ZAHLEN UND FAKTEN

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

SECURITY REPORT 2019/2020

Der AV-TEST Sicherheitsreport

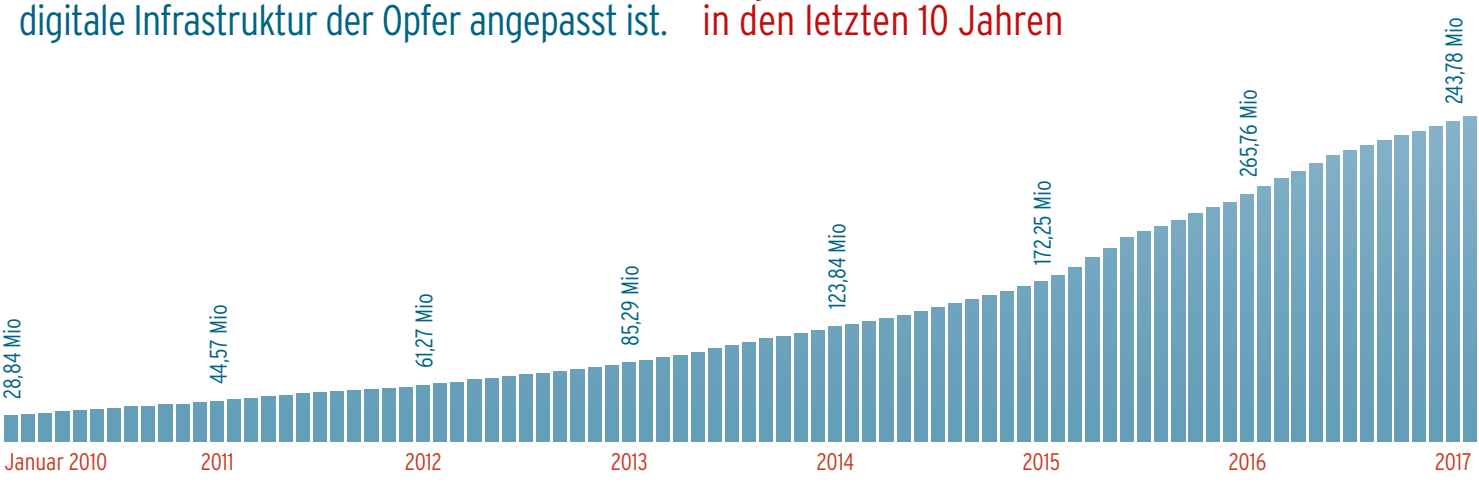
Wie die Auswertungen der Malware-Zahlen der Erfassungssysteme des AV-TEST Instituts belegen, zeigt das vergangene Jahr einen neuen Trend in der Malware-Industrie, der sich im 1. Quartal 2020 klar fortsetzt. Die Entwicklung von Malware teilt sich in zwei Bereiche auf: Während auf der einen Seite die automatisierte Produktion von Massen-Malware für breit angelegte Online-Attacken weiter stark anwächst, entwickeln Cyber-kriminelle auf der anderen Seite zunehmend ausgeklügelte Malware für spezialisierte Attacken. Dabei kommt eine Kombination speziell entwickelter Angriffswerkzeuge zum Einsatz, die genau auf die vorher erkundete digitale Infrastruktur der Opfer angepasst ist.

Massen-Malware mit massiver Steigerungsrate

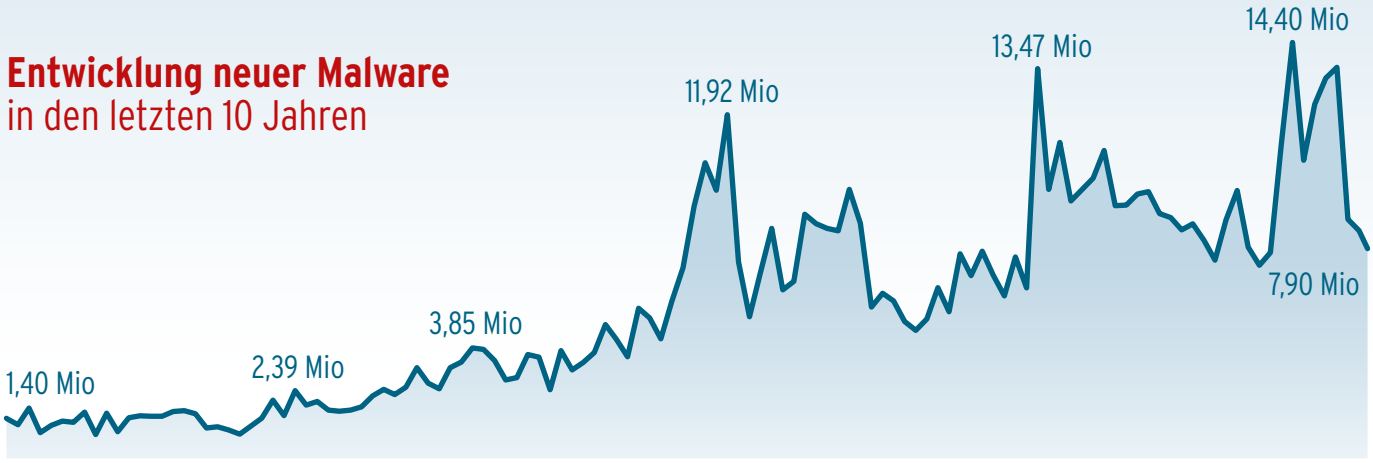
2019 brachte der Einsatz von Massen-Malware, also automatisiert erstellten Schadprogrammen, Cyberkriminellen erhebliche Gewinne. Dementsprechend stieg die Rate dieser meist in großen Kampagnen per Mail und über das Internet verteilten Malware weiter stark an. Mit mehr als 114 Millionen (114.312.703) neu entwickelter Schadprogramme durchbrach die Malware-Industrie 2019 erneut eine Schallmauer und war damit so aktiv, wie nie zuvor. Bis dato hatten die Erfassungssysteme des AV-TEST Instituts das Jahr 2018 mit über 105 Millionen neu entwickelter Samples als das aktivste Jahr krimineller Akteure verzeichnet.

Die Analyse der aktuellen Erfassungszahlen für das erste Quartal 2020 verheißt auch für dieses Jahr deutliche Zuwachsraten beim Einsatz von Massen-Malware: Bereits im ersten Quartal des laufenden Jahres verzeichnen die AV-TEST Systeme rund 43 Millionen neu programmierte Samples. Bis Ende 2020 ist dementsprechend mit einer Explosion der Entwicklung neuer Schadprogramme zu rechnen, die sich bei über 160 Millionen Samples für das gesamte Jahr einpendeln könnte – und damit eine neue Dimension erreicht. In der Langzeitbetrachtung des AV-TEST Instituts zeigt sich die Malware-Industrie damit aktiver als je zuvor und wird voraussichtlich im Laufe des Jahres die Grenze von insgesamt 700 Millionen bekannten Schadprogrammen überschreiten. Damit könnte die Bedrohungslage durch Massen-Malware 2020 einen neuen gefährlichen Höhepunkt erreichen. Aktuell liegt die Entwicklungsrate neuer Malware bei 4,2 Samples pro Sekunde!

Entwicklung Malware insgesamt in den letzten 10 Jahren

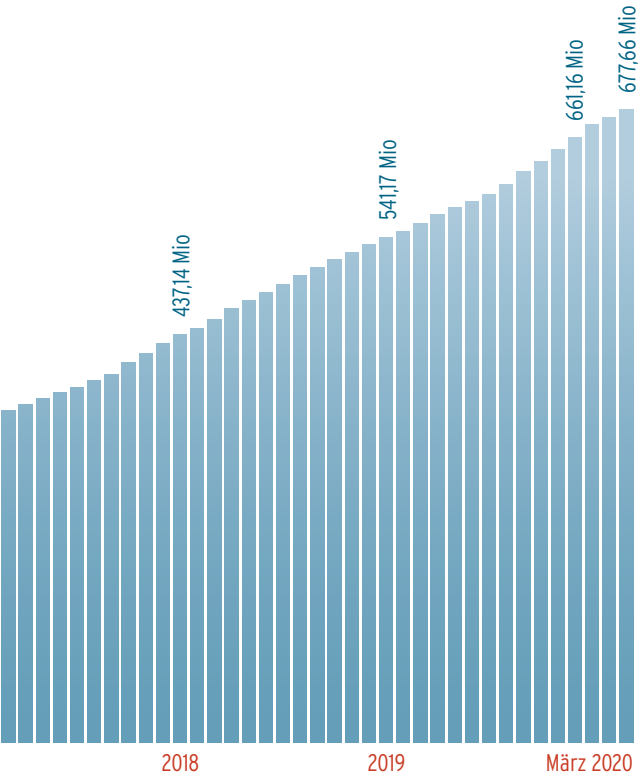


Entwicklung neuer Malware
in den letzten 10 Jahren



Steigende Erkennungsraten erhöhen Entwicklungsdruck

Ein Anlass für diese dramatische Entwicklung kann als positiv angesehen werden, denn die massenhafte Entwicklung neuer Malware-Samples ist unter anderem durch den hohen Schutzgrad aktueller Sicherheitsprodukte zu erklären. Das gilt insbesondere für Schutzlösungen für Windows-Systeme. Denn nach wie vor zielt der Großteil aller Schadprogramme auf das Betriebssystem, das weltweit mit Abstand am häufigsten zum Einsatz kommt. 2019 galten über 78 Prozent der von Cyberkriminellen neu entwickelten Schadcodes Windows-Systemen. Im ersten Quartal 2020 steigert sich dieser Wert weiter auf über 83 Prozent.



Unternehmer, wenn auch getrieben von einem eindeutig kriminellen Hintergrund, lockt der hohe Verbreitungsgrad des Redmonder Betriebssystems. Darüber hinaus sind Windows-Systeme offenkundig aber auch weiterhin noch nicht ausreichend gut geschützt, um für Kriminelle als Angriffsziel unattraktiv zu werden. Und so entwickeln sie im industriellen Stil Massen-Malware für internetangebundene Systeme, deren Schutzmechanismen nicht auf dem letzten Stand der Abwehrtechnik sind. Die Anzahl aller erfassten und analysierten Schadprogramme für Windows lag bei Drucklegung dieses Reports bei 517.465.709 Samples.
Genaue Zahlen und Analysen zur Bedrohungslage von Windows-Systemen finden Sie ab Seite 8.

AV-ATLAS: die Threat Intelligence Platform von AV-TEST

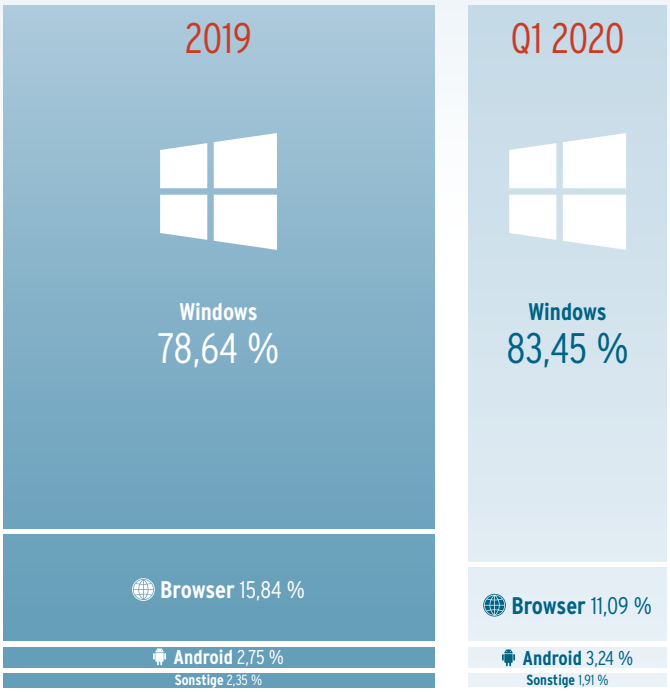
2019 startete AV-TEST seine Threat Intelligence Platform AV-ATLAS (av-atlas.org). Im Zuge dieser Entwicklung erfolgte auch die messtechnische Kalibrierung der institutseigenen Erfassungssysteme. Ein solcher Schritt erlaubt nicht nur die noch genauere Analyse von Malware-Samples, verhindert Dopplungen und False-Positives, sondern ermöglicht auch rückwirkend eine Anpassung der Erfassungszahlen nach dem neuesten Stand der Technik an. Damit ergeben sich gegebenenfalls Abweichungen gegenüber in vorherigen Sicherheitsreports veröffentlichten Erfassungszahlen. Mit AV-ATLAS bietet Ihnen das AV-TEST Institut ständig neue Statistiken und Auswertungen zur aktuellen Bedrohungssituation.

Android- und MacOS-Systeme oft noch ohne Schutz

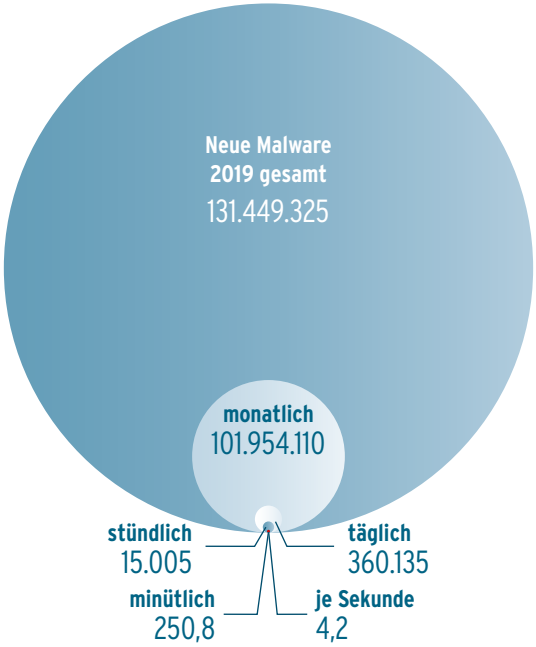
Einen leichten Rückgang der Rate neuentwickelter Malware verzeichneten die AV-TEST Systeme beim meistverbreiteten mobilen Betriebssystem von Google. Den Höchststand an Malware-Zuwächsen erreichte das Betriebssystem mit 6.201.358 neu programmierten Samples im Jahr 2017. Seither sinkt die Anzahl neuer Android-Malware und erreichte 2019 mit 3.170.140 den geringsten Stand seit drei Jahren. Auch wenn diese Entwicklung im Grunde erfreulich ist, bedeuten fallende Malware-Zahlen nicht automatisch eine abgeschwächte Bedrohungslage für Nutzer von Android-Geräten. Zudem zeigt die Entwicklung des ersten Quartals dieses Jahres bereits wieder steigende Malware-Trends für Android.

Auch für MacOS wiesen die Erfassungssysteme von AV-TEST in 2019 sinkende, wenn auch weiterhin hohe Malware-Zahlen aus. Während das Vorjahr mit über 90.000 neu programmierten Schadprogrammen einen unübersehbaren Meilenstein in der Entwicklungsgeschichte von MacOS-Malware setzte, halbierte sich die Anzahl der Neuentwicklungen im Folgejahr annähernd und blieb unter der 60.000-Marke. Den Zahlen des ersten Quartals dieses Jahres folgend, ist von einem weiteren Rückgang neuer Mac-Malware auszugehen. Zumindest statistisch dürfte sich die Anzahl neuer Schädlinge für Apple-Rechner gegen Jahresende bei etwa 40.000 neuen Samples einpendeln.

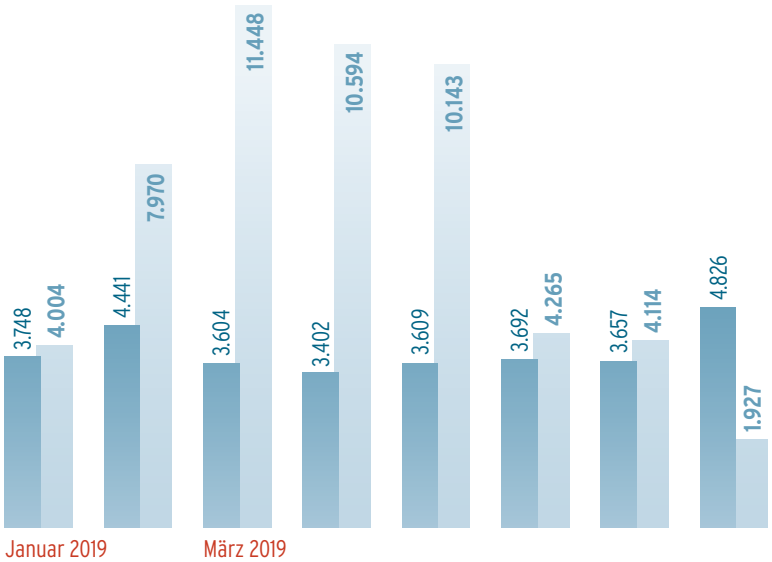
Malware-Erkennung nach Plattform



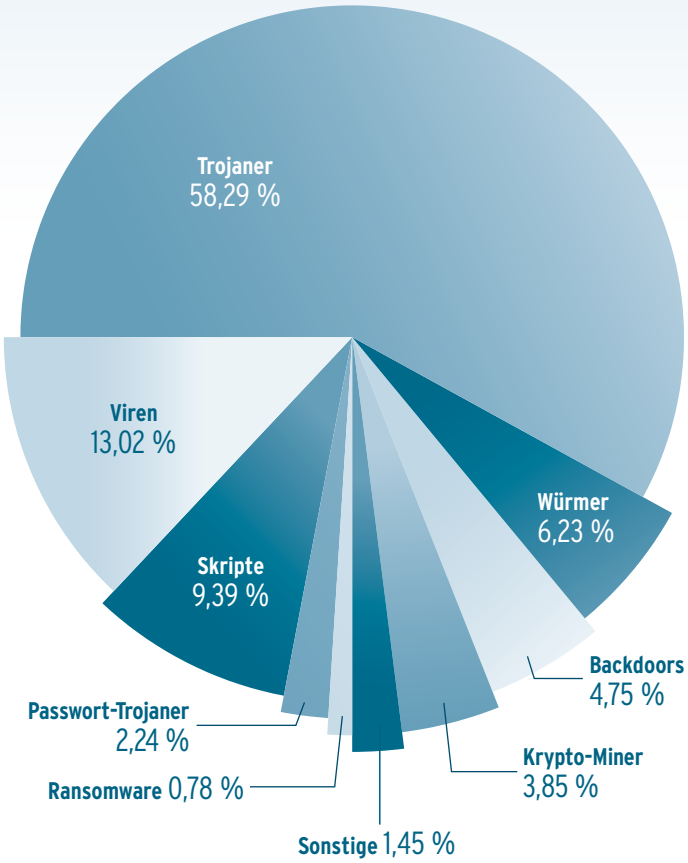
Durchschnittliche Bedrohungslage durch neue Malware 2019



MacOS: Verhältnis Malware/PUA 2019 + Q1 2020



Malware-Verteilung gesamt 2019

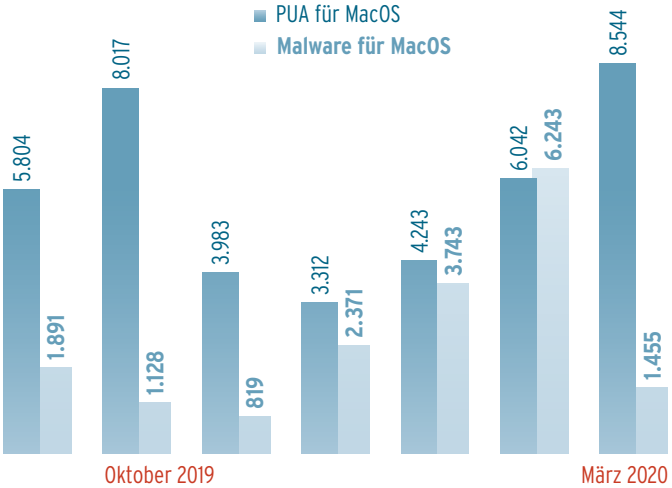


Allerdings sind sowohl diese Schätzungen als auch fallende Malware-Zahlen insgesamt mit Vorsicht zu bewerten, denn sie sind nicht automatisch einer abgeschwächten Bedrohungslage gleichzusetzen. Beide Betriebssysteme, sowohl Googles Mobilsystem Android als auch Apples MacOS, zeichnen sich im Vergleich zu Windows im negativen Sinne dadurch aus, dass die eingesetzten Endgeräte weitestgehend ohne effektive Schutz-Software genutzt werden. Dabei, das zeigen die regelmäßigen Prüfungen des AV-TEST Instituts, gibt es eine Vielzahl oft sogar kostenloser Apps und Antiviren-Lösungen für beide Systeme, mit denen sich ein ordentliches Sicherheitslevel erreichen ließe.

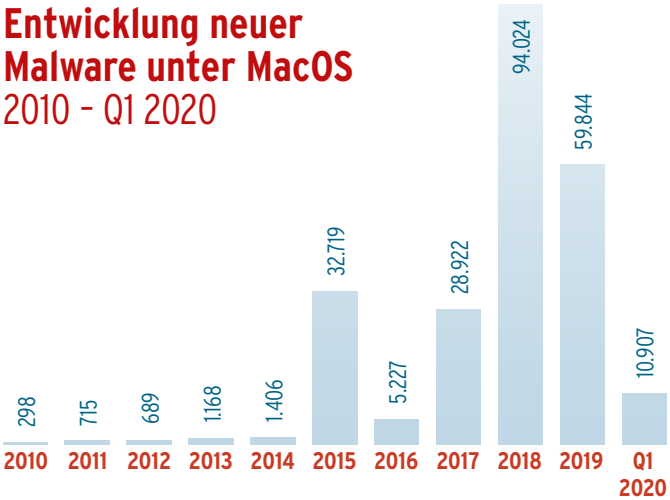
Genauere Analysen zur Bedrohungslage für Android-Geräte finden Sie in diesem Report ab Seite 12, für Geräte unter MacOS ab Seite 16.

Trojaner: die Allzweckwaffe

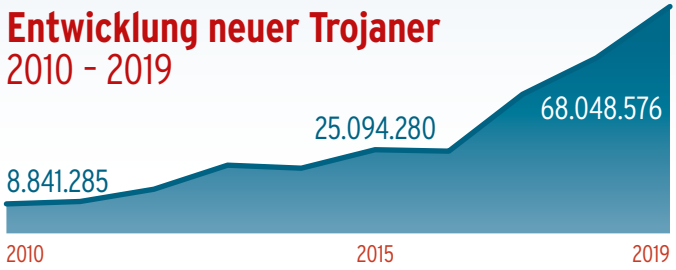
Mit über 58 Prozent Anteil des Malware-Aufkommens für alle Betriebssysteme zeigten sich auch im letzten Jahr Trojaner als das Mittel der Wahl von Cyber-kriminellen. Das ist nicht weiter verwunderlich: Diese Malware-Kategorie entert Zielgeräte über nahezu alle verfügbaren digitalen Kanäle. Trojaner lassen sich beim bloßen Besuch infizierter Websites übertragen, reisen gut versteckt in großen Spam-Wellen per E-Mail, lauern in harmlos erscheinenden Software- und App-Downloads, stecken in angeblichen Musik- und Filmdateien. Doch sie können auch äußerst präzise in Systeme von potentiellen Opfern eingebracht werden, etwa über QR-Code-Aufrufe oder als Köder ausgelegte Speichermedien, wie etwa angeblich verlorene USB-Sticks.



Entwicklung neuer Malware unter MacOS 2010 – Q1 2020



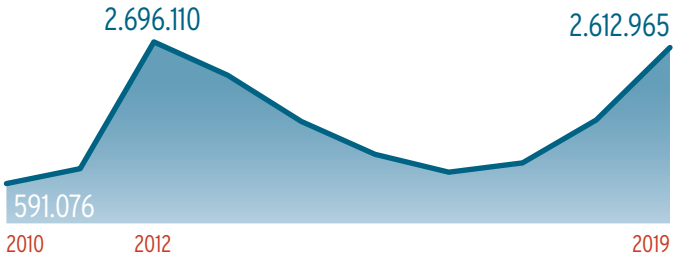
Entwicklung neuer Trojaner
2010 - 2019



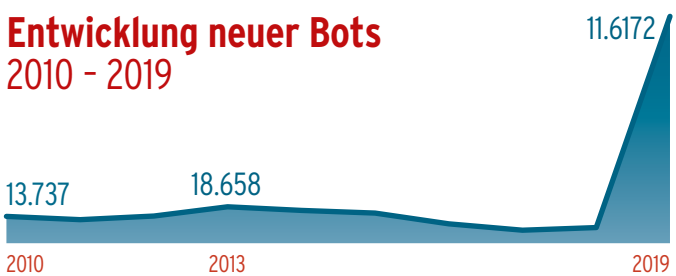
Entwicklung neuer Ransomware
2010 - 2019

Entwicklung neuer Krypto-Miner
2010 - 2019

Entwicklung neuer Passwort-Trojaner
2010 - 2019



Entwicklung neuer Bots
2010 - 2019



Neben den umfangreichen Schadfunktionen, die Trojaner enthalten, können sie darüber hinaus nahezu jeden beliebigen Schadcode auf gekaperte Systeme nachladen und bilden darum häufig nur die erste Welle eines Angriffs. Sind ausreichend Systeme infiziert, laden Cyberkriminelle spezialisierteren Schadcode nach. Abhängig vom kriminellen Geschäftsmodell der Angreifer kann es sich dabei um Ransomware zur Erpressung von Nutzern, um Bots und Krypto-Miner zum missbräuchlichen Einsatz gekaperter Rechenleistung und Bandbreite oder diverse andere Schadfunktionen handeln. Dieses Business Model hat sich 2019 offensichtlich so bewährt, dass die Cybermafia den Einsatz massenhaft verbreiteter Trojaner im ersten Quartal dieses Jahres weiter steigerte, so dass die aktuelle Trojaner-Quote bei 66,82 Prozent liegt.

Wachstumsmarkt Ransomware

Als weitere lukrative Einnahmequelle erwies sich im letzten Jahr die Schutzgelderpressung durch Ransomware. Die Entwicklung dieser Malware verdreifachte sich 2019 im Vergleich zum Vorjahr und erreichte den bisherigen Höchststand von über 900.000 Samples. Gleiches gilt für die rasant zunehmende Zahl an Krypto-Minern. Das illegale Schürfen von Onlinewährungen auf Kosten der Besitzer mit solcher Spezial-Malware infizierter Systeme, hat sich offensichtlich als lukrative Einnahmequelle erwiesen. Diese Entwicklung hatte der letzte Sicherheitsreport des AV-TEST Instituts bereits vorausgesehen.

Angriffe folgen ökonomischen Gesetzen

Wie zu Beginn des Reports erwähnt, richtet sich der Großteil der per Malware geführten Angriffe gegen Microsoft-Systeme. Damit handeln Cyberkriminelle rein ökonomisch. Denn neben der Verbreitung eines Zielsystems und dem folglich zu erwartenden Gewinn spielt natürlich auch die Angreifbarkeit eine wichtige Rolle in den wirtschaftlichen Erwägungen der Malware-Industrie. Und so zeigt ein Blick auf gefundene und veröffentlichte Schwachstellen unterschiedlicher Hersteller, wie auch in den Auswertungen des Online-dienstes CVE Details erkennbar, dass Microsoft in diesem Punkt das mit Abstand lukrativste Ziel darstellt. Zwar liegen Android und Debian mit der Anzahl der im letzten Jahr entdeckten Sicherheitslücken bei Produkten auf den Plätzen eins und zwei. Doch auf Platz drei folgt bereits ein Windows-System, und in den Top 20 gesellen sich noch weitere sieben hinzu. Insgesamt

gesehen erlangte Microsoft somit im Jahr 2019 den zweifelhaften Ruhm, auf Platz eins der Hersteller mit den meisten bekannten Sicherheitslecks zu stehen. Solche Zahlen interessieren selbstverständlich auch Kriminelle, die mit der Entwicklung von Massen-Malware ihr Geld verdienen.

APT: Trend zu zielgerichteten Angriffen

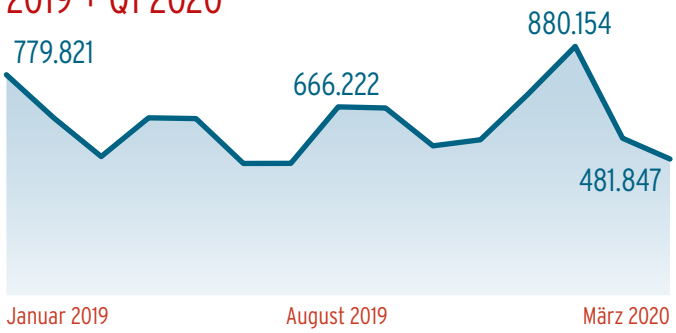
Die massive Zunahme von gezielten Attacken mittels Advanced Persistent Threats (APTs) ist aus verschiedenen Gründen kaum zu quantifizieren: Zum einen werden derart taktische Angriffe von langer Hand strategisch vorbereitet und gezielt gegen Unternehmen und Organisationen geführt, die extrem wertvolle Informationen verwalten. Zum anderen dringen solche meist von staatlich organisierten Angreifern gegen Ministerien, Forschungs- und Produktionsstätten sowie Finanzunternehmen und andere Institutionen eines Landes gerichtete Angriffe selten an die Öffentlichkeit. Fakt ist jedoch, dass insbesondere Unternehmen sich zunehmend gegen zielgerichtete Attacken auf ihre digitale Infrastruktur zur Wehr setzen müssen. Untermauert wird dies unter anderem seit 2006 durch Auflistungen in der Datenbank des Center for Strategic & International Studies (CSIS). Das AV-TEST Institut reagiert auf die Zunahme bereits bekannter APT-Attacken mit einem an den MITRE-Standard angelehnten Test- und Zertifizierungsprogramm von Sicherheitslösungen. Informationen zu den Tests zur Überprüfung der Abwehrfähigkeit gegenüber APT-Attacken finden Sie auf unserer Website.

PUA: unerwünscht, doch weit verbreitet

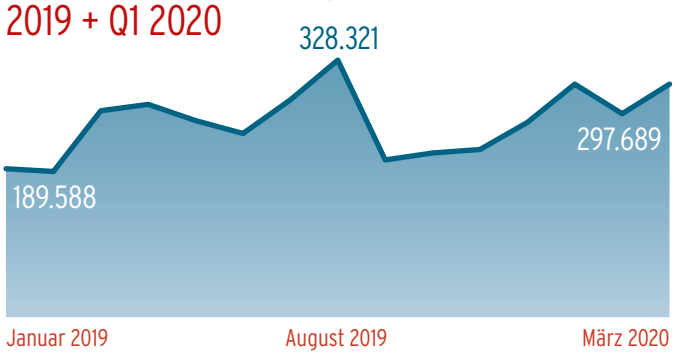
Neben Malware-Attacken müssen sich Internetnutzer aber auch gegen eine weitere Gefahr schützen: Potenziell Unerwünschten Anwendungen, kurz PUA. Diese Spionage-Software ist bei Auslieferung von Geräten mit Software-Bundles oft vorinstalliert, schleicht sich aber noch deutlich häufiger beim Download von Programmen und Apps auf die Geräte. Urheber ist meist die Werbeindustrie, die PUA nutzt, um private Informationen sowie Nutzerverhalten und Bewegungsmuster zu erfassen und zu analysieren. Im Gegenzug für die ungewollt und meist heimlich abgefragten Daten erhalten Nutzer personalisierte Werbung.

Während diese industriellen Schnüffel-Tools in Windows-Systemen seit Jahren auf dem Rückzug sind, nimmt ihre Zahl im Android-Bereich stark zu. Und bei MacOS-Systemen lag die Anzahl von PUA-Samples 2019 mit einer Gesamtzahl von 52.095 sogar nahezu gleichauf mit der Malware-Gesamtrate (60.674 Samples). Im ersten Quartal dieses Jahres übersteigt die Anzahl solcher Spitzel-Software für Macs sogar die Malware-Rate: Während die AV-TEST Systeme insgesamt 11.441 neue Malware-Samples detektierten, lag die PUA-Rate bereits bei 18.829 Samples. Dementsprechend entwickelt sich insbesondere diese Schädlingsgattung zur neuen Bedrohung für Mac-Nutzer.

Windows: Entwicklung neuer PUA
2019 + Q1 2020



Android: Entwicklung neuer PUA
2019 + Q1 2020



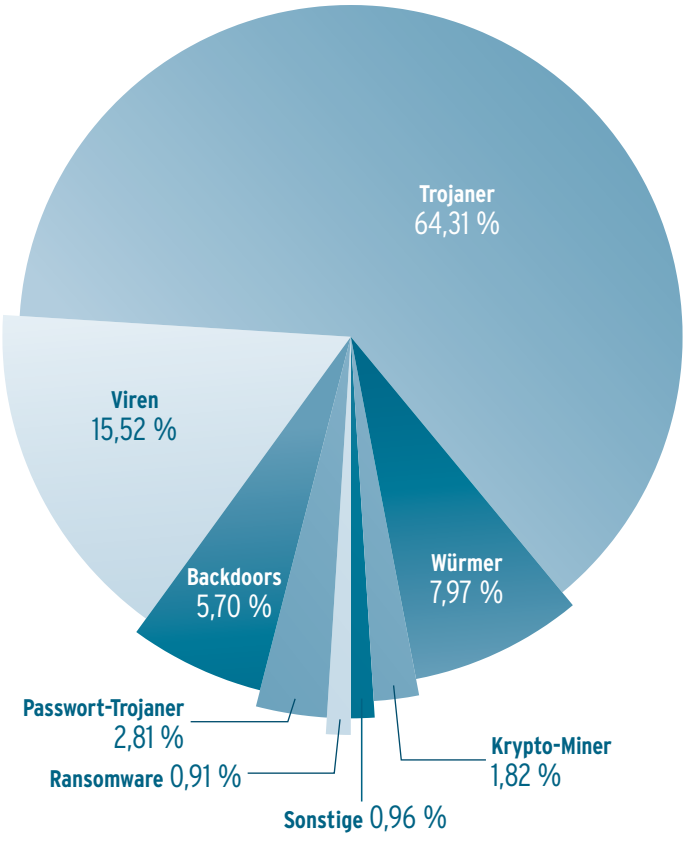
Sicherheitsstatus WINDOWS

Kein anderes Betriebssystem steht derart im Fokus der Malware-Industrie. Dafür gibt es einen klaren Grund, denn kein anderes Betriebssystem erreicht einen ähnlichen Verbreitungsgrad. Wer also als Cyberkrimineller wirtschaftlich erfolgreich sein will, hat ein glasklares Ziel vor Augen: Windows-Systeme. Dabei sind Angriffe auf das Redmonder Betriebssystem längst nichts mehr für Anfänger. Denn der hohe Verbreitungs- und Wirkungsgrad aktueller Sicherheitslösungen erfordert im Gegenzug hohe Geschwindigkeit und Innovation bei der Entwicklung und Distribution von Massen-Malware und ausgefeilte Techniken bei zielgerichteten Attacken.

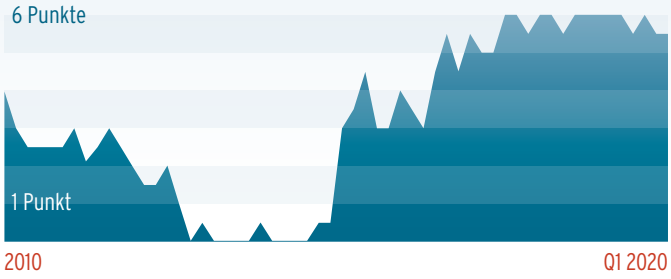
Anfälliger Branchen-Primus

Microsoft machte mit mehr als 660 offiziell in der CVE-Datenbank gemeldeten gefährlichen Sicherheitslücken im vergangenen Jahr keine gute Figur und erreichte Platz 1 der unsichersten Betriebssysteme. Allein 357 aller potentiellen Windows-Einfallstore für Angriffe gingen auf die Kappe des aktuellen Betriebssystems Windows 10. Einen ebenfalls hohen Anfälligkeitsgrad zeigten Windows Server 2016 und Windows Server 2019. Etwas abgeschlagen folgte Windows 7, das mit Beginn dieses Jahrs von Microsoft offiziell zum alten Eisen gelegt und nicht mehr mit Updates und Sicherheitspatches versorgt wird. Dennoch erfreut sich der Windows-Oldie nach aktuellen Auswertungen nach wie vor hoher Beliebtheit: In Rankings des ersten Quartals dieses Jahres rangiert Windows 7 mit nach wie vor über 30 Prozent immerhin noch auf Platz 2 der weltweit meistgenutzten Betriebssysteme. Klarer Marktführer ist Windows 10, das auf knapp der Hälfte (51,38 %) aller ans Internet angebundenen Rechner weltweit läuft.

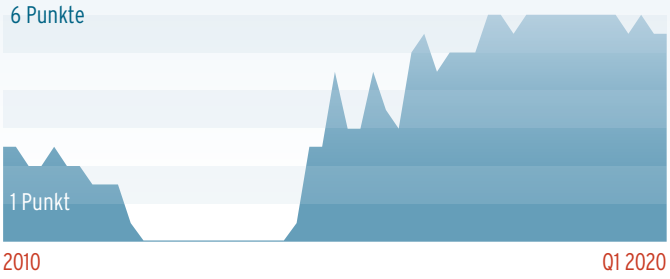
Malware-Verteilung unter Windows 2019



Schutzwirkung von Windows Defender Antivirus Home 2010 - Q1 2020



Schutzwirkung von Windows Defender Antivirus Business 2010 - Q1 2020



Offensichtlich haben sich vor allem Privatnutzer von der Einstellung des Windows 7 Supports überzeugen lassen und sind auf das Nachfolgesystem gewechselt. In vielen anderen Bereichen, etwa in der industriellen Fertigung, bei staatlichen Institutionen wie Verwaltung und Bildungseinrichtungen, Krankenhäusern aber auch in Unternehmen und Banken, gilt allerdings häufig der Grundsatz „Never change a running system". Da ein Betriebssystemwechsel hier oft als erheblicher Kostenfaktor gilt, dürfte die Wechselquote dementsprechend deutlich geringer ausfallen, als im Segment der Privathaushalte.

Windows-Lücken aktiv genutzt wie nie zuvor

Zu den bekannten und veröffentlichten Windows-Lücken gesellen sich selbstverständlich noch solche, die weder der Öffentlichkeit noch dem Hersteller selbst bekannt waren und sind. Leider werden die wenigsten solcher „geheimen" Sicherheitslecks mit den Herstellern kommuniziert, sondern beispielsweise zur geheimdienstlichen Aufklärung und Überwachung eingesetzt.

Entsprechend hoch werden solche Software-Lücken auf dem Schwarzmarkt gehandelt. Eine Praxis, die sowohl Software-Hersteller als auch Datenschützer und Bürgerrechtler zu Recht regelmäßig scharf kritisieren. Und neben möglichen Einfallstoren des Betriebssystems verschärfen zudem noch Sicherheitslücken weit verbreiteter Anwendungen sowie die Firmware angeschlossener Geräte die Gefahrenlage. So landeten 2019 Google, Oracle, Adobe, Cisco und IBM auf den Plätzen 2 bis 6 der Top 10 der Hersteller mit den meisten Sicherheitslücken. Allein Adobes weltweit eingesetzter Adobe Reader brachte es auf stattliche 342 bekannte Lecks.

Auf die bis dato höchste Anzahl an Sicherheitslücken für Windows und darauf laufender Software reagierte die Malware-Industrie 2019 entsprechend: Die Raten erfasster Windows-Exploits zur Ausnutzung entsprechender Sicherheitslücken erreichten den Höchststand im Vergleich der letzten 10 Jahre. Exploits verzeichneten insbesondere von August bis November ein mehr als exponentielles Wachstum. Deutliche Anstiege ließen sich allerdings bereits Anfang des Jahres erkennen. Zum Vergleich: Im Vorjahr lag der Jahresgesamtwert bei immerhin 71.377 Samples. 2019 verdoppelte sich dieser Wert nahezu auf exakt 130.776 neu programmierte Exploits.

Die hohe Entwicklungsrate wiederum kann als Indiz für zwei positive Entwicklungen des letzten Jahres gelten: Zum einen legte Microsoft als Anbieter des Betriebssystems mit den meisten Sicherheitslecks eine hohe Patch-Geschwindigkeit vor. Dieser Sachverhalt nötigte Cyberkriminelle entsprechend, Malware-Samples am Fließband zu produzieren, um weiterhin wirtschaftlich profitieren zu können. Zum anderen erwiesen sich die Windows-eigenen Abwehrsysteme als zuverlässiger Schutz gegen automatisierte Massen-Malware. In den regelmäßigen Zertifizierungstests des letzten Jahres erreichte Microsofts Privatanwenderprodukt „Microsoft Defender" fünf von sechs Mal die AV-TEST Bewertung „Top Product". Was unter anderem an der zuverlässigen Erkennungs- und Abwehrleistung gegenüber weit verbreiteter und häufig auftretender Malware lag. Die Business-Lösung von Microsoft zeigte 2019 noch bessere Testergebnisse und konnte den Titel „Top Product" sogar in sechs von sechs Jahrestests verteidigen.

Windows: Entwicklung neuer Exploits 2019 + Q1 2020

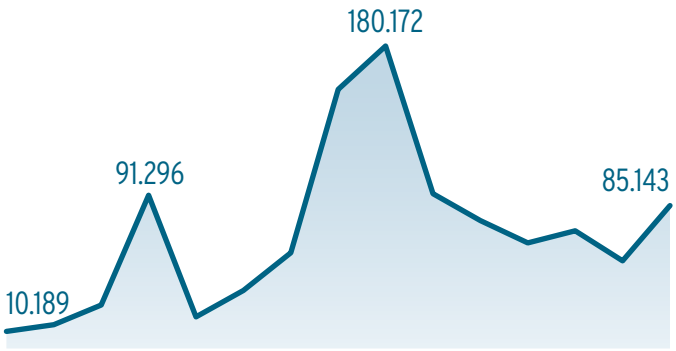
Windows: Entwicklung neuer Trojaner 2019 + Q1 2020

Anstieg von Windows-Trojanern über 35 %

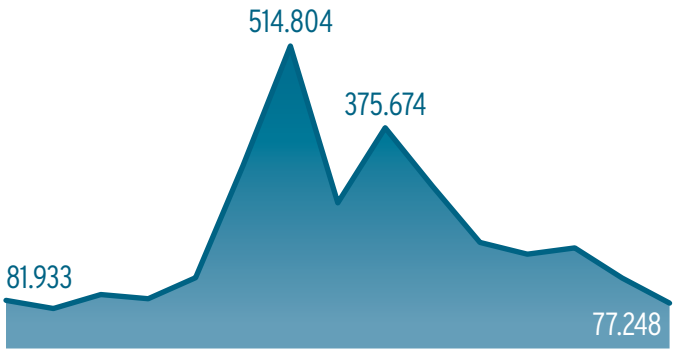
Gelang Kriminellen die Infektion von Windows-Systemen, wurden als Speerspitze von Angriffen in der Regel Trojaner genutzt. Zum einen, um möglichst langfristig auf gekaperte Systeme zugreifen zu können, zum anderen, um spezialisiertere Malware mit anderer Schadfunktion nachzuladen. Dementsprechend erreichte die Neuentwicklungsquote für Trojaner 2019 ihren bisherigen Höchststand. Den Vorjahreswert von 42.594.399 übertraf das vergangene Jahr mit einer Quote von insgesamt 57.612.235, das entspricht einer Zunahme von über 35 Prozent. Insgesamt machten Trojaner 2019 mit 64,31 Prozent den mit Abstand größten Teil der von Kriminellen eingesetzten Windows-Malware aus. Bemerkenswert sind dabei zwei Trojaner-Wellen, die jeweils im August sowie im November letzten Jahres ihren Anfang nahmen und somit in 2019 die höchste Gefahrenstufe für Windows-Nutzer einläuteten.

Denn nahezu zeitgleich mit der ersten Trojaner-Welle starteten umfangreiche Kampagnen anderer Malware-Gattungen. Dazu gehörten entsprechend der Analysen der Erfassungssysteme von AV-TEST insbesondere Bots, Ransomware, Passwort-Trojaner und Krypto-Miner. Im Ergebnis lässt sich feststellen, dass die Marschroute von Kriminellen vor allem Mitte bis Ende des Jahres eindeutig Richtung Monetarisierung mittels eingesetzter Massen-Malware ging. Angefangen bei der Erpressung von Windows-Nutzern durch das Sperren bzw. Verschlüsseln von Windows-Verzeichnissen oder kompletter Systeme über das Abgreifen von Zugangsdaten für Onlinekonten jeder Art bis hin zur missbräuchlichen Nutzung fremder Infrastruktur, Bandbreite und Rechenleistung zum Erlangen von Krypto-Währung wie Bitcoin. Insbesondere auch alternative Währungen, wie Binance Coin (BNB), Litecoin und Bitcoin Cash rückten 2019 nicht zuletzt aufgrund ihrer hohen Marktkapitalisierungsrate in das Blickfeld der Cyberkriminellen.

Windows: Entwicklung neuer Ransomware 2019 + Q1 2020

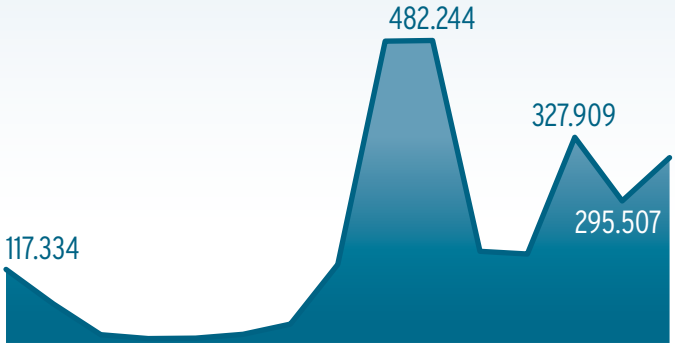


Windows: Entwicklung neuer Passwort-Trojaner 2019 + Q1 2020

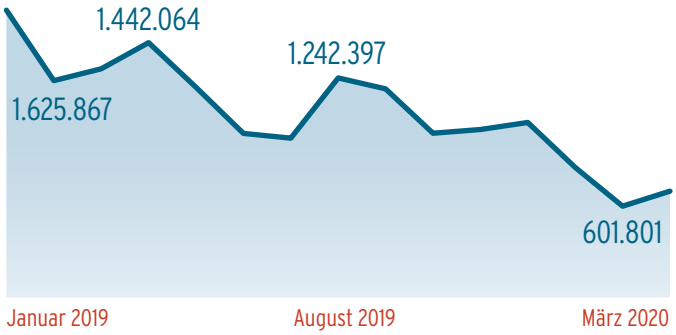


Windows: Entwicklung neuer Bots 2019 + Q1 2020

Windows: Entwicklung neuer Krypto-Miner 2019 + Q1 2020



Windows: Entwicklung neuer Viren 2019 + Q1 2020



Trend 2020

Während die Entwicklung von Passwort-Trojanern im ersten Quartal dieses Jahres regressiv verläuft, steigen die Entwicklungsraten von Krypto-Minern, Bots und Ransomware wieder an. Im Verhältnis steigt der Anteil der Trojaner zu anderen Malware-Gattungen weiter auf 69,63 Prozent.

Bemerkenswert ist, dass sich die Rate klassischer Viren im Vergleich zum Vorjahr mehr als halbiert (von 15,52 % auf 7,57 %) und diese Schädlingsgattung somit in der Waffenkammer der Cyber-kriminellen weiterhin drastisch an Bedeutung verliert.

TOP 10 Windows-Malware 2019

1	AGENT	8,19 %
2	VIRLOCK	5,81 %
3	DINWOD	5,06 %
4	VIRUT	3,71 %
5	KRYPTIK	2,99 %
6	DELF	2,74 %
7	UPATRE	2,71 %
8	INJECTOR	2,59 %
9	SIVIS	2,46 %
10	WABOT	1,87 %

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/ abgerufen werden.

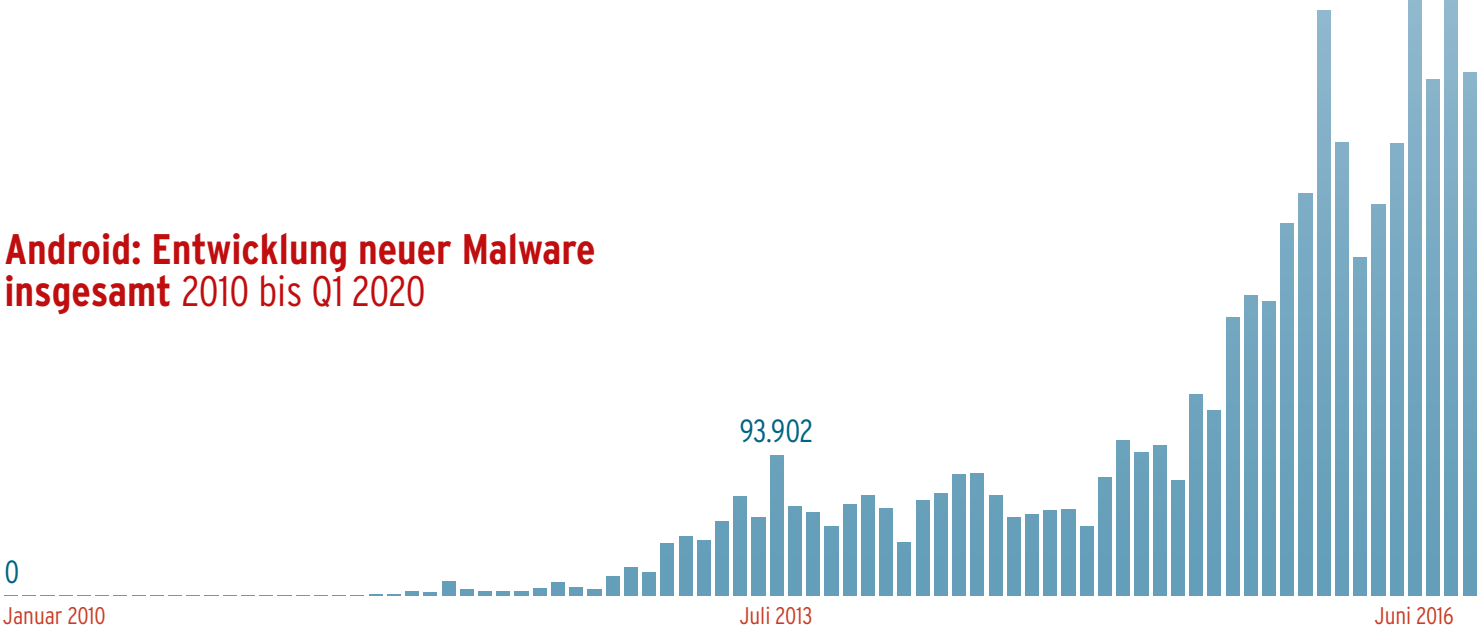
Sicherheitsstatus ANDROID

Sinkende Malware-Entwicklungsraten zeichneten das Jahr 2018 aus. Doch das war einmal. Denn seit Beginn des zweiten Quartals 2019 steigt die Rate neu entwickelter Android-Schädlinge wieder beständig an, seit dem letzten Quartal sogar sprunghaft. Wie sieht die Sicherheitslage für die weltweit meistgenutzte Mobil-Plattform aus?

Unsicherstes Betriebssystem 2019

Ein Blick auf die Entwicklungskurve neuer Android-Malware beruhigte sowohl die Besitzer des meistgenutzten Betriebssystems für Mobilgeräte als auch Anbieter Google in den letzten vier Jahren. Denn seit dem Höchststand der Malware-Entwicklung, verzeichnet Mitte 2016, verlief die Rate neu entwickelter Android-Malware klar rückläufig und erreichte Mitte des vergangenen Jahres ihren tiefsten Punkt innerhalb der letzten drei Jahre. Diese beruhigende Entwicklung endete allerdings Mitte des letzten Jahres. Seither steigt die Malware-Kurve für Android-Geräte stetig, im ersten Quartal dieses Jahres sogar exponentiell. Nicht weiter verwunderlich, denn in der Rangliste der anfälligsten Betriebssysteme und Programme belegt Android 2019 mit 417 bekannten und in der CVE-Datenbank verzeichneten Sicherheitslecks den unrühmlichen ersten Platz.

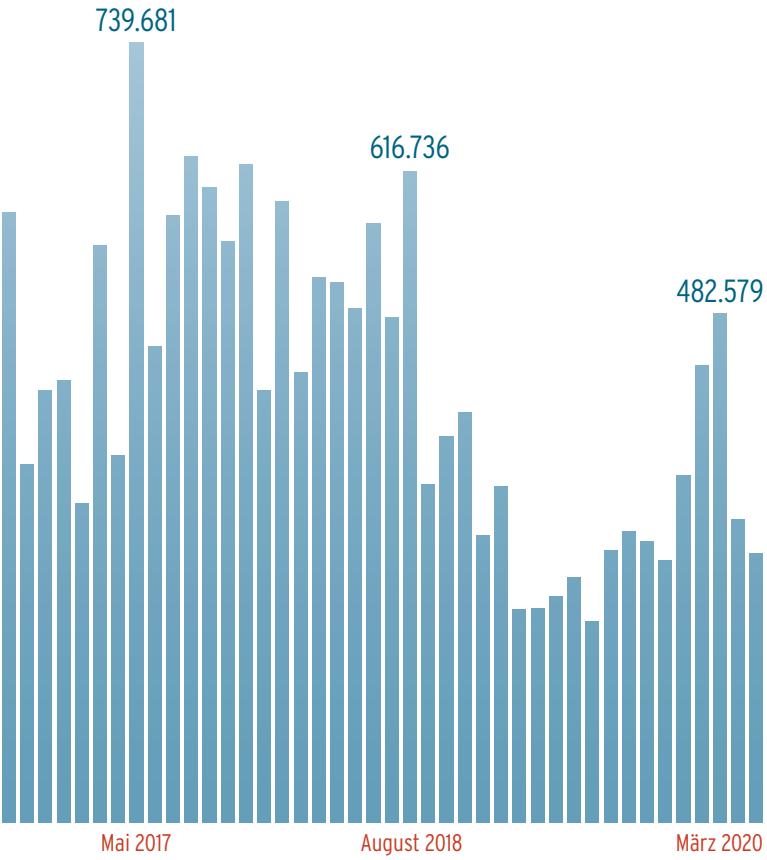
Android: Entwicklung neuer Malware insgesamt 2010 bis Q1 2020



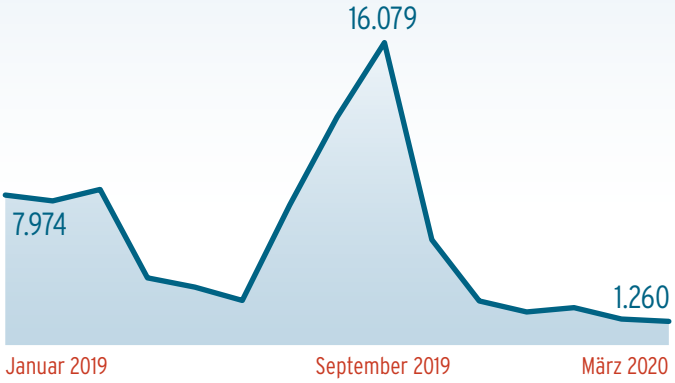
Über 90 % Trojaner

Den mit Abstand größten Anteil machten 2019 Trojaner aus. Nahezu 94 Prozent des neu programmierten Schadcodes für Android-Geräte ist auf diese Malware-Gattung zurückzuführen. Ein solcher Schädling war „Hiddad", der als Android-Trojaner bereits 2018 sein Unwesen trieb und im vergangenen Jahr in den Top 10 der Android-Malware immerhin von Platz 8 auf Platz 2 kletterte.

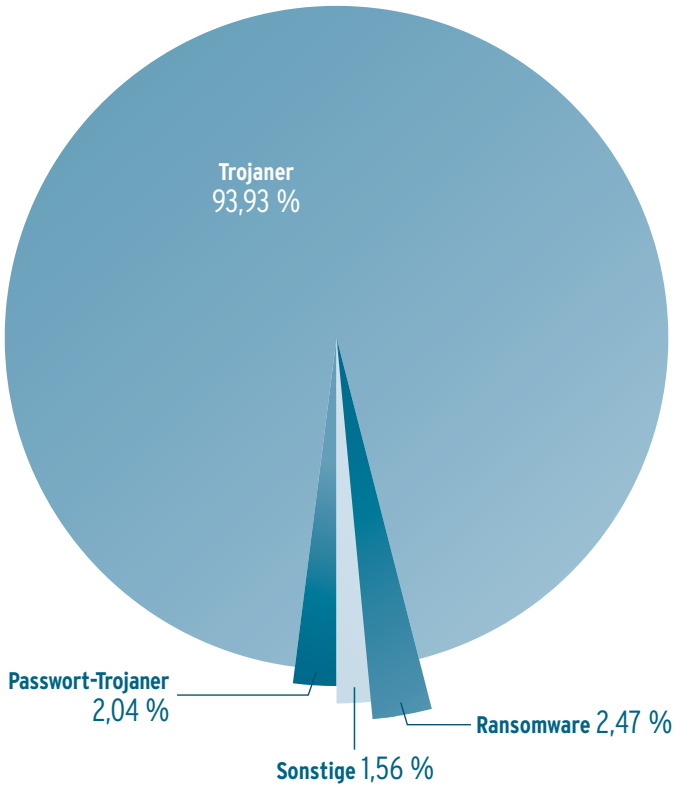
Hiddad (18,7 %) ist ein „Werbefachmann", der sich unter anderem in Apps versteckte, die auch über Googles Playstore ausgeliefert wurden. Nach der Installation von mit Hiddad geimpften Apps versteckt sich die Malware geschickt durch den Einsatz Android-typischer Dateinamen wie „Google Play Service", und Sicherheits-Apps erschwert sie durch die Nutzung von Superuser-Rechten und das Verstecken in Android-Systemordnern Detektion und Entfernung. Auf infizierten Endgeräten zeigt Hiddad in bestimmten Zeitintervallen Werbung im Vollbildmodus an und lässt seine Urheber auf diese Weise Kasse machen.



Android: Entwicklung neuer Ransomware 2019 + Q1 2020



Android: Malware-Verteilung 2019



Android: Entwicklung neuer Passwort-Trojaner 2019 + Q1 2020

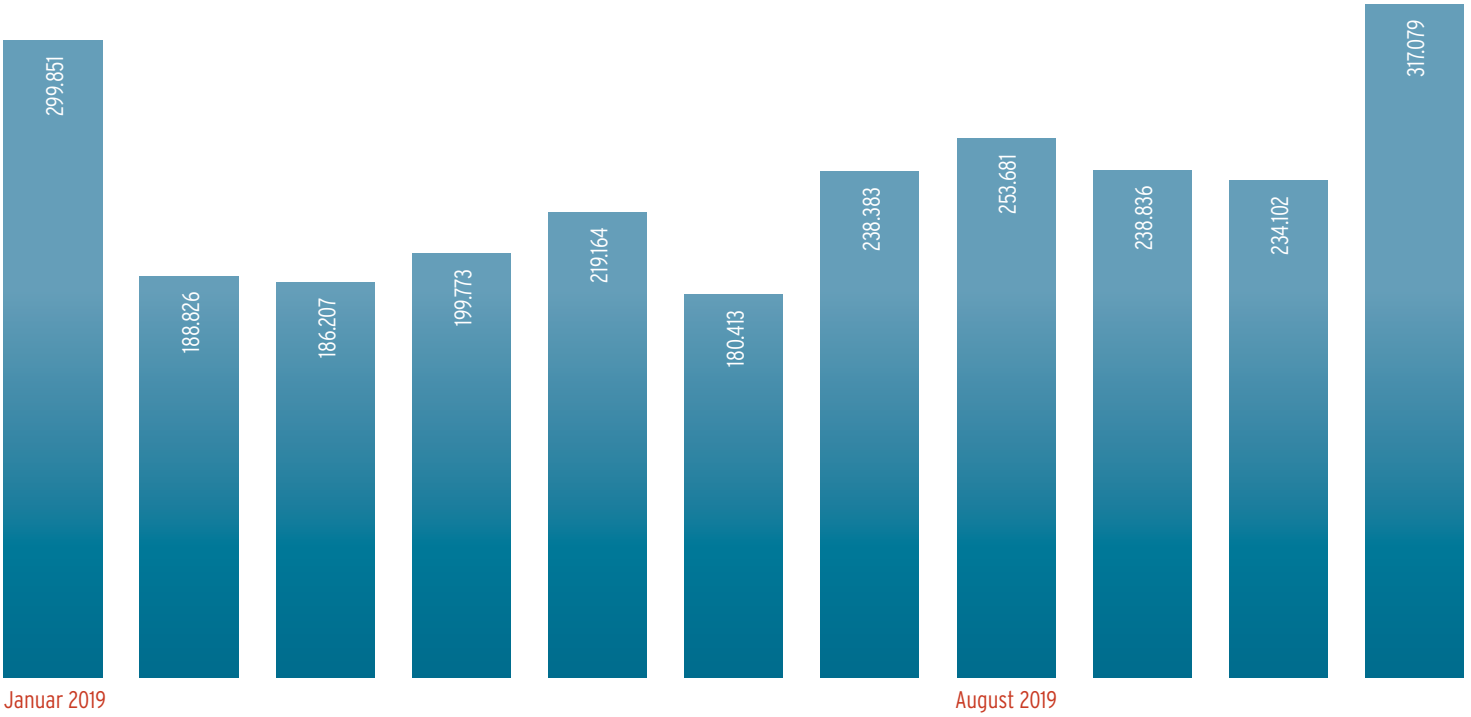
Die Anzeige unerwünschter Werbung auf Android-Geräten erweist sich für Kriminelle offenkundig immer häufiger als erfolgreiche Monetarisierungsstrategie. Denn mit Werbung verdienen auch Kriminelle gutes Geld.

Und so setzen die meisten Schädlinge der Android Top 10 auf dieses Verfahren. Gleiches gilt für „Shedun", der 2019 auf Platz 3 (9,7 %) rangierte und bereits seit 2015 für Kriminelle Geld verdient.

Mobile Erpressung: Android-Ransomware

Als weitere Einkommensquelle setzten kriminelle Android-Spezialisten 2019 Ransomware zur Erpressung von Gerätenutzern ein. Mit 2,47 Prozent des gesamten Malware-Anteils steht diese Malware-Gattung auf Platz 2 der eingesetzten Schadprogramme. Die wirtschaftliche Basis für diese Entwicklung gründet sich darin, dass Mobilgeräte längst in gleichem Umfang genutzt werden wie PCs und Notebooks. Hinzu kommt die ständige Verfügbarkeit der Geräte als Kamera für Schnappschüsse sowie eine deutlich geringere Backup-Quote, so dass über Ransomware gesperrte Geräte äußerst selten einfach über ein Backup in den Zustand vor dem Angriff zurückgeführt werden können. Und so detektierten die AV-TEST Analysesysteme 2019 über 78.000 neu programmierte Ransomware-Samples für Googles Betriebssystem.

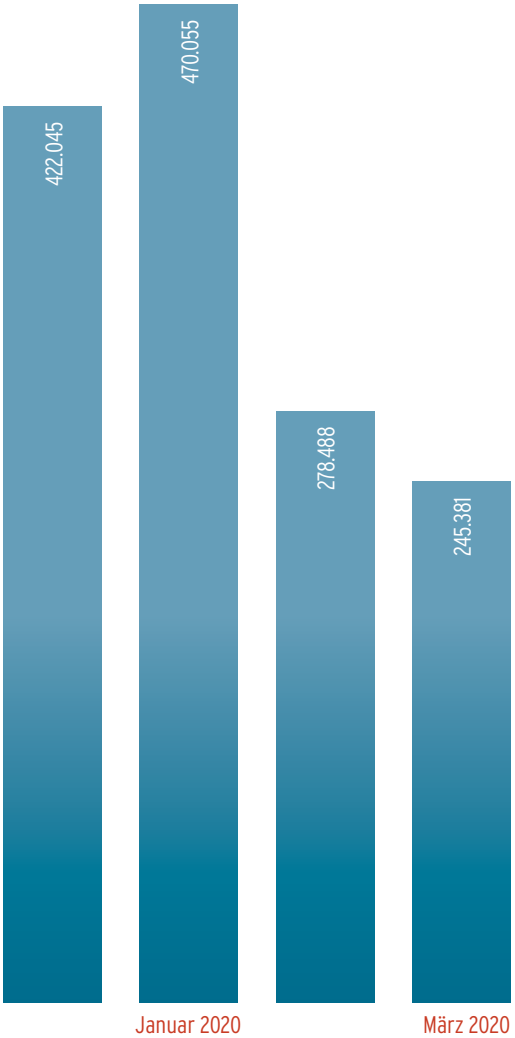
Android: Entwicklung neuer Trojaner 2019 + Q1 2020



An dritter Stelle rangierten in 2019 Android Passwort-Trojaner. Auch diese Malware lohnt sich für Kriminelle nur, weil Endgeräte mittlerweile in großem Umfang für Internet-Banking und den Einkauf auf Online-Plattformen genutzt werden. Und so ist das Abgreifen von Login-Daten und das nachfolgende Plündern unterschiedlichster Nutzerkonten längst ein lohnendes Angriffsziel von Cyberkriminellen. Aufgrund der immer noch geringen Verbreitung von Schutz-Apps ist für Android, im Gegensatz zu Windows-Systemen, auch der Entwicklungsdruck deutlich geringer. Hinzu kommen die freie Verfügbarkeit von App-Entwicklungstools, der relativ leichte Zugang zum Google Playstore sowie die Möglichkeit, verseuchte Apps zusätzlich über andere App-Stores auszuspielen. Und zu guter Letzt sorgen der hohe Marktanteil von Android (ca. 80 % weltweit) sowie die unterschiedlichen und oft nicht mehr gepatchten Android-Versionen, die noch in großer Zahl im Einsatz sind, für gute Geschäftsbedingungen für Kriminelle.

TOP 10 Android-Malware 2019

1	AGENT	26,64 %
2	HIDDAD	18,71 %
3	SHEDUN	9,70 %
4	SMSREG	8,60 %
5	CLICKER	4,51 %
6	SMSSEND	3,10 %
7	SMS	2,45 %
8	FAKEPLAYER	1,73 %
9	KOLER	1,60 %
10	LOCKER	1,49 %



Trend 2020

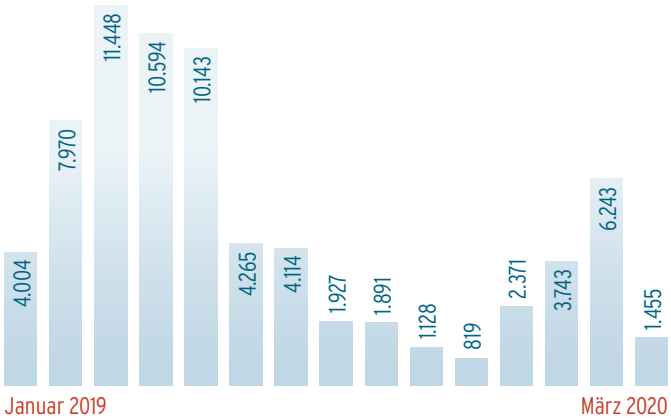
Das erste Quartal des laufenden Jahres deutet einen klaren Rückgang mobiler Ransomware an, deren Anteil gegenüber dem Vorjahr signifikant von 2,47 auf 0,45 Prozent sinkt. Ebenfalls rückläufig zeigt sich die Entwicklung von Passwort-Trojanern (2,04 % auf 1,33 %). Entsprechend steigt die Entwicklungsrate von Trojanern wie Shedun und Hiddad. Letzterer erhöht seinen Anteil am Malware-Gesamtaufkommen deutlich auf über 22 Prozent. Dies lässt zumindest vermuten, dass Cyberkriminelle 2020 vermehrt mit unerwünschten Werbeanzeigen Kasse machen werden.

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/ abgerufen werden.

Sicherheitsstatus MacOS

Gute Nachrichten für Apple-Nutzer: Die AV-TEST Erfassungssysteme verzeichnen insgesamt eine rückläufige Malware-Entwicklungsquote für MacOS-Systeme. Allerdings steht im Hintergrund dieser positiven Entwicklung auch der Fakt, dass Malware für Mac mittlerweile eine ernstzunehmende Bedrohung ist und dass 2019 der Höchststand der Malware-Entwicklung seit vier Jahren zu verzeichnen war. Grund zur Entwarnung ist diese Entwicklung also nicht, wie die Analyse der Malware-Entwicklung für MacOS zeigt.

MacOS: Entwicklung neuer Malware gesamt 2019 + Q1 2020



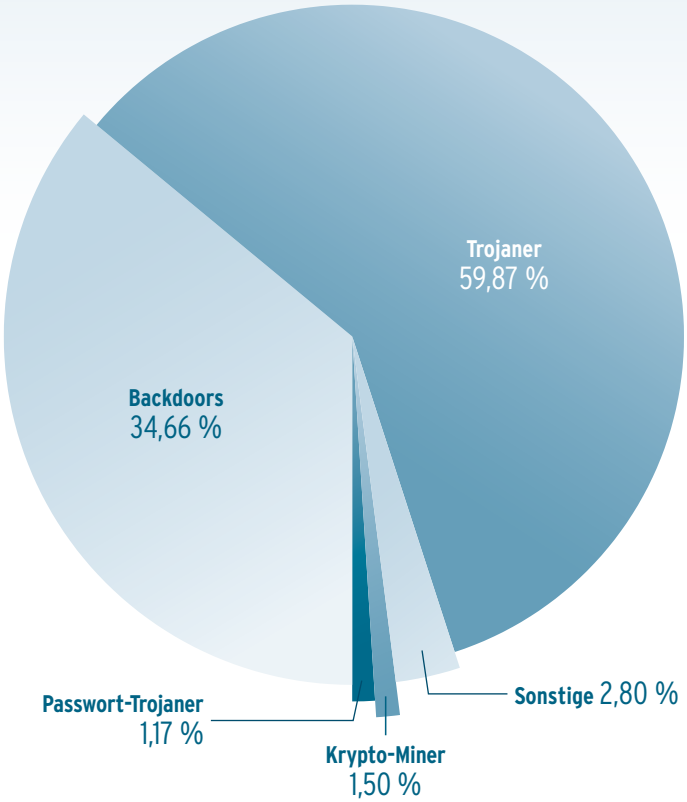
Alte Trojaner und Backdoors

Die eigentlich gute Nachricht wird überschattet, sobald der Blick auf die Malware-Verteilung des vergangenen Jahres fällt und die 2019er Kennzahlen einer genauen Analyse unterzogen werden. Zunächst muss man lange scrollen, um Apple beziehungsweise dessen aktuelles Betriebssystem in der Liste der Programme mit bekannten Sicherheitslecks zu finden: MacOS X taucht erst auf Platz 44 auf. Allerdings wurden 2019 diese bekannten und andere Sicherheitslecks auch ausgiebig genutzt. Die Anzahl der im vergangenen Jahr für MacOS programmierten Exploits mag im Verhältnis zu Windows-Systemen mit nur 107 Samples verschwindend gering erscheinen. Allerdings treffen diese auf fruchtbaren digitalen Boden, der nach wie vor kaum geschützt ist. Denn noch immer läuft auf vielen Mac-Systemen kein Virenschutz. Und so ließ sich Mitte letzten Jahres ein deutlicher Anstieg bei der Entwicklung von Exploits beobachten.

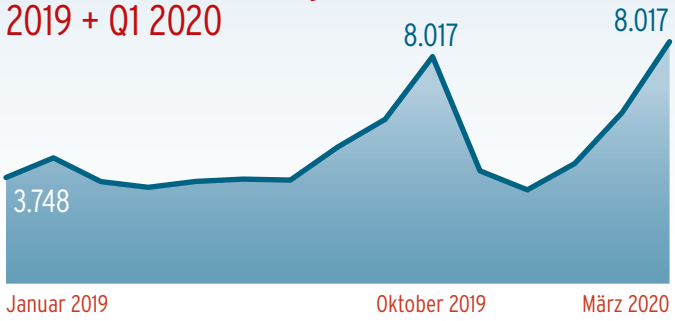
Auch die Zahl für MacOS verfügbarer Backdoors stieg insbesondere in der ersten Hälfte des vergangenen Jahres sprunghaft an und verdoppelte sich. Eine besorgniserregende Tatsache, wenn man bedenkt, dass Backdoors neben Trojanern mit 34,66 Prozent die zweitgrößte Gruppe der Apple-Malware stellen. Der Prozentwert der Trojaner lag 2019 bei 59,87 Prozent. Insgesamt lauerten damit im letzten Jahr 36.326 Trojaner auf Mac-Nutzer, eine klare und deutliche Bedrohung. Krypto-Miner (1,5 %) und Passwort-Trojaner (1,17 %) stellten 2019 ebenfalls eine Gefahr für Mac-Nutzer dar, auch wenn sie zahlenmäßig deutlich unterrepräsentiert sind.

Dementsprechend werden die Malware Top 10 auch klar von einem Trojaner sowie einer Backdoor mit jeweils extrem hohem Verbreitungsgrad angeführt. Auf Platz 1 steht mit dem Trojaner „Flashback" (38,36 %) ein Schädling, der Mac-Rechner seit über zehn Jahren in den unterschiedlichsten Varianten infiziert und dafür oft eine Java-Lücke nutzt. Ist im Browser Java aktiviert, entert Flashback beim Besuch einer Webseite per Drive-by-Infektion unbemerkt den Rechner. Infizierte Systeme zwingt Flashback in eine ferngesteuerte C&C-Server-Struktur und ist durch erschlichene Administratoren-Rechte in der Lage, beliebige Schadkomponenten nachzuladen oder über Keylogger Passwörter auszulesen und heimlich zu verschicken. Dass diese Universalwaffe auch nach 10 Jahren offensichtlich noch ein lohnendes Werkzeug für Cyberkriminelle zu sein scheint, wirft kein gutes Licht auf den Schutzstatus aktueller Mac-Rechner. Kriminelle brauchen demnach keinen großen Aufwand zu betreiben, um mit ihrer Malware wirtschaftlich erfolgreich zu sein.

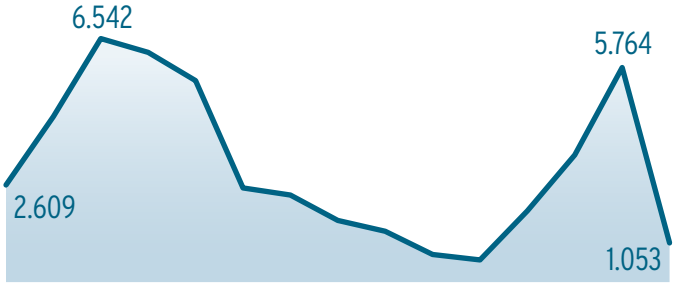
MacOS: Malware-Verteilung 2019



MacOS: Entwicklung neuer PUA 2019 + Q1 2020



MacOS: Entwicklung neuer Trojaner 2019 + Q1 2020



TOP 10 MacOS-Malware 2019

1	FLASHBACK	43,33 %
2	MACKONTROL	39,74 %
3	SHLAYER	10,90 %
4	AGENT	1,60 %
5	TINIV	1,42 %
6	BUNDLORE	1,13 %
7	APTORDOC	0,18 %
8	TINYV	0,16 %
9	ADLOAD	0,11 %
10	INSTALLCORE	0,07 %

Trend 2020

Der Trend bei Mac-Malware zeigt im ersten Quartal dieses Jahres eine spannende Entwicklung: Während sich die Anzahl neuentwickelter Trojaner massiv von ca. 60 auf nahezu 90 Prozent erhöht, fällt der Anteil neuer Backdoors ins Bodenlose: Von den 34,66 Prozent des Vorjahres bleiben im ersten Quartal 2020 gerade noch 0,3 Prozent übrig. Eine Erklärung für diese Entwicklung könnte in den Veränderungen der Sicherheitsarchitektur von MacOS zu finden sein. Allerdings muss dieser Trend für eine klare Aussage weiter beobachtet werden. Eine deutliche Steigerungsrate zeigen auch die Krypto-Miner, die ihren Anteil am Malware-Gesamtvolumen mit 6,56 Prozent mehr als vervierfachen.

AV-TEST
av-test.org

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

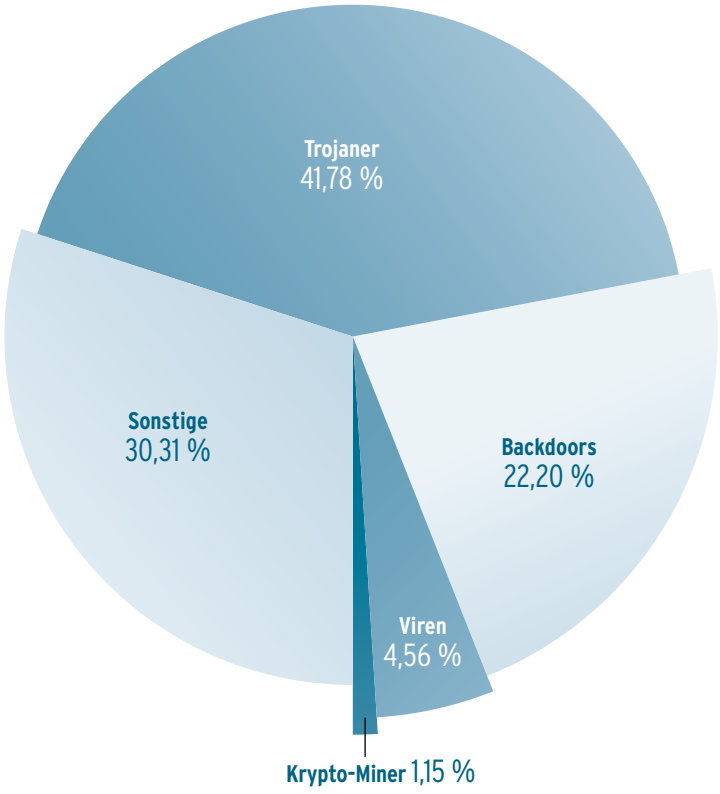
Kaum ein IT-Marktsektor legte in den letzten Jahren und Monaten derartige Wachstumsraten vor, wie der in Verbindung mit vernetzten Geräten (IoT). Die Konsequenz für Cyberkriminelle mit wirtschaftlichen Absichten ist damit unausweichlich, und folglich boomte nicht nur das Geschäft legaler IoT-Unternehmen, sondern auch das der Schattenwirtschaft. Doch während seriöse Produkthersteller und Service-Anbieter bei Kunden mühsam für Verständnis bei der IT-Sicherheit werben müssen, können Kriminelle ihre Geschäftsmodelle auf Basis massenhaft schlecht oder komplett ungeschützter IoT-Systeme aufbauen. Und mit der zunehmenden Durchdringung von IoT-Geräten in industrieller Produktion, der Medizin und weiteren wirtschaftlichen Bereichen sowie Privathaushalten wächst die Bedrohung durch ungesicherte IoT-Geräte ständig weiter.

IoT-Malware-Bedrohung: Verdopplung der Linux-Malware-Rate

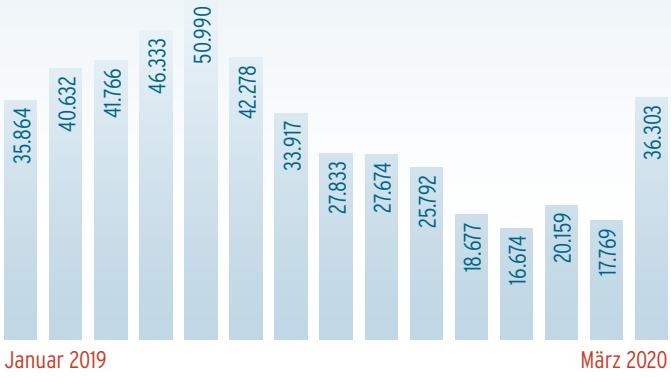
Die Warnungen des AV-TEST Instituts in Verbindung mit der IoT-Sicherheitslage sind alles andere als neu. Bereits im Sicherheitsreport 2016 erhielt das Thema ein eigenes Kapitel. Und auch im Report des letzten Jahres war die Warnung aus dem IoT-Labor unmissverständlich: „Im Wettrennen um lukrative Marktanteile entwickelt die IoT-Industrie weiter massenhaft internetangebundene Produkte ohne ausreichendes Sicherheitskonzept und lässt häufig selbst absolute Mindeststandards der IT-Sicherheit außer Acht." An diesen Fakten und der daraus resultierenden Bedrohungslage hat sich allerdings kaum etwas geändert.

Während sich im Bereich des Schutzes von IoT-Strukturen seither wenig bewegt, sieht es auf der entgegengesetzten Seite anders aus: So verzeichneten die AV-TEST Systeme insbesondere Anfang des vergangenen Jahres exponentiell wachsende Malware-Raten für IoT-typische Linux- und Unix-Versionen wie Canonical Ubuntu und andere. Diese Entwicklung

IoT: Malware-Verteilung 2019



IoT/Linux: Entwicklung neuer Malware insgesamt 2019 + Q1 2020



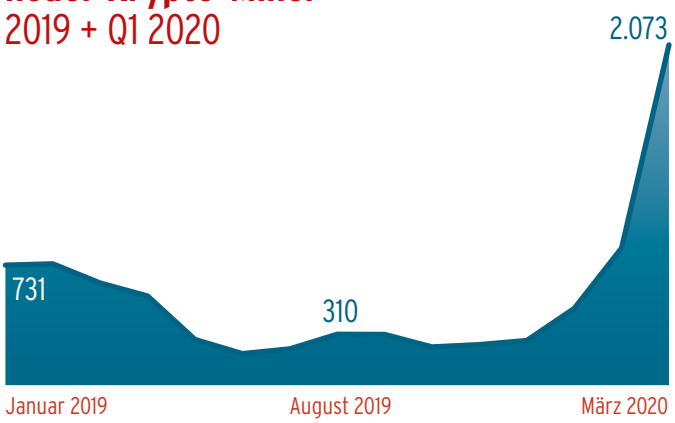
IoT/Linux: Entwicklung neuer Trojaner 2019 + Q1 2020

zeichnete sich bereits zu Beginn des Jahres 2018 in den Erfassungsdaten der AV-TEST Systeme ab, überholte in seiner Entwicklung 2019 allerdings selbst die pessimistischsten Prognosen. Verzeichnete die Analyse neuer Linux-Malware-Samples für 2018 bereits einen Gesamtwert von 188.902 neu programmierten Schadprogrammen, meldeten die AV-TEST Systeme 2019 mit 408.430 neuen Samples einen mehr als verdoppelten Wert.

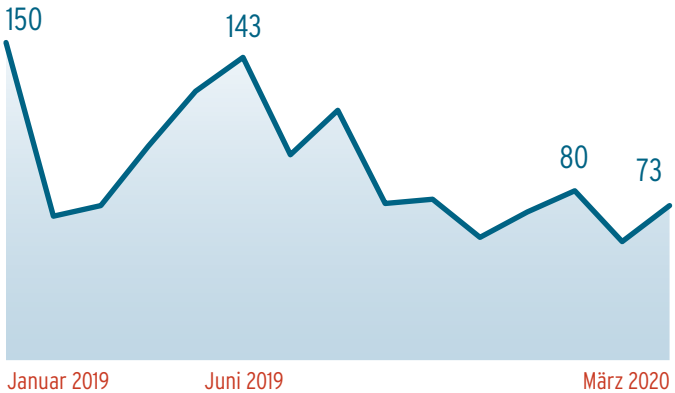
Lehre aus den Mirai-Attacken lässt auf sich warten

Den Großteil der Schadprogramme für IoT-Geräte auf Linux-Basis stellten 2019 mit 41,78 Prozent Trojaner. Wenig überraschend und symptomatisch für die unbefriedigende Reaktion von IoT-Herstellern auf selbst längst bekannte Bedrohungen, führen diverse Varianten des Schädlings „Mirai" nach wie vor die Top 10 der IoT-Malware an und stellten satte 40,84 Prozent des gesamten Malware-Aufkommens. Der ursprünglich im September 2016 von Jugendlichen programmierte Schadcode sorgte aufgrund von völlig aus dem Ruder gelaufenen Distributed Denial of Service-Attacken (DDoS) auf große Online-Dienste, darunter Dyn, Twitter, Spotify, Amazon, sowie auf Router der Telekom Deutschland weltweit für Aufsehen. Dementsprechend kann sicherlich kein Hersteller von IoT-Geräten behaupten, diese Gefahr nicht zu kennen. Darüber hinaus wuchsen durch den Trojaner Mirai angelegte Bit-Netze auch 2019 weiter. Neue Varianten des Mirai-Schadcodes arbeiten entsprechend mit neuen Taktiken und Techniken und werden beispielsweise zum Kapern digitaler Infrastrukturen im industriellen IoT-Sektor (IIoT) eingesetzt. So eroberten Cyberkriminelle etwa schlecht geschützte Industrieanlagen, konnten diese sabotieren oder Rechenleistung für das Schürfen digitaler Währung oder für DDoS-Angriffe einsetzen.

IoT/Linux: Entwicklung neuer Krypto-Miner 2019 + Q1 2020



IoT/Linux: Entwicklung neuer Exploits 2019 + Q1 2020



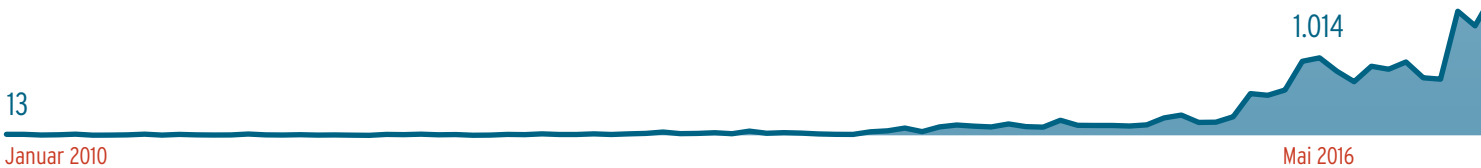
Krypto-Miner setzen auf ungeschützte IoT-Infrastruktur

Die auch ansonsten nahezu unveränderte Rangliste der meistgenutzten IoT-Schädlinge lässt erahnen, dass es mit dem Schutz internetbasierter Geräte nicht weit her ist. Denn nach wie vor reichen den Angreifern neue Varianten längst bekannten Schadcodes, um wirtschaftlich erfolgreich zu sein.

Im Ergebnis gelten in diesem Sicherheitsreport also dieselben Warnungen, die bereits im Report 2016 zu finden sind: Trojaner wie Gafgyt (19,04 %), Hajime und Tsunami stellen auch weiterhin eine ernstzunehmende Bedrohung für die IoT-Infrastruktur dar. Doch zunehmend gesellen sich Schadcodes zur direkten Monetarisierung fremder Ressourcen in die Spitze der IoT-Malware. So rangierten 2019 bereits zwei Krypto-Miner unter den Malware Top 10 für IoT.

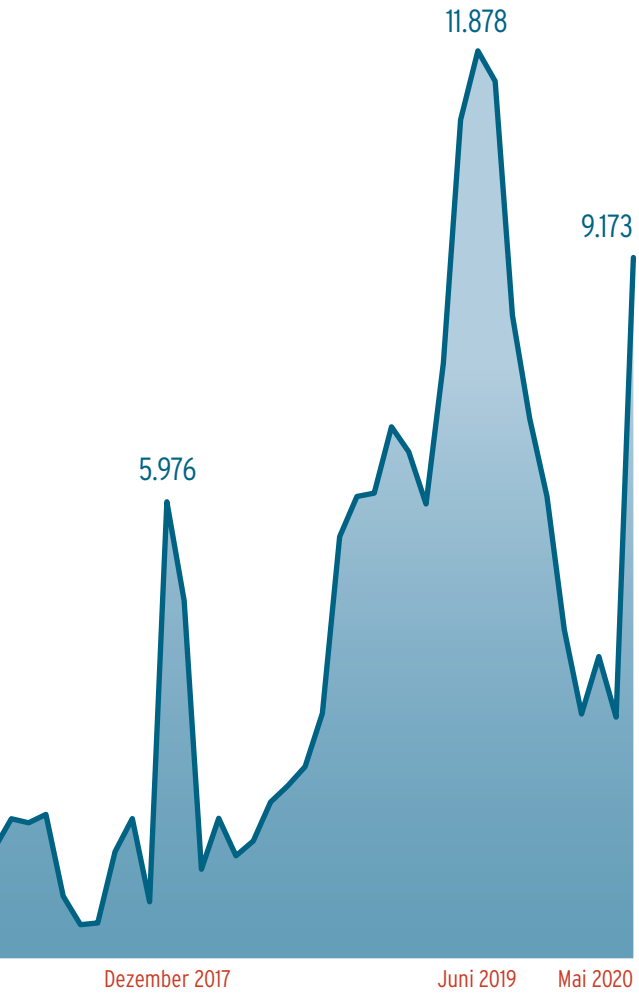
Einer davon, Coinhive, ist ein Schadcode mit ursprünglich zumindest semi-legalem Anwendungsbereich. Der JavaScript-Code diente anfänglich zur Browser-basierten Errechnung der Kryptowährung Monero und wurde, etwa als Bezahloption für Onlinedienste, von Website-Anbietern in ihre Onlineangebote eingebaut. Während der umstrittene Anbieter des Skripts im März des vergangenen Jahres seine Pforten schloss, nutzen Kriminelle den verfügbaren Java-Code offensichtlich weiter, um sich auf Kosten unbedarfter IoT-Nutzer zu bereichern. Insgesamt 4.697 neue Samples dieser Malware-Gattung stellte AV-TEST 2019 fest, und damit eine Zunahme gegenüber der Vorjahreswerte um über 46 Prozent. Es spricht also einiges dafür, dass sich der Einsatz fremder IT-Ressourcen im IoT-Sektor für Kriminelle rechnet. Auf anderen Plattformen genutzte „Business-Modelle", wie etwa die digitale Erpressung durch Sperren von Geräten, werden aktuell von Kriminellen zwar erprobt, konnten sich bisher jedoch noch nicht durchsetzen. Dafür spricht unter anderem die noch geringe Verbreitung erfasster IoT-Ransomware, die 2019 bei genau 56 Samples lag. Doch mit zunehmender Durchsetzung von IoT-Geräten in der industriellen Fertigung sowie der medizinischen Versorgung könnte in absehbarer Zeit auch die digitale Schutzgeld-Erpressung durch Sabotage-Androhung von IoT-Geräten bittere Realität werden. Gerätehersteller und Serviceanbieter beider Sektoren täten darum gut daran, sich dieser Gefahr bewusst zu sein und ihr zu begegnen.

IoT/Linux:
Entwicklung neuer Backdoors
2010 - Q1 2020



TOP 10 IoT-Malware 2019

1	MIRAI	40,84 %
2	GAFGYT	15,04 %
3	VIT	4,36 %
4	AGENT	1,32 %
5	HAJIME	0,88 %
6	TSUNAMI	0,84 %
7	COINHIVE	0,70 %
8	BITCOINMINER	0,62 %
9	DOFLOO	0,53 %
10	SHELLDL	0,40 %



Trend 2020

Die IoT-Erfassungszahlen des ersten Quartals des laufenden Jahres liefern bereits einige Rückschlüsse auf die zu erwartende Malware-Entwicklung für vernetzte Geräte. So erhöht sich die Rate der zur Infektion von IoT-Infrastruktur eingesetzten Trojaner merklich von knapp 40 auf über 65 Prozent.
Und die Steigerung der Rate neu entwickelter Krypto-Miner entspricht der vorangegangenen Analyse. Diese Schädlinge erhöhten ihren Anteil am Malware-Gesamtaufkommen gegenüber dem vergangenen Jahr von 1,15 auf 4,55 Prozent.

AV-ATLAS unterstützt Anbieter mit Echtzeitdaten zu IoT-Angriffen

Mit dem Launch der IoT-Sektion in der Threat Intelligence Platform AV-ATLAS (av-atlas.org) bietet das AV-TEST Institut nun auch Echtzeit-Bedrohungs-analysen nahezu aller relevanten IoT-Plattformen zur Orientierung von Nutzern sowie zur Unterstützung von Herstellern an. Über das kostenlos nutzbare Internetangebot lassen sich sowohl Informationen zu vergangenen wie laufenden Angriffen, darunter genutzte Logins, Ursprungsserver, Art der Angriffe und dabei genutzte Befehle, als auch eingesetzte Malware und deren genaue Analyse abrufen.

AV TEST
av-test.org

Die AV-TEST GmbH überprüft und zertifiziert ständig auf dem Markt relevante Smart Home-Produkte und IoT-Lösungen. Die aktuellen Testergebnisse können kostenlos über den IoT-Security-Blog unter https://www.iot-tests.org/ abgerufen werden.

Teststatistiken

Mit selbstentwickelten Analysesystemen und ausgeklügelten Testverfahren garantiert AV-TEST unabhängige Prüfungen für IT-Sicherheitsprodukte und ist so seit über 16 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 16 Jahren kontinuierlich auf über 40 Servern mit einer Speicherkapazität von mehr als 2.500 Terabyte. Zum Veröffentlichungsdatum dieses Jahresreports beinhaltete die AV-TEST Datenbank knapp 700 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. 2019 wurden so über 365 Produkttests allein für Privatanwender- und Unternehmensprodukte durchgeführt. Dabei wurden pro Produkt 84.477 Malware-Attacken gefahren sowie 8.999.133 einzelne Datensätze für Fehlalarmtests eingesetzt und ausgewertet. Im gesamten Jahr 2019 waren das 4.368.921.256 von den Testexperten zu überprüfende Datensätze. In den monatlichen Android-Tests überprüften die Tester über das Jahr insgesamt 153 Produkte. Dabei musste sich jede überprüfte Sicherheits-App gegen 51.548 spezielle Android-Schädlinge zur Wehr setzen. Zur Gegenprobe erfassten die Experten zudem über 22.825 Scans sicherer Apps pro Produkt, um die Anfälligkeit für Fehlalarme zu überprüfen. Im Labor wurden in Tests von Sicherheitsprodukten für Android also allein 7.886.844 Scan-Vorgänge analysiert und reproduzierbar ausgewertet. 4.103.154 Scans entfielen hierbei auf das speziell entwickelte Android-Security-Cluster, das parallele Echtzeittests von Android-Security-Lösungen ermöglicht.

1.000.000 SPAM-MAILS

4.368.921.256
2019 ÜBERPRÜFTE DATENSÄTZE

3 Mio
DATEIEN PRO TAG

500.000
URLs

40
SERVER

2.500
TERABYTE

Über das AV-TEST Institut

Die AV-TEST GmbH ist das unabhängige Forschungsinstitut für IT-Sicherheit aus Deutschland. Seit mehr als 15 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 selbstentwickelte 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 ebenfalls auf den Gebieten der Sicherheit von IoT- und eHealth-Produkten, Anwendungen für Mobilgeräte sowie in dem Bereich Datenschutz von Anwendungen und Dienstleistungen.

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