mit geringer Mac-Malware-Entwicklung, haben Cyberkriminelle Apple-Nutzer klar als lukratives Ziel ausgemacht. Die knapp unter hunderttausend Malware-Samples in 2018 sprechen eine deutliche Sprache.

## Apple-Attacken sind Trojaner-Attacken

Wie bei den meisten anderen Betriebssystemen auch, zeigen sich Trojaner als Mittel der Wahl der Cyberkriminellen bei Angriffen auf Apple-Systeme. Satte 61,39 Prozent aller macOS-Schädlinge waren 2018 Trojaner. Gepaart mit Backdoors, die 35,7 Prozent der Gesamt-Malware-Summe ausmachten und somit Platz 2 belegten, eine brisante Mischung. Denn beide Malware-Typen zielen darauf ab, beliebige Schadfunktionen nach Infektion auf Opfer-Systeme nachzuladen.

Dieses Ziel verfolgt auch der Trojaner Flashback, der zum dritten Mal in Folge Platz 1 der Malware Top 10 für macOS verteidigt. Erste Flashback-Versionen tarnten sich als Installationspaket des beliebten Flash Players. Doch eine neue Variante des Trojaners bietet Angreifern wesentlich umfangreichere Infektionswege, darunter etwa der Drive-by-Download über infizierte Websites. Bei aktiviertem Java-Code entert Flashback Apple-Rechner dann automatisch über den Browser. Dass ständige Modifikationen dieses bereits 2012 erkannten Schadcodes nach wie vor erfolgversprechend für Cyber-kriminelle sind, lässt tief blicken. Im vergangenen Jahr machten Flashback-Samples über 40 Prozent der kompletten Malware für Macs aus (43,33 %)! Doch Flashback ist kein Einzelfall. In den Malware Top 10 für Apple-Rechner tummeln sich jede Menge „alter Bekannter" wie „Mac Control", „Getshell" und „Keranger". Was verdeutlicht, dass der Innovationsdruck bei den Entwicklern von Mac-Malware aufgrund geringer Gegenwehr nicht allzu groß sein kann.

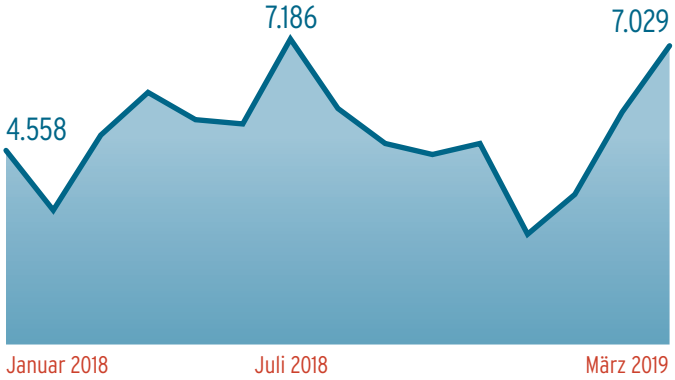
## macOS: Malware-Verteilung 2018



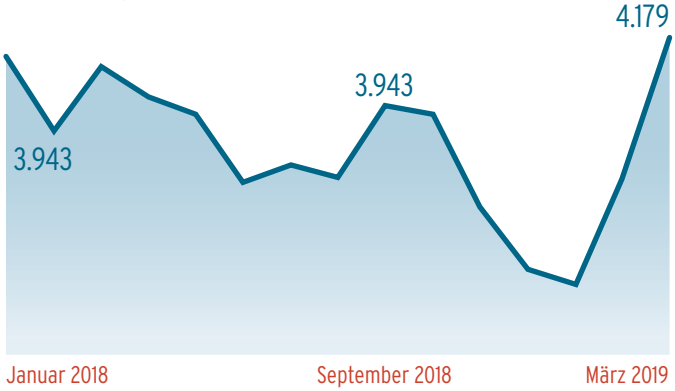

## TOP 10 macOS-Malware 2018

| | | |
|---|---|---|
| 1 | FLASHBACK | 43,33 % |
| 2 | MAC CONTROL | 39,74 % |
| 3 | SHLAYER | 10,90 % |
| 4 | AGENT | 1,60 % |
| 5 | ADLOAD | 1,42 % |
| 6 | APTORDOC | 1,13 % |
| 7 | GETSHELL | 0,18 % |
| 8 | MACNIST | 0,16 % |
| 9 | KERANGER | 0,11 % |
| 10 | XCODEGHOST | 0,07 % |

## macOS: Entwicklung neuer Trojaner 2018 + Q1 2019



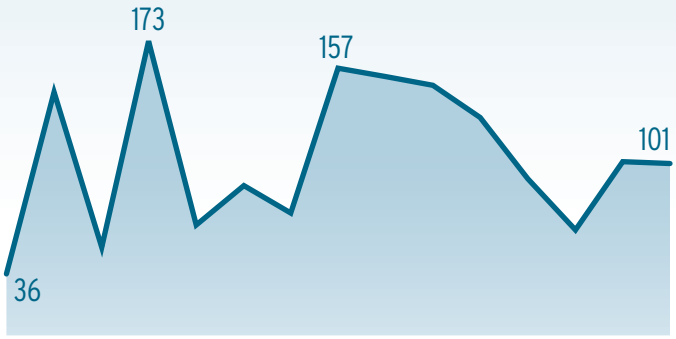

## macOS: Entwicklung neuer Backdoors 2018 + Q1 2019



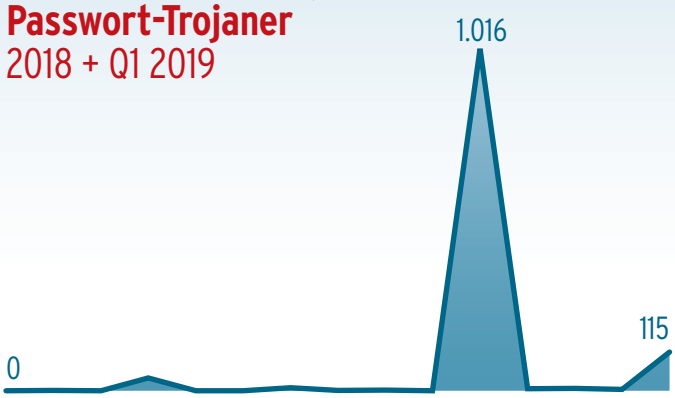

## Malvertising für macOS im Trend

Doch das Jahr 2018 hatte auch Malware-Neuentwicklungen wie „Shlayer" zu bieten. Dieser Mac-Trojaner nutzt seit Ende des vergangenen Jahres die Malvertising-Masche, indem er seine Opfer über angekaufte Werbebanner auf infizierte Websites führt und sich so verbreitet. Öffnet der Browser eine entsprechende Website, leitet das Banner auf eine verseuchte Website weiter. Hier bietet sich der Trojaner dann als Update-Paket des Flash Player zum Download an. Shlayer belegte mit 10,9 Prozent des Gesamt-Malware-Aufkommens auf Anhieb Platz 3 der Malware Top 10. Shlayer zielt ebenfalls darauf ab, weiteren Schadcode mit weiteren Funktionen nachzuziehen.

## macOS: Entwicklung neuer Crypto-Miner
2018 + Q1 2019




## macOS: Entwicklung neuer Passwort-Trojaner
2018 + Q1 2019




## Mac-User direkt ausgecasht

Gemessen an den reinen „Stückzahlen" könnte es so wirken, als handele es sich bei spezialisierter Malware für Macs um eine geringe Bedrohung. Tatsache ist aber, dass es sie gibt, und dass sie auf wenig Gegenwehr trifft. Während klassische Viren, die bei der Windows-Malware immerhin über 20 Prozent ausmachen, für Mac-Rechner kein Thema sind (0,04 %), lohnt sich der Einsatz von Highend-Malware für Kriminelle bereits bei geringen Stückzahlen. Im Gegensatz zu Windows-Nutzern setzen Kriminelle bei Mac-Usern direkt auf Malware, die sich mehr oder weniger sofort in bare Münze umsetzen lässt. Dazu gehörten 2018 insbesondere Crypto-Miner, Passwort-Trojaner und Ransomware. Die Möglichkeit, Ressourcen der meist mit leistungsfähiger Hardware ausgestatteten Apple-Rechner zum Schürfen digitaler Währung zu missbrauchen, stand 2018 hoch im Kurs. Insgesamt 1.305 Malware-Samples der Gattung Crypto-Miner erfassten die AV-TEST Systeme für Mac-Malware (1,31 %). Dahinter folgten Passwort-Trojaner zum Abgreifen von Kontodaten (1,13 %), danach Erpresser-Trojaner (0,16 %).

## Trend 2019

**Im ersten Quartal 2019 verlieren Backdoors in der Gesamt-Malware-Verteilung knapp fünf Prozent an die Gattung der Trojaner, die mit über 66 Prozent klar den Großteil der Mac-Malware stellen. Während der Stellenwert der Crypto-Miner bei Cyberkriminellen leicht sinkt, steigt die Neuentwicklungsrate von Ransomware um das Vierfache. Dementsprechend sind Mac-Nutzern nicht nur ein gutes Virenschutzprogramm, sondern auch regelmäßige Backups zu empfehlen.**

**AV-TEST GmbH überprüft in regelmäßigen Abständen alle marktrelevanten Antiviren-Lösungen für Mac. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/ abgerufen werden.**

# Sicherheitsstatus IoT/LINUX

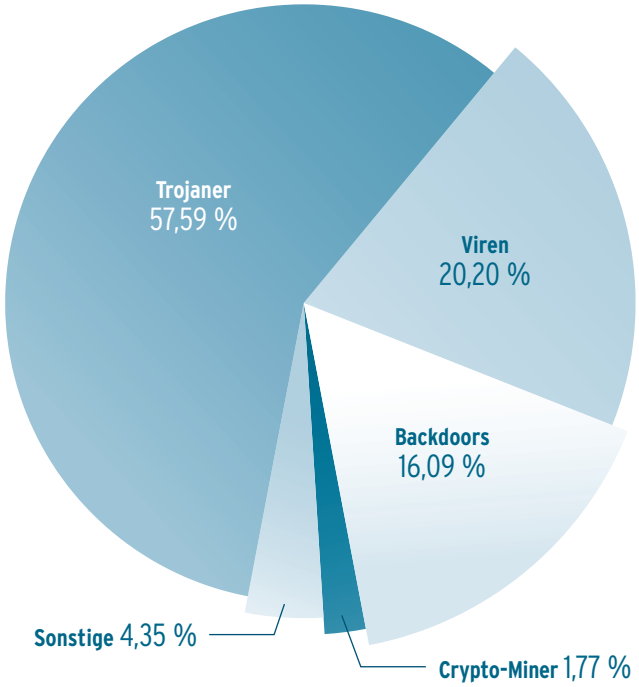
Mit einer mittlerweile nahezu unüberschaubaren Zahl vernetzter Geräte und Services ist das Internet der Dinge in der Entwicklung von IT-Märkten ein absoluter Boom-Sektor. Doch im Wettrennen um lukrative Marktanteile entwickelt die IoT-Industrie weiter massenhaft internetangebundene Produkte ohne ausreichendes Sicherheitskonzept und lässt häufig selbst absolute Mindeststandards der IT-Sicherheit außer Acht.

## Verdoppelung vernetzter Geräte in vier Jahren

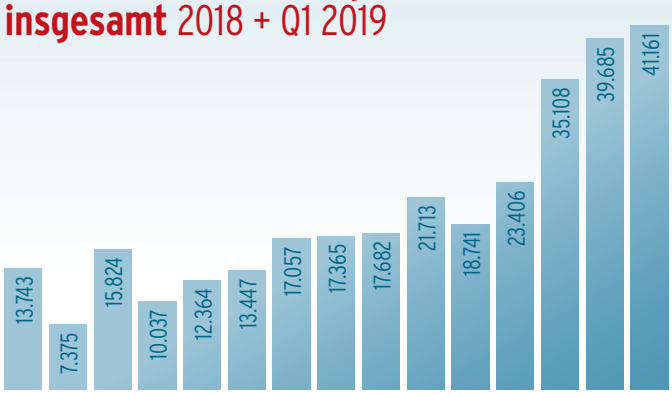
Für Cyberkriminelle ist die rasant wachsende Zahl gar nicht oder bestenfalls schlecht geschützter Geräte ein leichtes und willkommenes Angriffsziel. Das Risiko tragen arglose Nutzer vernetzter Geräte. Sie verlassen sich auf fehlende rechtliche Vorgaben sowie das Verantwortungsbewusstsein der Hersteller und riskieren so den Verlust ihrer Privatsphäre.

Die Gesamtzahl von Geräten, die bis 2022 über das Internet der Dinge miteinander kommunizieren werden, schätzen Juniper-Analysten in einer aktuellen Studie auf mehr als 50 Milliarden. Gegenüber dem Stand von 21 Milliarden im Jahr 2018 ist also mehr als eine Verdoppelung des IoT-Kosmos in nur vier Jahren zu erwarten. Das starke Wachstum des Internets der Dinge bezieht sich auf nahezu alle Bereiche unseres Lebens und wird unsere Arbeitswelt ebenso verändern, wie unsere Freizeit. Solche Geräte und Dienste können uns das Leben erleichtern, doch auch das genaue Gegenteil kann der Fall sein. Denn immer mehr Geräte, die wir ganz selbstverständlich im Alltag

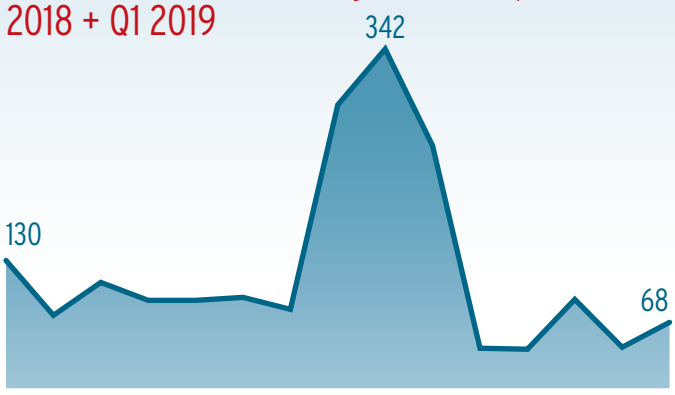
## IoT: Malware-Verteilung 2018



## IoT/Linux: Entwicklung neuer Malware insgesamt 2018 + Q1 2019




## IoT/Linux: Entwicklung neuer Exploits 2018 + Q1 2019




nutzen, und von denen wir es zum Teil gar nicht erwarten, werden mit dem Internet verknüpft. Statt wie bisher Fernseher, Kameras und smarte Sprachassistenten werden in naher Zukunft alltägliche Gebrauchsgegenstände, wie Staubsauger oder Zahnbürsten, Informationen über ihre Nutzer sammeln und an ihre Hersteller und deren Geschäftspartner senden.

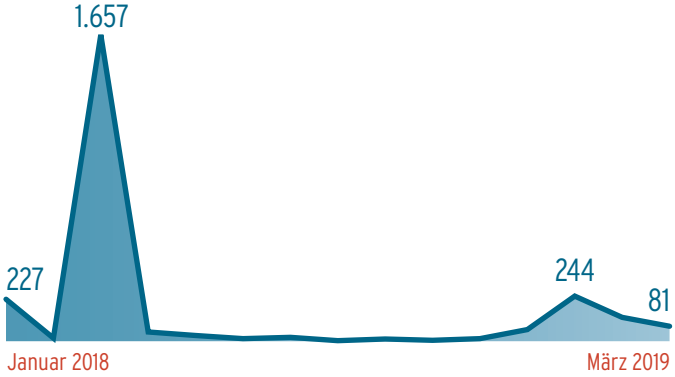
Tatsache ist, dass Sicherheitsexperten wie die des AV-TEST Instituts bereits seit Jahren vor den Gefahren angreifbarer IoT-Geräte warnen, diese Rufe allerdings weiterhin häufig ungehört verhallen. Dabei begehen gerade die Hersteller von Endanwenderprodukten, insbesondere solche, die nicht ursprünglich aus der IT-Industrie kommen, dieselben Fehler, wie sie bereits vor 30 Jahren bei PCs und vor 10 Jahren bei Smartphones und anderen Mobilgeräten begangen wurden: schlecht bis gar nicht geschützte Zugangskonten, schwache oder meist fehlende Verschlüsselung bei Speicherung und Transport von Daten, veraltete Software und mangelhafte bis fehlende Versorgung mit Sicherheitsupdates. Diese Fehler öffnen Angreifern nach wie vor bei der Mehrzahl der Geräte, Tendenz steigend, Tür und Tor. Hinzu kommt, dass die IT-fremde Branche ihre Geräte zunehmend „smart" anbietet, sprich mit Internetanbindung und App verkauft. Allerdings findet dabei die Entwicklung IT-typischer Module, wie Onlinedienste und Apps, zumeist durch Drittanbieter statt. Und so wissen die Anbieter vernetzter Produkte oft nicht, was in ihren Apps oder hinter ihren Onlinediensten steckt und können diese aus eigener Kraft auch nicht warten, prüfen und selbst mit den notwendigen Sicherheitsupdates versehen.

## Fehlende Standards und alte Lücken

Grundsätzlich bieten IoT-Geräte und Dienstleistungen eine Vielzahl an Angriffsvektoren: Die Hauptangriffsziele Krimineller sind die Endgeräte selbst, angebundene Apps sowie die Mobilgeräte, auf denen die Applikationen zur Steuerung von IoT-Geräten meist laufen. Das durch die Serverstrukturen und Geräteanbindung eingesetzte Backend der Hersteller sowie die Übertragungswege notwendiger und darüber hinaus erfasster Daten sind weitere Einfallstore für digitale Angriffe. Dennoch erobern weiter IoT-Geräte mit man-

## IoT: Entwicklung neuer Gafgyt-Trojaner 2018 + Q1 2019


## IoT: Entwicklung neuer Hajime-Trojaner 2018 + Q1 2019



## IoT: Entwicklung neuer Mirai-Trojaner
2018 + Q1 2019

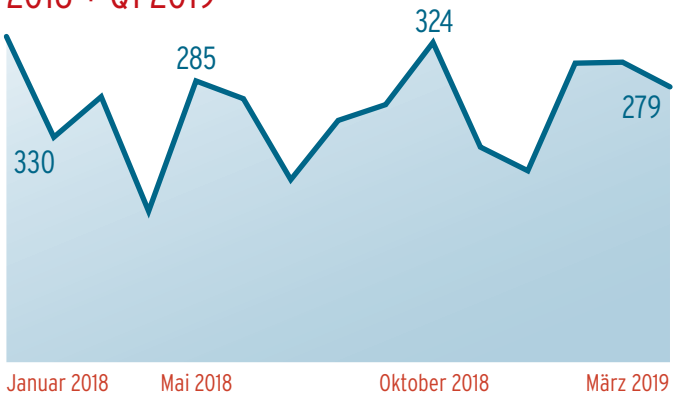

## IoT: Entwicklung neuer Vit-Trojaner
2018 + Q1 2019


gelhafter IT-Sicherheit den Markt. Und auf die wachsende Zahl an ungeschützten Geräten wartet bereits eine Flut von Schadprogrammen, die sich aktuell zumeist deren geballte und vernetzte Rechenleistung zu eigen machen will.

Aufgrund der Anforderungen, dass gängige und kompatible IoT-Systeme auch auf Mikrocontroller-Ebene lauffähig sein müssen, kommen meist abgespeckte Linux-Versionen wie Canonical Ubuntu zum Einsatz. Im letzten Quartal von 2017 verzeichneten die Erfassungssysteme des AV-TEST Instituts eine rasant steigende Zahl neu entwickelter Malware für IoT-Systeme auf Linux-Basis. 2018 erhöhte sich die Schlagzahl der Malware-Neuentwicklungen noch einmal drastisch: 15.730 neue Schadprogramme für Angriffe auf IoT-Geräte und Infrastrukturen wurden im Durchschnitt pro Monat des vergangenen Jahres entwickelt. Und dieser ohnehin kritische Wert für eine rasant wachsende Geräte-Gruppe, die zum Großteil ohne oder bestenfalls mit schlechtem Schutz im Netz steht, verschärft sich im ersten Quartal 2019 dramatisch: Innerhalb von drei Monaten verdoppelte sich die IoT-Schädlingsrate auf den aktuellen Höchststand von über 40.000 neuen Samples pro Monat.

Doch selbstverständlich sind auch andere IoT-Betriebssysteme, wie etwa die quelloffenen Systeme Contiki und RIOT OS sowie Googles abgespeckte Android-Version Brillo OS anfällig für Angriffe. Den Großteil neu entwickelter Malware für IoT-Systeme stellte 2018 mit 57,59 Prozent die Gattung der Trojaner. Großen Anteil daran hatte ein „alter Bekannter", der bereits in den Sicherheitsreports der letzten zwei Jahre eine tragende Rolle spielte: „Mirai". Die Erkennungssysteme von AV-TEST erfassten den Schädling erstmals im August 2016, und im Oktober 2016 führte Mirai bereits breit angelegte DDOS-Angriffe gegen große Onlinedienste in den USA und Europa aus. Die Rechenleistung dafür bezog Mirai aus einem Botnetz hunderttausender gekaperter Router, Drucker, Webcams und Online-Videorecorder ohne wirkungsvolle Authentifizierungsverfahren und mit schlechter oder fehlender Verschlüsselung.

## IoT: Entwicklung neuer Tsunami-Trojaner
2018 + Q1 2019




## IoT/Linux: Entwicklung Backdoors
2018 + Q1 2019

## Hohe Malware-Kurve contra geringe Lernkurve

Gemessen an den Entwicklungszahlen scheint sich die Nutzung des Mirai-Schadcodes für Kriminelle weiterhin zu lohnen. So machte der Mirai-Code 2018 insgesamt über 40 Prozent des gesamten Schadcodes für IoT-Geräte aus (41,19 %). Leider spricht die steile Entwicklungskurve von Mirai-Samples nicht für eine entsprechend hohe Lernkurve bei den Geräteherstellern, denen diese Gefahren spätestens seit Oktober 2016 geläufig sein sollten. Eine Reaktion scheint allerdings nicht zu erfolgen und dementsprechend nutzen Kriminelle Mirai weiterhin erfolgreich für Angriffe auf IoT-Geräte und angeschlossene Infrastruktur. Die Sample-Zahlen der Haupt-Malware für IoT-Geräte explodieren seit Anfang letzten Jahres. Mit 78.186 Varianten führt Mirai die Rangliste klar an, vor anderen IoT-Trojanern wie „Vit" (37.807 Samples), „Gafgyt" (36.769 Samples) und „Tsunami" (2.959 Samples).

Eine Entwicklung, die Cyberkriminellen dabei sicher in die Hände spielt, ist die steigende Anzahl bekannter Sicherheitslücken von IoT-Geräten sowie die zunehmende Möglichkeit, diese über automatisierten Schadcode anzugreifen.

Entsprechend steigen die Messungen verfügbarer Backdoors. Im vergangenen Jahr standen Angreifern insgesamt 188.754 dieser Einfallstore allein für Linux-Systeme zur Verfügung. Im ersten Quartal des Jahres 2019 waren es bereits 115.954!

Gefährdungen anderer Art, etwa in Richtung digitaler Erpressung, oder durch den Ausfall wichtiger IoT-Geräte, Dienste und Funktionen, sind ein weiteres Horrorszenario der digitalisierten Zivilgesellschaft. Aktuelle Messungen erfassen zwar erste Versuche auf dem Gebiet der Ransomware, allerdings sind diese zumindest zahlenmäßig noch nicht als akute Bedrohung auszumachen. Hingegen zeigen bereits erfolgte Mirai-Attacken, in 2018 etwa 0,01 Prozent der Gesamt-Malware, dass für Erpressungsmodelle auf IoT-Basis nicht zwingend ein spezialisierter Ransomware-Code vonnöten sein muss.

### TOP 10 IoT-Malware 2018

| | | |
|---|---|---|
| 1 | MIRAI | 41,19 % |
| 2 | VIT | 19,93 % |
| 3 | GAFGYT | 19,40 % |
| 4 | TSUNAMI | 1,57 % |
| 5 | AGENT | 1,41 % |
| 6 | BITCOINMINER | 1,25 % |
| 7 | DDOSTF | 1,11 % |
| 8 | HAJIME | 1,11 % |
| 9 | DOFLOO | 0,92 % |
| 10 | SHELLDL | 0,89 % |

# Trend 2019

Neben der langjährigen, systematischen Erfassung neuer Malware-Samples für IoT-Geräte, die im ersten Quartal insbesondere für Mirai, Vit und Gafgyt weiter massiv ansteigen, analysiert das AV-TEST Institut seit 2017 die Systematik von Angriffen auf vernetzte Geräte mit eigenen Honeypot-Systemen. Diese offenbaren alarmierende Zahlen: Auf die offen im Netz stehenden IoT-Systeme fanden allein im ersten Quartal 2019 insgesamt 3.200.000 Angriffe statt! Dabei versuchten die Angreifer in 41.213 Fällen, die ins Netz gestellte Hardware mit Schadprogrammen zu kapern. In 71,44 Prozent aller erfolgreichen Malware-Infektionen identifizierten die AV-TEST-Ingenieure den Mirai-Code als Waffe der Wahl der Angreifer. Zudem fanden häufig Versuche statt, mit Linux-Shell-Befehlen Zugriff auf die SSH/Telnet-Verbindung der Honeypot-Systeme zu erhalten. Dabei wurde meist über automatisierte Angriffe versucht, einen möglichen Kennwortschutz der Geräte zu umgehen. Die am meisten probierten Nutzernamen solcher Versuche waren „root“ und „admin“; Brute-Force-Angriffe auf Passwörter nutzen am häufigsten die Begriffe „admin“ und „default“. Dies zeigt unter anderem, wie wichtig es ist, dass Hersteller von IoT-Produkten bei Installation durch den Kunden den Wechsel von Standard-Passwörtern verlangen!

Die Top 10 der für Angriffe auf die AV-TEST IoT-Honeypots verantwortlichen Ursprungsländer führen übrigens die USA an, gefolgt von den Niederlanden und Deutschland. An vierter Stelle steht China. Russische Hacker belegen derzeit Platz 9.

## TOP 10
## Ursprungsländer Angriffe IoT 2018

| | | |
|---|---|---|
| 1 | US | 1.287.700.195 |
| 2 | NL | 40.048.945 |
| 3 | DE | 15.359.619 |
| 4 | CA | 10.412.092 |
| 5 | ZA | 9.345.064 |
| 6 | GR | 6.894.600 |
| 7 | IN | 5.930.786 |
| 8 | GB | 4.292.386 |
| 9 | RU | 3.680.935 |
| 10 | IT | 2.700.082 |

AV-TEST GmbH überprüft in regelmäßigen Abständen alle marktrelevanten Antiviren-Lösungen für Mac. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/ abgerufen werden.

# 2018: Das Jahr der CRYPTO-MINER

Das aussichtsreiche und nahezu risikolose Geschäftsmodell, auf Kosten Dritter mit Crypto-Minern abzusahnen, entpuppte sich 2018 für Cyberkriminelle als voller Erfolg und hat sich im Vergleich zu anderen Malware-Arten nach extrem kurzer Probephase schnell etabliert. Wie hoch die Bedrohung durch Crypto-Miner einzuschätzen ist, zeigt sich auch daran, dass Browser-Anbieter wie Mozilla Schutzmodule gegen ungewollte Mining-Prozesse implementieren.

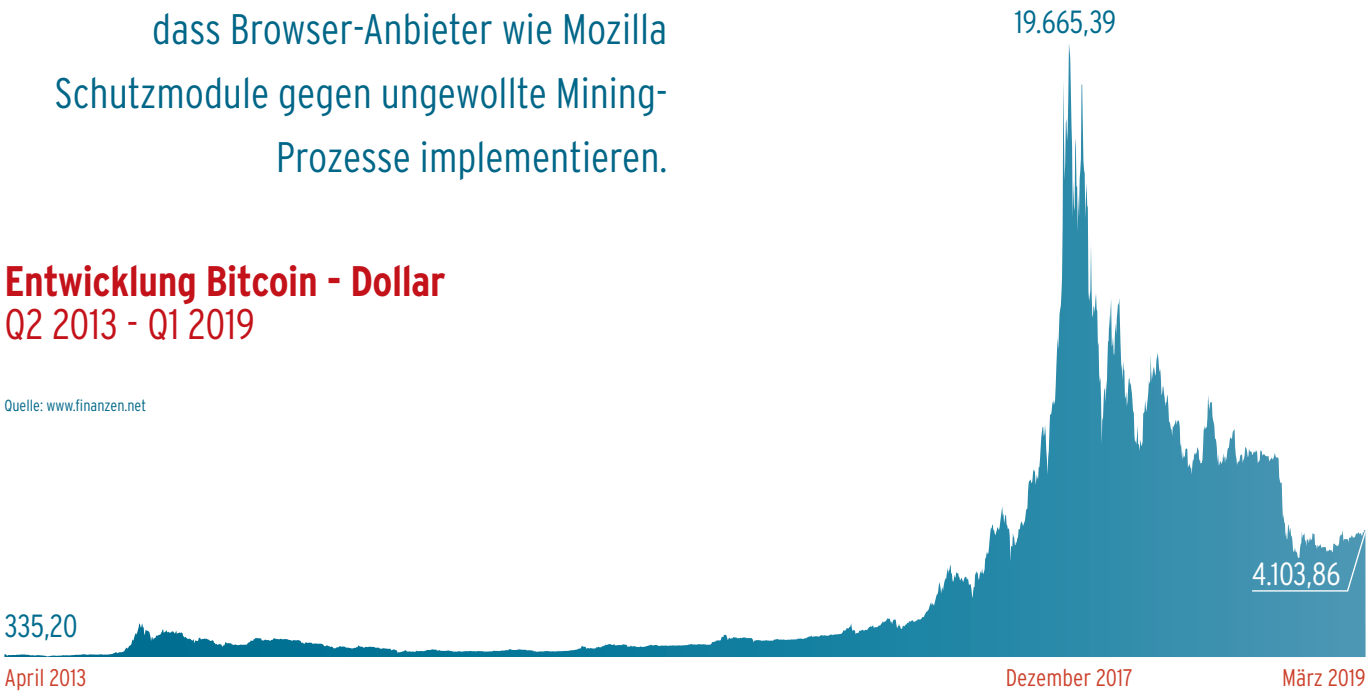
## Auf fremde Kosten reich

Das „Geschäftsmodell" funktioniert folgendermaßen: Die Einen stellen die komplette Infrastruktur zur Verfügung und tragen alle Kosten für Hardware beziehungsweise deren Rechenleistung. Auch auf den Kosten für deren Betrieb, etwa für Energie und Internetbandbreite, bleiben sie sitzen. Die Anderen nutzen dagegen einfach eine Software, die diese Ressourcen zur Berechnung von Kryptowährungen einsetzt und kassieren den kompletten Gewinn für sich selbst. Da bei diesem Geschäftsmodell nur eine Seite gewinnt, während der anderen massiv geschadet wird, beruht es natürlich nicht auf Freiwilligkeit, sondern funktioniert nur, wenn die Opfer von dieser Abzocke nichts mitbekommen.

Der für solch krumme Geschäfte notwendigen Mining-Malware räumte das AV-TEST Institut bereits im 2017er-Sicherheitsreport ein eigenes Kapitel ein, das die Arbeitsweise der Malware ausführlich erklärt (https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2017-2018.pdf). Gegen Ende 2017 erfassten die Systeme von AV-TEST zum ersten Mal Schadprogramme zum Schürfen digitaler Währungen in größerer Konzentration. Als im ersten Quartal des Jahres 2018 die Kurse wesentlicher Kryptowährungen wie Bitcoin, Etherium, Ripple, Monero und Bitcoin Cash zeitweilig auf Hochstände schnellten, zog die Entwicklung illegaler Schürf-Programme schnell nach. Mit Vorlage des letzten Reports in Q1 2018 umfasste die Sammlung von Crypto-Minern bereits über eine Million Schädlinge. Prognose der Sicherheitsexperten: Diese Malware wird sich klar durchsetzen.

**Entwicklung Bitcoin - Dollar**
Q2 2013 - Q1 2019

Quelle: www.finanzen.net

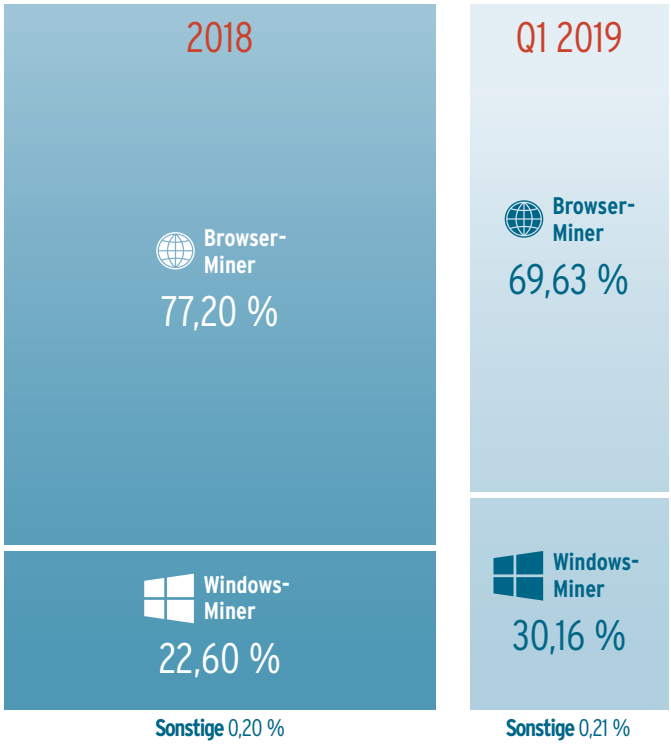


## Crypto-Miner legen stark zu

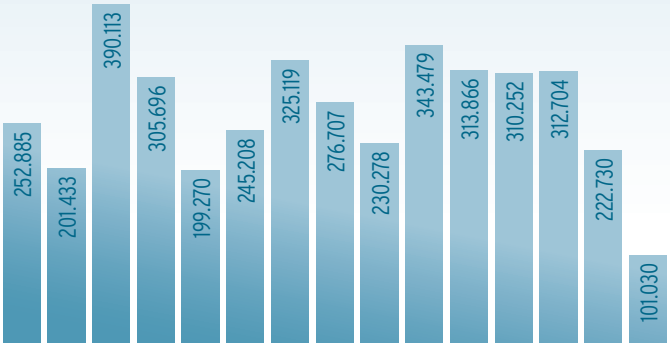
Die Zahlen des aktuell vorliegenden Reports bestätigen diese Einschätzung: Bis Abschluss des ersten Quartals 2019 hat sich die Anzahl an Crypto-Minern mehr als vervierfacht. Die AV-TEST-Datenbank führt bis zur Drucklegung dieses Berichts exakt 4.328.372 unterschiedliche Exemplare dieser Malware-Kategorie für alle gängigen Betriebssysteme!

Bei der Analyse der Entwicklungszahlen neuer Crypto-Miner werden starke Verlagerungen der zum Schürfen von Kryptowährung ausgenutzten Plattformen und Betriebssysteme erkennbar: Während 2017 noch 55 Prozent der Mining-Malware auf Windows-Systemen schürfte und 44 Prozent sich in gängigen Browser festsetzte, zeigte sich im vergangenen Jahr ein komplett anderes Bild. Der Kurs von Windows als Mining-Plattform sank deutlich (auf 22,6 %) und mehr als drei Viertel aller Crypto-Miner nutzten gängige Standard-Browser, um ihre kriminellen Urheber auf fremde Kosten zu bereichern.

## Verteilung Crypto-Miner




## Entwicklung Crypto-Miner gesamt
2018 + Q1 2019




Die Gründe für diese Schwankungen lassen sich bei dieser recht neuen Malware-Gattung nur erahnen. Als betriebssystemunabhängige Standard-Programme stellen Browser für Kriminelle gewiss eine Plattform mit dem größten Verbreitungsgrad für Crypto-Miner dar. Dementsprechend dürfte die Streuung solch hochtechnischer Malware für Browser am effektivsten sein. Ein weiterer Punkt, der für das Ausnutzen von Browsern spricht, ist deren direkte und ständige Internetanbindung. Dies senkt gleichzeitig die Gefahr, von Schutzprogrammen entdeckt zu werden.

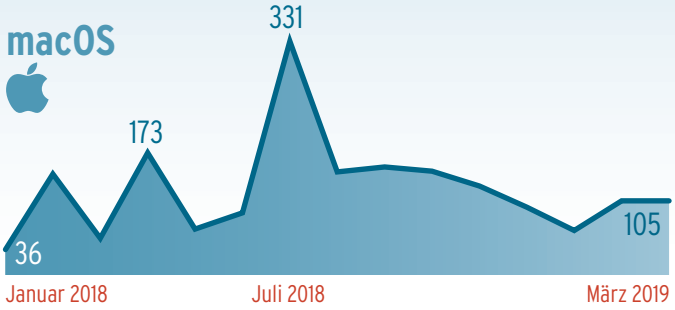
Im Weiteren scheint es bei einem Gesamtvergleich der Entwicklungszahlen neuer Mining-Malware kaum Vergleichswerte zu geben, die die klar vorhandenen Entwicklungsspitzen bei Crypto-Minern für die unterschiedlichen Plattformen erklären. So zeigt etwa die Neuentwicklung von Mining-Malware auf Browser-Basis klare Höchstwerte für den Juni und August des letzten Jahres an, für Linux-Miner im Juni. Windows-Miner fanden dagegen im März des vergangenen Jahres ihren Höhepunkt und bei macOS war im Juli Hauptsaison. Ein Abgleich mit Kursen der unterschiedlichen Kryptowährungen, der allerdings nicht Bestandteil dieser Analyse ist, könnte sicher spannende Ergebnisse zutage fördern.

Neben Browsern und der Microsoft-Plattform nutzen Kriminelle selbstverständlich auch die meisten anderen verfügbaren Systeme aus, wenn auch mit deutlich geringerem Anteil. So erfassten die Erkennungssysteme von AV-TEST 2018 insgesamt 3.323 Miner, die auf Linux-Systeme zielten und sich darum auch gut zum Einsatz auf großen Server sowie auf meist ungeschützter IoT-Hardware eignen (0,1 % der Gesamtsumme). Mit 1.729 neuen Mining-Samples folgte Android an vierter Stelle (0,05 %), danach macOS mit 1.556 neuen Schädlingen. Für Apples mobiles Betriebssystem iOS konnten die Erkennungssysteme von AV-TEST dagegen bisher keinen einzigen Crypto-Miner feststellen.

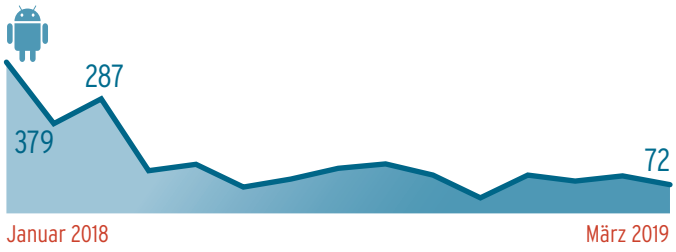
## Entwicklung Crypto-Miner 2018 + Q1 2019

### Windows

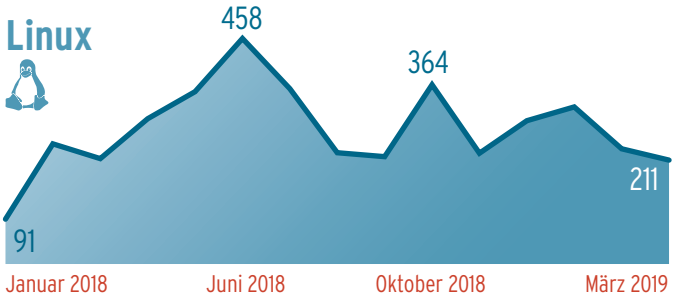

### macOS



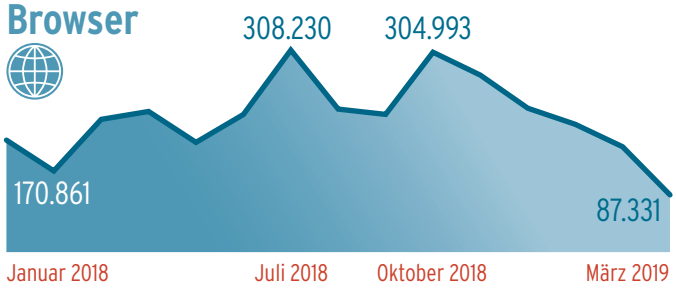

### Android




### Linux




### Browser




# Trend 2019

**Für das erste Quartal 2019 melden die Erfassungssysteme von AV-TEST einen moderaten Rückgang der Neuentwicklung von Mining-Malware, was insbesondere an einem Rückgang der dominierenden Browser-Malware liegt. Dementsprechend steigt der Anteil von Windows-Minern von 22,6 auf 30,16 Prozent. Allerdings sind diese Trends mit Vorsicht zu genießen. Zum einen ist das Forschungsfeld der Crypto-Miner noch recht neu. Zum anderen zeigte diese Art von Malware bisher, ähnlich wie die ausgemachten Ziele Kryptowährungen selbst, ebenfalls extreme Kursschwankungen.**

# Sicherheitsstatus INTERNET-GEFAHREN

Der Ausgangspunkt nahezu jeder Malware-Attacke hat seinen Ursprung online. Meist reisen Schadprogramme in groß angelegten Spam-Wellen von Kontinent zu Kontinent. Doch auch Drive-by-Downloads über infizierte Websites, Massenverbreitung infizierter Apps sowie automatisierte Brute-Force-Attacken auf ungeschützte IoT-Geräte gehören zu den Malware-Verbreitungskanälen von Cyberkriminellen. AV-TEST bündelt jetzt einen Großteil seiner Messungen und weltweit einzigartigen Analysedaten des Instituts in seinem neuen Onlineportal „AV-atlas". Das System informiert nicht nur in Echtzeit über das Malware-Aufkommen, sondern durchleuchtet auch Quellen und Ursprünge und ermöglicht Malware-Monitoring auf dem neuesten Stand der Technik.

## Verseuchte Massen-Mails

Einer der Hauptinfektionswege zur Verbreitung von Malware ist und bleibt der Versand von E-Mails. Es kann sich dabei um gezielte Spear-Phishing-Angriffe auf bestimmte Opfer handeln, deren Verhalten etwa auf Social Media-Plattformen lange im Voraus in Erfahrung gebracht wurde. Oder es kann sich um weit gestreute Massen-Mail-Kampagnen handeln, die Kontodaten abfragen, verseuchte Dateien im Anhang transportieren oder auch über einen interessanten Link massenhaft Opfer auf verseuchte Websites lotsen. Zum Abschlusszeitpunkt dieses Reports waren 77,6 Prozent aller mit Malware infizierten Websites, auf die in Spam-Mails verwiesen wurde, unter der Top-Level-Domain (TLD) „COM" registriert. Danach folgten „ORG" (4,7 %) und „NET" (3,2 %). Als erste länderspezifische TLD folgt die Kennung „ME" der kleinen südeuropäischen Republik Montenegro.

Diese Websites übermittelten nach Aufruf im Browser infizierte Datenpakete. Am häufigsten kam dabei das HTML-Format zum Einsatz. In 21,1 Prozent der Fälle brachten die infizierten Websites ihren Malware-Code im Format der Web-Programmiersprache in Umlauf. Danach folgt mit deutlichem Abstand das gängige Komprimierungsformat ZIP (2,6 %) und erst dann ausführbare Dateiformate mit der Endung EXE (2,3 %).

### TOP 10
### Gefährliche Top Level Domains 2018

| | | |
|---|---|---|
| 1 | COM | 77,6 % |
| 2 | ORG | 4,7 % |
| 3 | NET | 3,2 % |
| 4 | ME | 2,8 % |
| 5 | ID | 2,8 % |
| 6 | TO | 2,3 % |
| 7 | TV | 2,2 % |
| 8 | LV | 1,7 % |
| 9 | PL | 1,7 % |
| 10 | TIPS | 1,2 % |

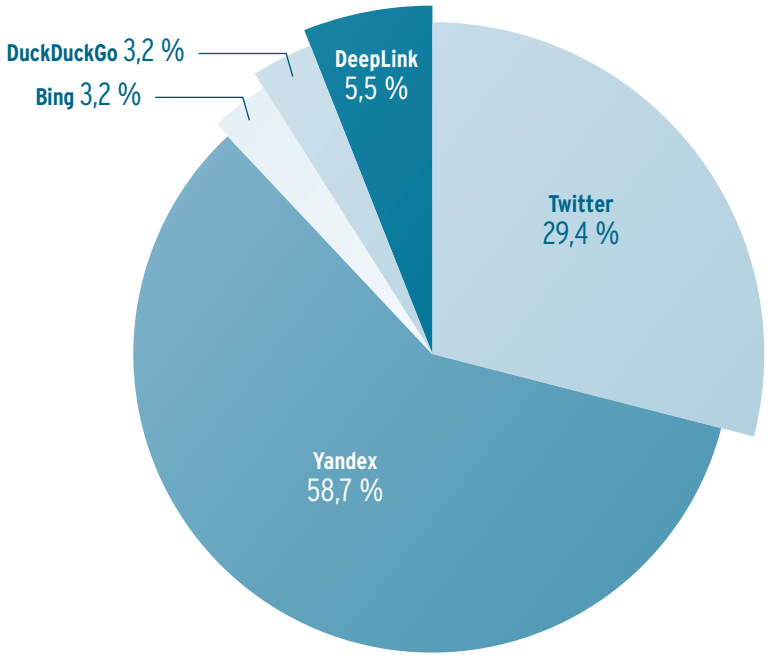
## Malvertising über Suchmaschinen

Im Rahmen des sogenannten Malvertising mieten Kriminelle auf Suchmaschinen trendende Domains mit möglichst gleichlautenden Begriffen in der URL an und bewerben die verseuchten Websites gleichermaßen über Suchmaschinen. Das AV-TEST Institut überprüft zu diesem Zweck gängige Suchmaschinen auf Verlinkungen zu infizierten Websites. Mit über der Hälfte aller infizierten Websites (58,7 %) erwies sich die russische Suchmaschine Yandex am anfälligsten für die Verbreitung von Links zu Malware-infizierten Websites. Mit 29,4 Prozent folgte der US-amerikanische Mikrobloggingdienst Twitter, über den Kriminelle ebenfalls im großen Stil auf trendende Themen aufspringen, um über massentaugliche Tweets möglichst viele Opfer auf im Tweet verlinkte Websites zu lotsen. Diese beiden Dienste rangieren im Kurs von Cyberkriminellen mit weitem Abstand vor alternativen Webdiensten, wie etwa DuckDuckGo (3,2 %). Microsofts Suchmaschine Bing rangiert an fünfter Stelle (3,2 %), Google spielt in diesem Vergleich aufgrund zu geringer Zahlenwerte gar keine Rolle.

## TOP 10 Malware Payloads 2018

| | | |
|---|---|---|
| 1 | NO EXTENSION | 71,4 % |
| 2 | HTML | 21,1 % |
| 3 | ZIP | 2,6 % |
| 4 | EXE | 2,3 % |
| 5 | PHP | 1,4 % |
| 6 | RAR | 0,6 % |
| 7 | HTM | 0,3 % |
| 8 | ASP | 0,2 % |
| 9 | KZJV | < 0,1 % |
| 10 | JPG | < 0,1 % |

## Gefährliche URLs nach Quellen 2018



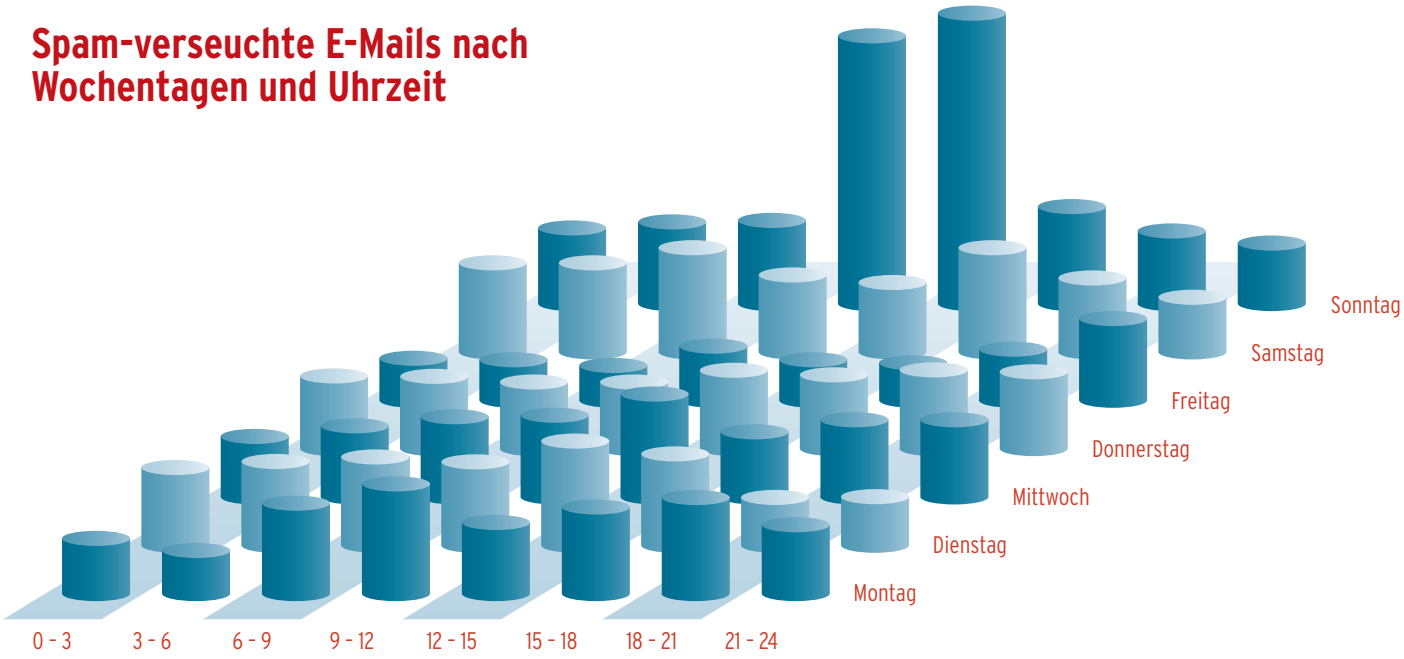
## Die Spam Top 10

Zu den größten Spam-Versendern gehörte 2018 auf Platz 1 Brasilien. Das südamerikanische Land verursachte über 14 Prozent des weltweiten Gesamtaufkommens unerwünschter Massen-E-Mails. Dicht gefolgt von der Russischen Föderation, die nur 0,3 Prozentpunkte hinter Brasilien lag. An Stelle drei folgte Japan, mit knapp zehn Prozent des Welt-Spam-Aufkommens. Die meisten verseuchten E-Mails kommen übrigens laut Erfassung durch AV-atlas an Sonntagen in der Vormittags- und Mittagszeit (MEZ) an.

## TOP 10 Spamversender 2018

| | | |
|---|---|---|
| 1 | BRASILIEN | 14,6 % |
| 2 | RUSSISCHE FÖDERATION | 14,3 % |
| 3 | JAPAN | 9,5 % |
| 4 | UKRAINE | 5,3 % |
| 5 | VEREINIGTE STAATEN VON AMERIKA | 5,2 % |
| 6 | INDIEN | 4,6 % |
| 7 | INDONESIEN | 4,5 % |
| 8 | BANGLADESCH | 3,6 % |
| 9 | CHINA | 2,8 % |
| 10 | KOLUMBIEN | 2,2 % |

## Spam-verseuchte E-Mails nach Wochentagen und Uhrzeit




AV-TEST GmbH überprüft regelmäßig alle relevanten Schutzlösungen auf Internetgefahren. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/ abgerufen werden.

# Teststatistiken

Mit selbstentwickelten Analysesystemen und ausgeklügelten Testverfahren garantiert AV-TEST unabhängige Prüfungen für IT-Sicherheitsprodukte und ist so seit über 15 Jahren das führende Institut im Bereich Sicherheitsforschung und Produktzertifizierung.

## Millionen Malware-Samples für Ihre Sicherheit

Mehr als 3 Millionen Dateien scannen die Systeme von AV-TEST pro Tag, darunter ein einzigartiges Multi-Virenscanner-System zur Malware-Analyse für die Plattformen Windows und Android. Ein Verbund aus über 25 einzelnen Virenscannern liefert anhand dieser Ergebnisse eine vollautomatisierte Mustererkennung und analysiert und klassifiziert auf diese Weise Malware. Sämtliche proaktiven Erkennungen sowie die Reaktionszeiten der jeweiligen Hersteller auf neue Bedrohungen erfasst das System automatisiert.
So erweitert sich eine der weltweit größten Datenbanken für Schadprogramme ständig. Ihr Datenbestand wächst seit über 15 Jahren kontinuierlich auf über 40 Servern mit einer Speicherkapazität von mehr als 2.500 Terabyte. Zum Veröffentlichungsdatum dieses Jahresreports beinhaltete die AV-TEST Datenbank über 900 Millionen Schadprogramme für Windows und über 28 Millionen Schädlinge für Android!

## AV-TEST Qualitätssiegel für Antiviren-Produkte

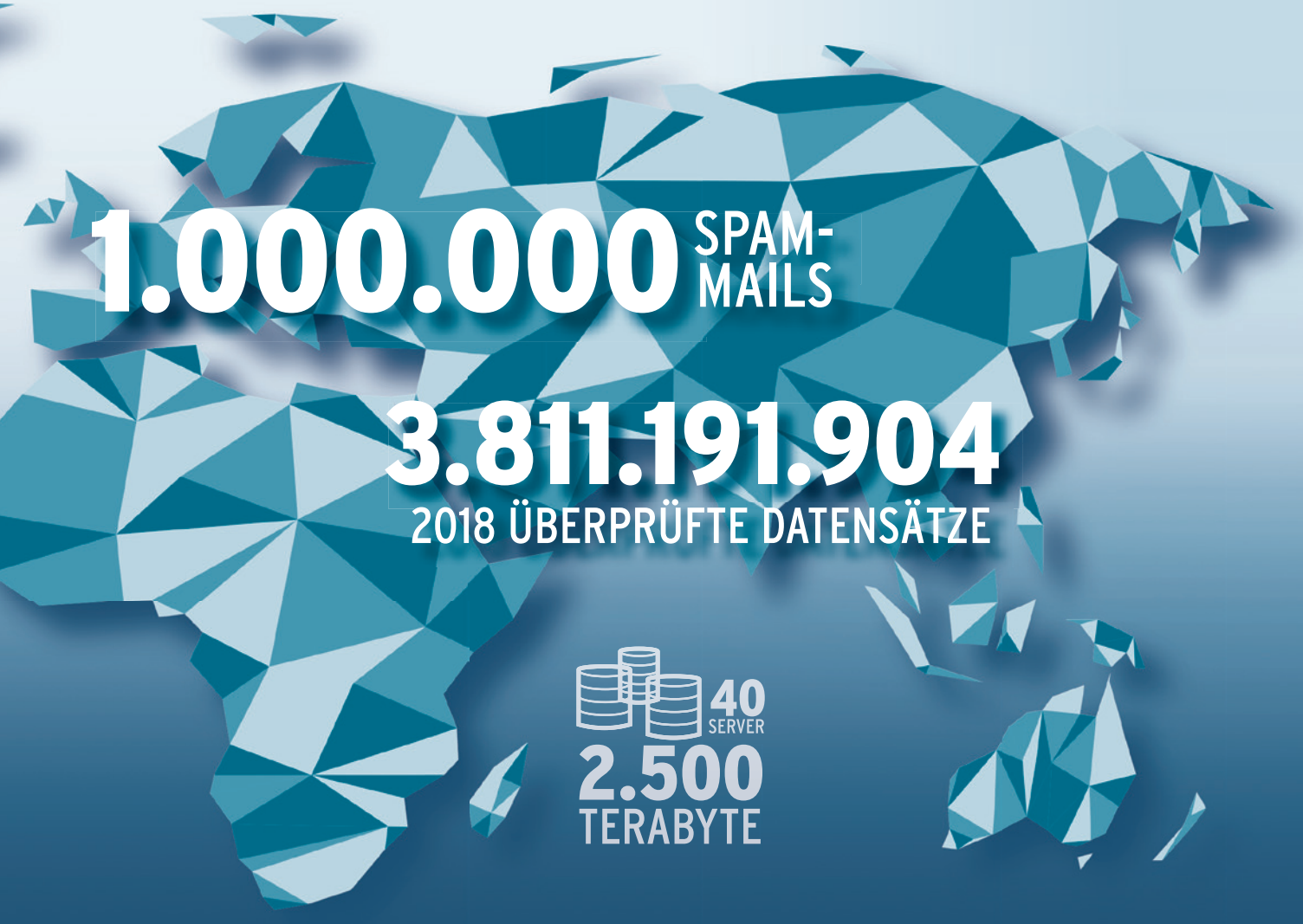




## AV-TEST Qualitätssiegel für IoT-Produkte


Zur gezielten Malware-Analyse bringt AV-TEST selbstentwickelte Systeme zum Einsatz. Diese Analysesysteme ermöglichen das kontrollierte Ausführen potenziellen Schadcodes auf sauberen Testsystemen und erfassen daraus resultierende Systemveränderungen sowie entstehenden Netzwerkverkehr. Basierend auf diesen Analysen wird Malware zur weiteren Verarbeitung klassifiziert und kategorisiert. Auf diese Weise erfassen und prüfen die AV-TEST Systeme Tag für Tag 1.000.000 Spam-Mails, 500.000 URLs, 500.000 potenziell bösartige Dateien, 100.000 harmlose Windows-Dateien sowie 30.000 Android-Apps.

Die von den AV-TEST Systemen erfassten Daten werden unter anderem für die monatlichen Tests von Sicherheitsprodukten für Windows eingesetzt. 2018 wurden so über 315 Produkttests allein für Privatanwender- und Unternehmensprodukte durchgeführt. Dabei wurden pro Produkt 78.121 Malware-Attacken gefahren sowie 9.026.094 einzelne Datensätze für Fehlalarmtests eingesetzt und ausgewertet. Im gesamten Jahr 2018 waren das 3.811.191.904 von den Testexperten zu überprüfende Datensätze. In den monatlichen Android-Tests überprüften die Tester über das Jahr insgesamt 123 Produkte. Dabei musste sich jede überprüfte Sicherheits-App gegen 72.818 spezielle Android-Schädlinge zur Wehr setzen. Zur Gegenprobe erfassten die Experten zudem über 34.516 Scans sicherer Apps pro Produkt, um die Anfälligkeit für Fehlalarme zu überprüfen. Im Labor wurden in Tests von Sicherheitsprodukten für Android also allein 7.700.742 Scan-Vorgänge analysiert und reproduzierbar ausgewertet. 5.035.258 Scans entfielen hierbei auf das speziell entwickelte Android-Security-Cluster, das parallele Echtzeittests von Android-Security-Lösungen ermöglicht.

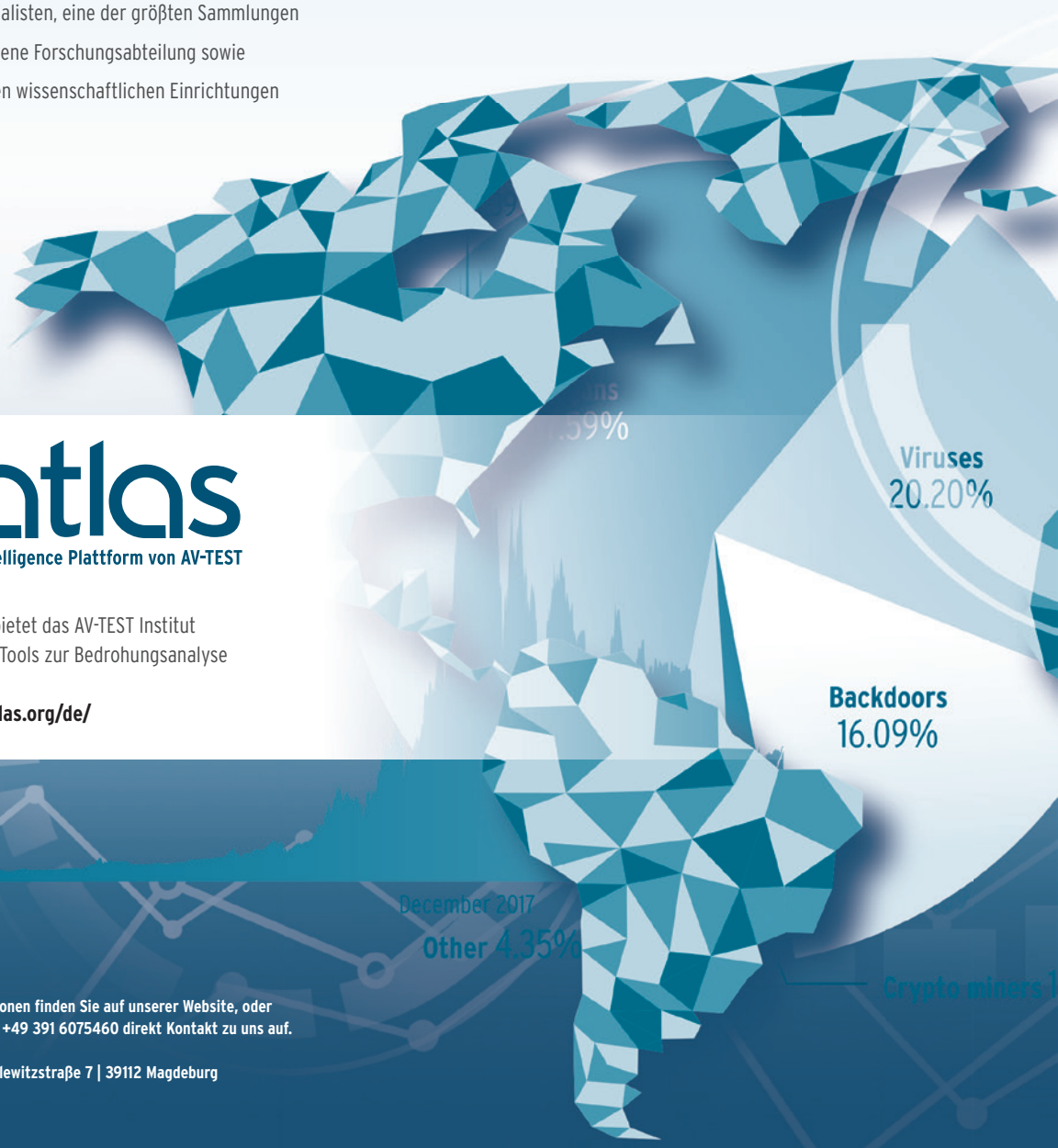


# Über das **AV-TEST Institut**

Die AV-TEST GmbH ist das unabhängige Forschungsinstitut für IT-Sicherheit aus Deutschland. Seit mehr als 10 Jahren garantieren die Sicherheitsexperten aus Magdeburg qualitätssichernde Vergleichs- und Einzeltests von nahezu allen international relevanten IT-Sicherheitsprodukten. Dabei arbeitet das Institut absolut transparent und stellt der Öffentlichkeit regelmäßig neueste Tests und aktuelle Forschungsergebnisse unentgeltlich auf der Website zur Verfügung. AV-TEST hilft damit Herstellern bei der Produktoptimierung, unterstützt Presseorgane bei Publikationen und berät Nutzer bei der Produktauswahl. Zudem hilft das Institut Branchenverbänden, Unternehmen und staatlichen Einrichtungen in Fragen der IT-Sicherheit und entwickelt für sie Sicherheitskonzepte.

Über 30 ausgewählte Sicherheitsspezialisten, eine der größten Sammlungen digitaler Schädlinge weltweit, eine eigene Forschungsabteilung sowie intensive Zusammenarbeit mit anderen wissenschaftlichen Einrichtungen gewährleisten Tests auf international anerkanntem Niveau und letztem Stand der Technik. AV-TEST nutzt für Tests selbst entwickelte Analysesysteme und garantiert so von Dritten unbeeinflusste und jederzeit reproduzierbare Testergebnisse für alle gängigen Betriebssysteme und Plattformen.

Dank langjähriger Expertise, intensiver Forschung und ständig aktualisierten Laborumgebungen gewährleistet AV-TEST höchste Qualitätsstandards getesteter und zertifizierter IT-Sicherheitsprodukte. Außer in der klassischen Viren-Forschung arbeitet AV-TEST außerdem auf den Gebieten der Sicherheit von IoT- und eHealth-Produkten, Anwendungen für Mobilgeräte sowie in dem Bereich Datenschutz von Anwendungen und Dienstleistungen.




AV-atlas

**Die Threat Intelligence Plattform von AV-TEST**

Mit AV-ATLAS bietet das AV-TEST Institut umfangreiche Tools zur Bedrohungsanalyse in Echtzeit.
**https://av-atlas.org/de/**

**Weitere Informationen finden Sie auf unserer Website, oder nehmen Sie unter +49 391 6075460 direkt Kontakt zu uns auf.**

**AV-TEST GmbH | Klewitzstraße 7 | 39112 Magdeburg**