ZAHLEN UND FAKTEN

SECURITY REPORT 2017/18

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Der AV-TEST Sicherheitsreport

Die Anzahl neu entwickelter Schadprogramme bleibt auf einem konstant hohen Niveau. Doch die seit 2016 messbare Stagnation ist trügerisch, denn sie erlaubt ausschließlich quantitative Aussagen zum Gefahrenstand. Aussagen zur Gefährlichkeit kursierender Malware sowie zu den daraus resultierenden Schäden geben diese Messwerte nicht wieder. Doch hier sind die Aussichten weniger rosig: Die Schadensummen steigen, ebenso wie gegen Ende des Jahres die Anzahl neu programmierter Malware wieder zunimmt. Von Entspannung also keine Spur, wie der diesjährige Sicherheitsreport des AV-TEST Instituts belegt.

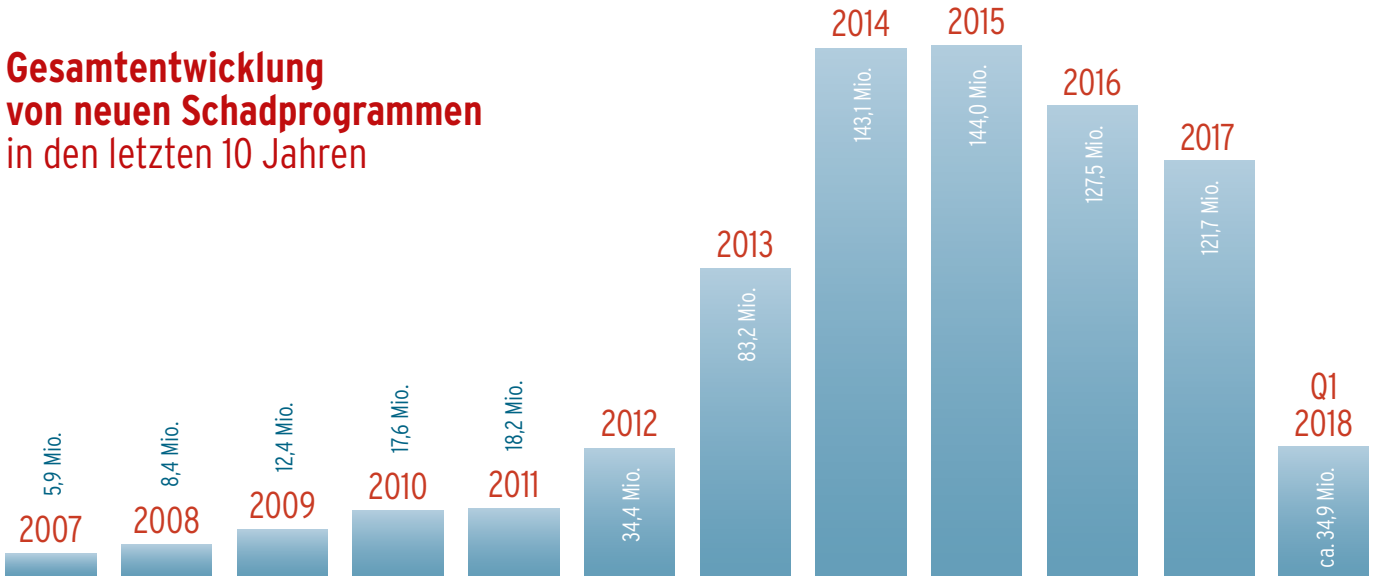
Malware-Entwicklung auf hohem Niveau

Für das Jahr 2016 verzeichneten die Erfassungssysteme rückläufige Zahlen neu entwickelter Malware, und das AV-TEST Institut prognostizierte diese Entwicklung auch für das Folgejahr. Zu Recht, wie die 2017er Messungen beweisen: Auch im zurückliegenden Jahr blieb die Anzahl neu entwickelter Schadprogramme unter den Zahlen des Vorjahres – zumindest in den ersten drei Quartalen. Insgesamt ist dieser Rückgang rechnerisch zwar nachweisbar, allerdings keine signifikante Veränderung. Wurden im Jahr 2016 genau 127.473.381 neue Malware-Samples entdeckt, waren es 2017 immer noch 121.661.167. Die Entwicklungsgeschwindigkeit neuer Malware, auf die Schutzsysteme reagieren müssen, sank damit minimal von 4,0 auf 3,9 neue Schadprogramme pro Sekunde.

Trend: verdoppelte Malware-Entwicklung

Seit September 2017 wandelt sich diese Entwicklung allerdings dramatisch und dreht sich ins Gegenteil: Seit Oktober letzten Jahres verzeichnen die Erfassungssysteme des AV-TEST Instituts nahezu eine Verdoppelung der monatlichen Malware-Neuentwicklungsraten. Lagen die Messwerte erfasster Neuentwicklungen im Oktober 2016 noch bei knapp 7.629.305 Samples, liegen sie im Monat des Folgejahres bei 17.445.659. Der letzte Oktober ist damit der Monat mit der zweithöchsten je gemessenen Anzahl neu entwickelter Schadprogramme seit Erfassungsbeginn durch AV-TEST. Nur im August des Jahres 2014 war eine noch größere Malware-Welle zu verzeichnen.

Gesamtentwicklung von neuen Schadprogrammen in den letzten 10 Jahren

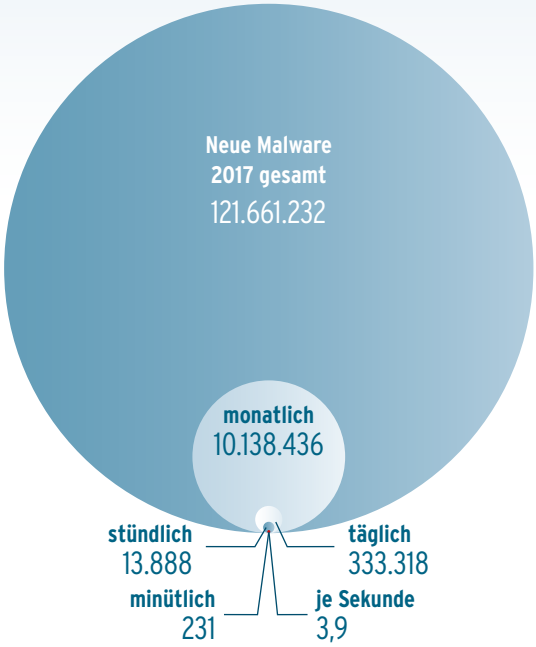


2017 vergleichbar mit 2014

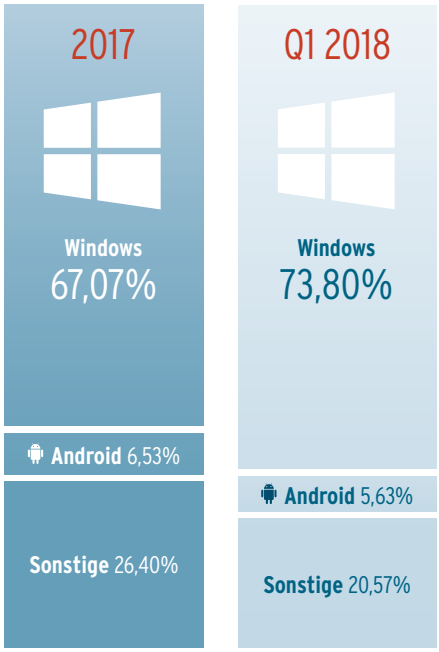
Das zurückliegende Jahr bot für Cyberkriminelle ähnlich gute Grundlagen zur Verbreitung von Malware: Mit „Cloudbleed" ergab sich für Kriminelle eine massive Sicherheitslücke in der auf Millionen Websites eingesetzten Serversoftware von Cloudflare. Die ebenfalls millionenfach genutzte Freeware „CCleaner" wurde von Angreifern zur Verbreitung von Malware eingesetzt. Und das Bekanntwerden der vorher lange heimlich durch die NSA genutzten Sicherheitslücke „Eternal Blue" bot Kriminellen die Möglichkeit, umfangreiche Ransomware-Kampagnen mit Schädlingen wie „WannaCry", „NotPetya" und „Bad Rabbit" zu starten, die nach wie vor anhalten, wenn auch mit sinkendem Wirkungsgrad.

Das hohe Malware-Aufkommen des letzten Quartals in 2017 spiegelt einen deutlichen Trend wider, denn die Messungen der Folgemonate liefern nahezu identisch hohe Werte und zeigen eine Verdopplung der Sample-Zahlen im Vergleich zu den Monaten des Vorjahres. Eine beunruhigende Tendenz, die sich in den Messungen des 1. Quartals 2018 fortsetzt. Die Malware-Datenbank von AV-TEST verzeichnete zu diesem Zeitpunkt insgesamt 771.077.699 Schadprogramme für alle bekannten Betriebssysteme. Ein guter Virenschutz ist und bleibt also weiterhin ein klares Muss.

Durchschnittliche Bedrohungslage durch neue Malware 2017



Malware-Erkennung nach Betriebssystem



Ransomware auf dem Rückzug?

Neben der rein quantitativen Einschätzung der Bedrohungslage anhand kursierender Malware-Samples bietet der Rückblick auf das vergangene Jahr im Vergleich zum 1. Quartal 2018 zudem weitere interessante Fakten zur ökonomischen Entwicklung der „kriminellen IT-Industrie". Exemplarisch dafür sind etwa die Verbreitungszahlen von Ransomware, die im 1. Quartal 2018 signifikant sinken. Allerdings lässt diese kurzfristige Beobachtung aufgrund der starken Schwankungen der bisherigen Ransomware-Entwicklung noch keine festen Rückschlüsse zu, sondern beschreibt lediglich den aktuellen Trend, den es weiter zu beobachten gilt. Denn als Einkunftsquelle bleibt Ransomware für Kriminelle nach wie vor attraktiv, was sowohl an der Möglichkeit der breiten Streuung per E-Mail oder über infizierte Websites, als auch an der weiterhin hohen Zahlungsbereitschaft der Opfer, insbesondere im Unternehmensbereich, liegt. Doch offensichtlich konnte sich die Cybercrime-Industrie neue Geschäftsmodelle mit noch höherem „Return on Investment" erschließen, die mehr Gewinn bei gleichzeitig geringerem Aufwand ermöglichen.

Zeitalter der Kryptominer bricht an

Und tatsächlich bietet sich Kriminellen dank des Booms von Krypto-Währungen wie Bitcoin, Litecoin und Ethereum im letzten Jahr ein neues, wirtschaftlich extrem attraktives und zukunftstaugliches Geschäftsmodell. Das profitiert ebenso wie Ransomware von der geringen Gefahr der Nachverfolgbarkeit anonymer Krypto-Währungen, allerdings bei deutlich höheren Gewinnmargen und noch geringerem Aufwand. Die Rede ist von Schadcode, der digitale Gewinne sofort und ohne Umwege auf anonyme Onlinekonten von Cyberkriminellen schaufelt und Gewinnverluste – etwa durch zahlungsunwillige Opfer, die Beschränkung auf bestimmte Betriebssysteme und Geräteklassen sowie zusätzlichen Verwaltungsaufwand – minimiert. Und so verwundert es nicht, dass die Anzahl von Schad–programmen, die heimlich die Leistung infizierter Geräte zum Errechnen digitaler Währung missbraucht, explosionsartig ansteigt. Aus diesem Grund widmet dieser Sicherheitsreport Kryptomining-Malware ab Seite 11 ein eigenes Kapitel und weist die Zahlen zur Entwicklung der neuesten Malware-Generation zusätzlich in den folgenden Kapiteln zum Sicherheitsstatus einzelner Betriebssysteme gesondert aus.

Windows weiter unter Feuer

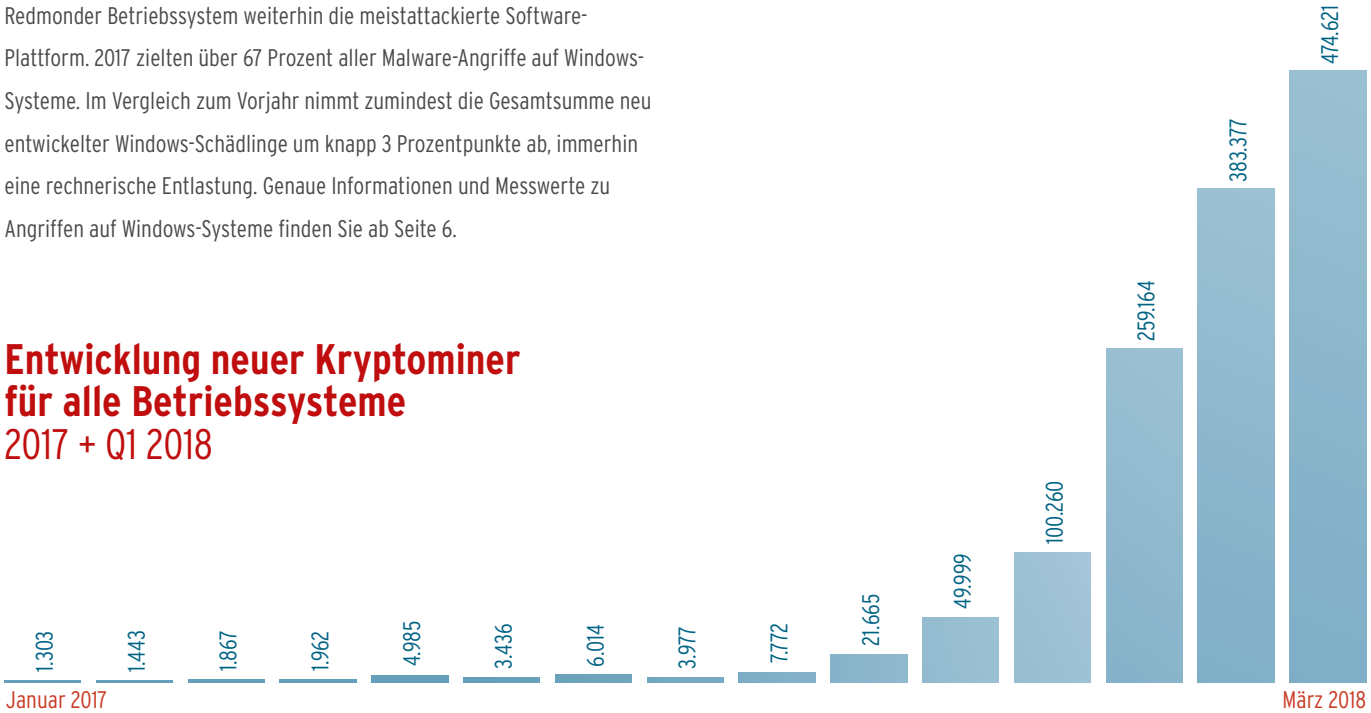
Wer Malware-Angriffe im großen Stil wirtschaftlich effizient planen und umsetzen will, pflanzt seine Schädlinge am besten in Schwachstellen des weltweit meistverbreiteten Software-Ökosystems. Und so ist und bleibt das Redmonder Betriebssystem weiterhin die meistattackierte Software-Plattform. 2017 zielten über 67 Prozent aller Malware-Angriffe auf Windows-Systeme. Im Vergleich zum Vorjahr nimmt zumindest die Gesamtsumme neu entwickelter Windows-Schädlinge um knapp 3 Prozentpunkte ab, immerhin eine rechnerische Entlastung. Genaue Informationen und Messwerte zu Angriffen auf Windows-Systeme finden Sie ab Seite 6.

Android-Schutz weiter kritisch

Im Gegenzug nahm die Angriffsintensität auf Googles Mobil-Plattform weiter zu: 2017 zielten 6,53 Prozent aller Schadprogramme auf Android-Geräte. Im Vergleich zum Vorjahr eine Zunahme von 0,88 Prozentpunkten. Was marginal klingt, hat in Wirklichkeit eine durchschlagende Wirkung, denn bisher kommt auf den wenigsten Mobilgeräten unter Android eine Sicherheits-App, geschweige denn wirkungsvoller Virenschutz zum Einsatz. Gleichzeitig läuft auf mehr als jedem dritten weltweit genutzten Android-Gerät eine veraltete Version des Betriebssystems (Version 1.1 bis 5.1.1), für die keine Sicherheits-Updates mehr verfügbar sind. Mit der aktuellen, uneingeschränkt mit Sicherheits-Updates versorgten Android-Version 8 aka „Oreo“ sind nicht mehr als 5,2 Prozent aller Android-Nutzer unterwegs!

Dennoch lassen sich auf ungesicherten Geräten weiterhin Versionen der meisten Apps nutzen, darunter auch Online-Banking-Apps und andere Applikationen, mit denen kritische Informationen übermittelt und rechtsgültige Geschäfte abgeschlossen werden. Für Angreifer könnte die Situation kaum besser sein. Denn das massenhafte Vorhandensein schlecht oder gar nicht geschützter Geräte erspart die kosten- und zeitintensive Entwicklung neuer Schadprogramme. Warum Zeit und Geld für neue „Produkte“ verschwenden, wenn die alten noch ausreichend Ertrag bringen?

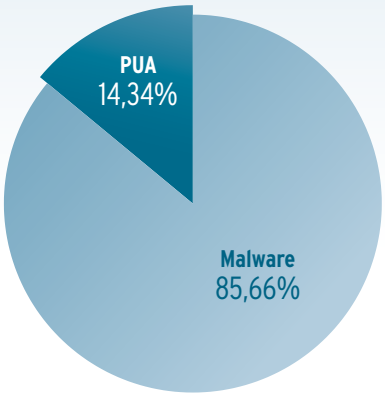
Entwicklung neuer Kryptominer für alle Betriebssysteme
2017 + Q1 2018



Entspannung für Apple?

Sahen sich Apple-Nutzer 2016 einer über 370-prozentigen Malware-Steigerungsrate gegenüber, kehrte 2017 zumindest rechnerisch Entspannung ein: Der Anteil am Malware-Gesamtaufkommen sank auf 0,23 Prozent. Dennoch ist dies kein Grund zur Entwarnung, denn auf die Frage „Welche Virenschutz-Software nutzen Sie?“ dürften immer noch viele macOS-Nutzer mit einem Schulterzucken antworten. Das bedeutet allerdings auch, dass Angreifern 0,21 Prozent der Gesamt-Malware ausreicht, um bei macOS-Nutzern erfolgreich zu sein. Dafür stand Angreifern 2017 ein Arsenal von 37.768 Schadprogrammen zur Verfügung. Was die alles drauf haben, erfahren Sie ab Seite 14.

Verhältnis PUA zu Malware 2017



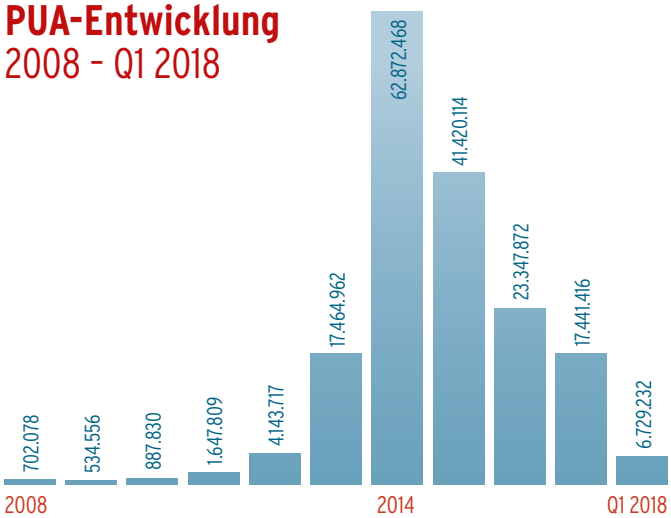
IoT-Geräte im Fadenkreuz

Bereits 2016 standen die Zeichen für Linux-basierte Systeme auf Sturm: Die Anzahl neu entwickelter Schadprogramme verdreifachte sich im Vergleich zum Vorjahr. Daran hat sich im Folgejahr nichts geändert. Im Vergleich zu 2016 erhöhte sich die Anzahl der Malware-Neuentwicklungen von 25.671 auf 64.087 Samples, so dass vor allem auf Linux aufbauende IoT-Geräte, von denen die meisten ohne Malware-Schutz im Netz stehen, leichte Beute werden dürften. Welche Gefahren auf Router, Smart-TVs und das weite und ständig wachsende Feld von Smart-Home-Geräten lauern und warum das Internet of Things besonders im Fadenkreuz von Cyberkriminellen steht, lesen Sie ab Seite 23.

Nutzer-Tracking rückläufig

Ganz ohne eine positive Nachricht soll der Blick auf die Entwicklung des letzten Jahres allerdings nicht enden. Und so bleibt zu berichten, dass das Ausspionieren des Nutzerverhaltens mittels potentiell unerwünschter Anwendungen (PUA) durch Unternehmen in 2017 weiter rückläufig war. Im Unterschied zu der von den AV-TEST Systemen erfassten Malware stellt PUA zwar keine direkte Bedrohung für befallene Systeme dar, allerdings erfassen solche Spionageprogramme heimlich Daten, blenden unerwünschte Werbung ein und können die Performance der Hardware spürbar herabsetzen. Darum war der zumindest für das letzte Jahr feststellbare Rückgang von PUA erfreulich.

PUA-Entwicklung 2008 - Q1 2018



Trend 2018

Dieser Sicherheitsreport umfasst neben dem Datenstand für das Jahr 2017 auch Messwerte der AV-TEST Analysesysteme für das erste Quartal 2018. So lassen sich schon jetzt mit Daten untermauerte Trends für das laufende Jahr erkennen.

War die Malware-Gesamtentwicklung 2017 noch rückläufig, steigt sie im 1. Quartal 2018 deutlich spürbar an. Bereits der Januar wartet mit klar erhöhten Malware-Zahlen auf. Mussten Virenscanner im Anfangsmonat des Vorjahres noch 8.852.322 neue Schadprogramme abwehren, waren sie in diesem Januar bereits 13.695.241 solcher Programme ausgesetzt. Dieser Trend setzt sich in den Messwerten des gesamten 1. Quartals 2018 konsequent fort.

Tiefergehende Analysen der hier dargestellten Gesamtzahlen finden sich in den einzelnen Kapiteln dieses Sicherheitsreports.

Sicherheitsstatus WINDOWS

Nach einer Phase der Entspannung steigt die Zahl der Angriffe durch neue Windows-Malware in 2017 wieder spürbar an. Doch nicht nur die Menge der Schadprogramme nimmt zu. Neue, ausgeklügelte Angriffsvarianten erschweren die Abwehr und verschaffen Cyberkriminellen entscheidende wirtschaftliche Vorteile.

Angriffsziel Nummer 1

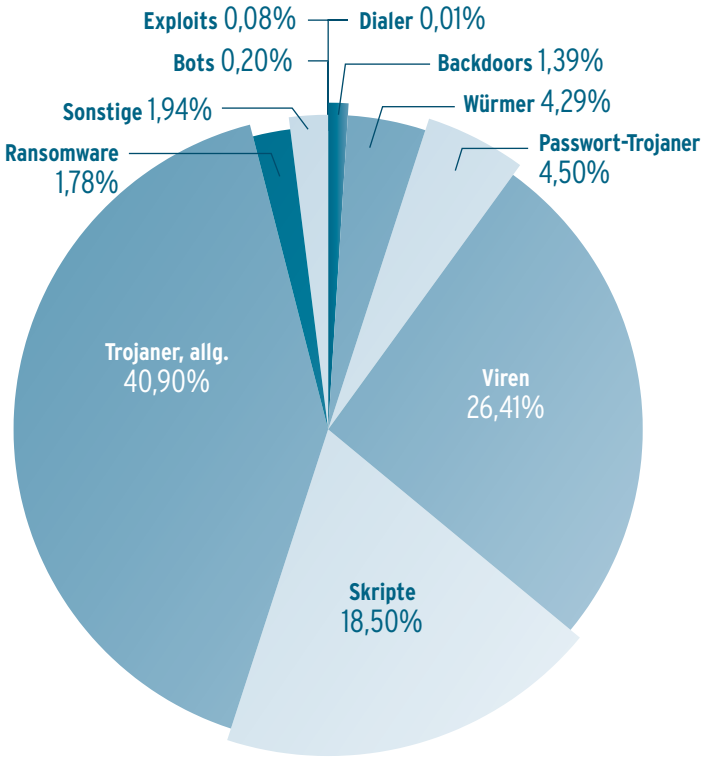
An weltweiten Nutzerzahlen gemessen ist und bleibt Windows das Betriebssystem Nummer 1. Das sehen auch die Akteure der „Malware-Industrie" so, und damit bleiben Microsoft-Systeme auch das Hauptangriffsziel von Cyberkriminellen. Während die Zahl der Malware-Neuentwicklungen seit 2015 sank, zog sie im letzten Jahr nach zwei Jahren wieder spürbar an. Und so ermittelten die Erfassungssysteme des AV-TEST Instituts für 2017 den Gesamtstand von 81.598.221 neu entwickelter Malware-Samples und verzeichnen gegenüber dem Vorjahr (71.430.700 Samples) eine Zunahme von über 14 Prozent. In der Gesamtschau aller Betriebssysteme zielten 2017 damit mehr als 67 Prozent aller Schadprogramme auf Windows-Nutzer.

Zwang zur Innovation

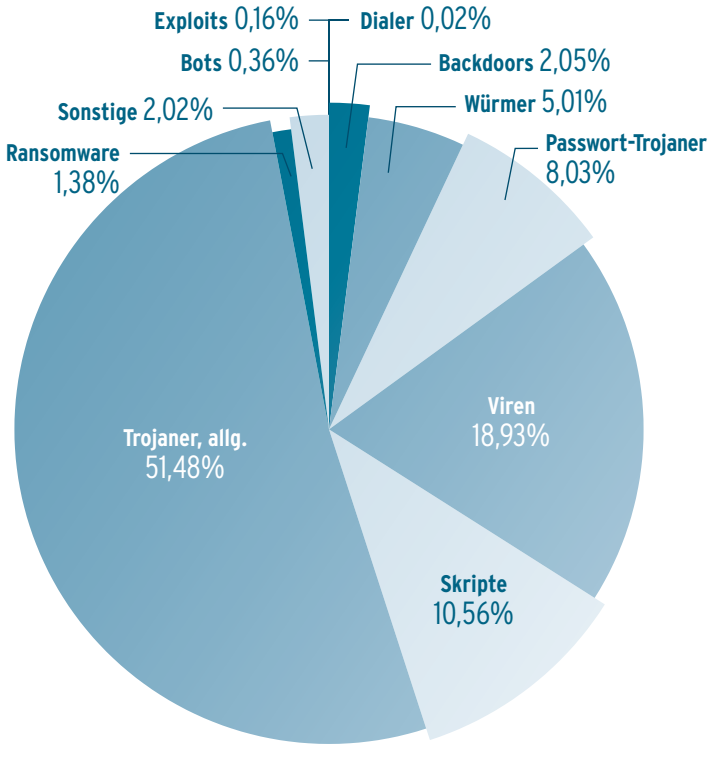
Eine Ursache für die zunehmende Aktivität bei der Entwicklung neuer Windows-Schädlinge könnte eine eigentlich positive Entwicklung sein. Denn im letzten Jahr gelang es Microsoft, das Immunsystem von Windows durch klare Verbesserung der Abwehrmechanismen des Betriebssystems erheblich zu steigern. So bewies die systemeigene Malware-Abwehr mit

Malware-Verteilung unter Windows

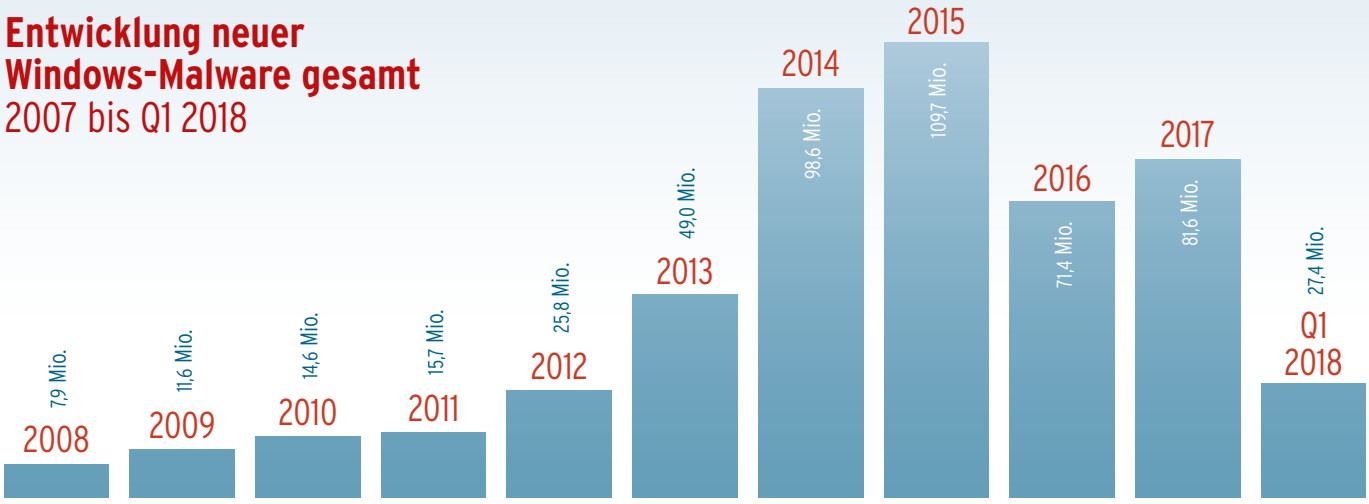
2017



Q1 2018



Entwicklung neuer Windows-Malware gesamt
2007 bis Q1 2018



„Windows Defender" und „Security Essentials" in den Jahrestests des AV-TEST Instituts deutlich verbesserte Erkennungsraten gegenüber den letzten Jahren.

Im Umkehrschluss bedeutet diese Entwicklung allerdings für Kriminelle, dass sie ihre „Produkte" den neuen Gegebenheiten anpassen müssen, sollen ihre Schadprogramme auf Windows-Systemen weiterhin wirtschaftlichen Erfolg versprechen. Das machte sich vor allem im letzten Quartal des letzten Jahres bemerkbar, denn seit Oktober 2017 verdoppelte sich die Anzahl der Malware-Neuentwicklungen gegenüber dem Vormonat. Dieser sprunghafte Anstieg schwächte sich in der Folge leicht ab, blieb seither aber weiter auf deutlich höherem Niveau als in den vorherigen Quartalen des Jahres 2017.

Malware-Verteilung unter Windows

Von welcher Form von Angriffen sich Kriminelle in 2017 den größten Erfolg versprachen, zeigt der Blick auf die Verteilung unterschiedlicher Malware-Arten für Microsoft-Betriebssysteme. Die quantitative Analyse der Verbreitung neuen Schadcodes gibt Auskunft darüber, in welche Malware-Gattung Kriminelle 2017 am meisten Zeit und Geld investierten und lässt zumindest vermuten, welcher kriminelle „Businessplan" bei der massenhaften Verbreitung von Schadcode am lukrativsten war. Dabei ist zu berücksichtigen, dass entsprechende Entwicklungen über das Jahr auch weiteren Faktoren unterliegen, etwa dem Bekanntwerden nutzbarer Sicherheitslücken in Betriebssystemen oder darauf laufender Standardanwendungen.

Tarnen, Täuschen, Ausspionieren, Stehlen

Mit immerhin 40 Prozent aller Schadprogramme für Windows dominierten Trojaner 2017 ganz klar die Waffenkammern von Cyberkriminellen, allerdings erfassen Schutzprogramme dabei Schädlinge aller Art unter diesem Sammelbegriff. Dass Kriminelle dieses Mittel wählen verwundert nicht, erlauben erfolgreich eingeschleuste Trojaner doch nahezu uneingeschränkte Schadwirkung auf befallenen Systemen. Über entsprechende Malware-Funktionen ermöglicht der Schadcode Angreifern Zugang zum System und bietet die Möglichkeit, beliebigen Schadcode nachzuladen. Neben der heimlichen Übertragung aller Arten gespeicherter Daten verfügen Trojaner zudem über ein umfangreiches Arsenal weiterer Schadfunktionen und gelten darum als „Schweizer Offiziersmesser" im Werkzeugkasten von Cyberkriminellen, mit denen sich Daten nicht nur stehlen, sondern auch unterdrücken, blockieren, löschen und verändern lassen.

Zudem bieten Trojanern ihren Meistern umfangreiche Spionagefunktionen; dazu zählen neben den Möglichkeiten, Kennwörter für diverse Onlinekonten abzugreifen oder der gezielten Suche nach bestimmten Dateien auch das heimliche Aktivieren von eingebauten Kameras und Mikrofonen. Diese Funktion macht sie unter anderem nicht nur für Kriminelle, sondern auch für Polizeien und staatliche Überwachungsorganisationen vieler Länder interessant.

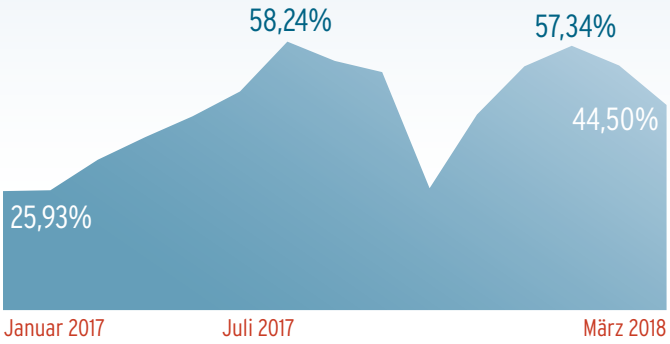
Zur ständig steigenden Attraktivität der Trojaner tragen neben ihrem flexiblen Schadcode aber auch die vielfältigen Möglichkeiten zu ihrer Verbreitung bei. Getarnt als E-Mail-Anhang oder kostenloser Programm-Download, eingebettet in andere Programme oder als Drive-by-Download beim Besuch infizierter Internetseiten – die Möglichkeiten, Trojaner im großen Stil zu streuen sind ebenso vielseitig wie ihre umfangreichen Schadfunktionen vielfältig sind.

Das untermauern auch die Zuwachsraten dieser Schädlingsgattung: Lagen Trojaner im letzten AV-TEST Sicherheitsreport mit 23,74 Prozent noch auf Platz 3 der Windows-Schadprogramme – hinter Viren (37,6%) und Würmern (25,44%) –, wendete sich das Blatt 2017 dramatisch. Dabei gilt es zu beachten, dass zum ohnehin hohen Trojaner-Wert der Malware-Statistik der Erfassungssysteme des AV-TEST Instituts noch weitere Unterformen dieser Schädlingsgattung addiert werden. Aufgrund ihrer besonderen Malware-Funktionen erfasst AV-TEST Banking-Trojaner und Ransomware gesondert und nicht unter dem Sammelbegriff „Trojaner".

TOP 10 Windows-Malware 2017

1	RAMNIT	21,54%
2	AGENT	13,78%
3	VIRUT	6,37%
4	VIRLOCK	6,25%
5	ALLAPLE	4,69%
6	VB	3,98%
7	SIVIS	2,39%
8	UPATRE	2,03%
9	INJECTOR	2,00%
10	KRYPTIK	2,00%

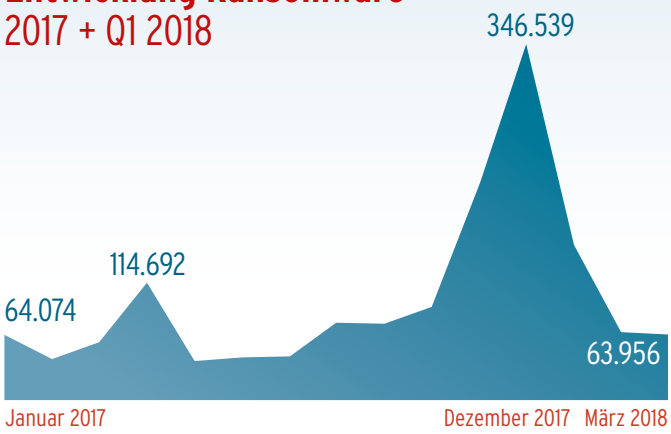
Entwicklung Trojaner, allgemein 2017 + Q1 2018



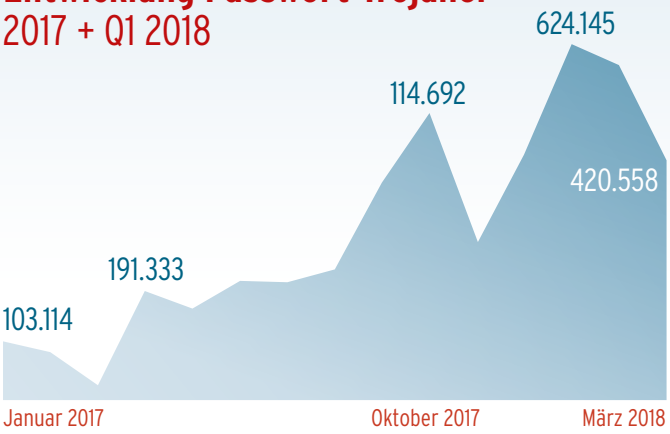
Das Jahr der digitalen Erpressung

Das Jahr 2017 war nicht nur medial das „Jahr der Ransomware", auch die von AV-TEST gemessenen Zuwachsraten bestätigen, dass sich digitale Erpressung als sicheres Geschäftsmodell der Cyberkriminellen etablierte. Im Vergleich zum Vorjahr steigt der Anteil der Erpresser-Trojaner von 0,94 auf 1,78 Prozent und verdoppelt sich damit annähernd. Trotz des geringen Anteils von Ransomware in Bezug auf alle erfassten Schadprogramme, ist das Erfolgskonzept dieser Malware nicht von der Hand zu weisen. Denn mit Ransomware erzielen Cyberkriminelle mit einem im Vergleich zu anderen Schadprogrammen deutlich geringeren Aufwand bereits bei geringen Opferzahlen schon hohe Gewinne. Und Dank anonymer Online-Währungen fließt das Geld sofort und direkt in ihre Kassen, ohne weiteren Aufwand und mit sehr überschaubarem Risiko, dafür aber mit maximalem Schaden für die Betroffenen.

Entwicklung Ransomware
2017 + Q1 2018



Entwicklung Passwort-Trojaner
2017 + Q1 2018



Attacken mit NSA-Unterstützung

Besonders drastisch fielen die Folgen der Ransomware „NotPetya“ aus. Allein das global agierende Logistikunternehmen Maersk meldete eine Schadensumme von mehreren hundert Millionen Dollar. Die Reederei transportiert mit seinen Containerschiffen knapp 20 Prozent des gesamten Welthandels. Durch den Angriff der Ransomware am 27. Juni 2017 erlitt es einen Totalausfall aller IT-Systeme: 45.000 Client-Rechner sowie 4.000 Server rund um den Globus seien ausgefallen, in einem zehntägigen Kraftakt habe man 2.500 verschiedene Programme neu installiert oder zurückgespielt, berichtet Maersk-Vorsitzender Jim Hagemann Snabe auf dem diesjährigen Weltwirtschaftsforum in Davos. Im Grunde sei man noch glimpflich davongekommen, so der Konzernlenker, denn normalerweise hätte ein Wiederhochfahren der globalen Maersk-Logistik ein halbes Jahr gedauert.

Auch andere Großunternehmen, darunter Pharmariese Merck, der durch den NotPetya-Angriff eine Schadensumme von über 300 Millionen beklagte, und das Logistikunternehmen FedEx gehörten zu den Opfern. Doch ebenso wie Maersk waren sie gar nicht das eigentliche Ziel der Ransomware-Attacke, denn eine Lösegeldforderung hat es während des Angriffs nie gegeben. Gemeinsam hatten alle Betroffenen, dass ihr Geschäftsfeld auch die Ukraine umfasst und sie dort dementsprechend Steuern zahlen müssen. Und so wurden sie Kollateralopfer eines gezielten Angriffs gegen die hauptsächlich in der Ukraine eingesetzte Steuersoftware MeDoc. Die Angreifer verbreiteten NotPetya vom 14. April bis zum 22. Juni in drei Angriffswellen als infiziertes Programm-Update der ukrainischen Steuer-Software. Mit großer Wahrscheinlichkeit handelte es sich bei NotPetya um einen gezielten staatlichen Cyberangriff gegen die Ukraine.

Bei den NotPetya-Attacken nutzten die Täter genau dieselben Windowslücken, die schon vorher für staatliche Angriffe herhalten mussten – allerdings kamen diese aus einer ganz anderen Ecke. Bereits im August 2016 veröffentlichte die Hackergruppe „Shadow Brokers“ Teile der Programmcodes einer Cyberwaffe, die sie bei einem Hack der NSA-Abteilung „Equation Group“ erbeutete. Diese 256 Mbyte große Datei ließ 2016 zumindest erahnen, welches Potential in dem staatlich entwickelten Schadcode steckt. Brisant wurde die Situation jedoch erst am 14. April 2017. An diesem Tag entschlossen sich die Shadow Brokers nämlich, den kompletten Code der Cyberwaffe im Internet zu veröffentlichen – die Geburtsstunde der Ransomware „WannaCry“.

Wie lange die NSA die nun frei zugänglichen Exploits namens „Eternal Blue“ im Server Message Block (SMB) nahezu aller Windows-Systeme (CVE-2017-0144) bereits nutzte, ist umstritten. Schätzungen gehen von über fünf Jahren aus. Fakt ist, dass Microsoft die Lücken des Netzwerkprotokolls unter der Kennung „MS17-010 – Kritisch“ am 14. März 2017 patchte. Am 12. Mai starteten die ersten groß angelegten Cyberattacken von WannaCry. Und wie sich herausstellte, war auf mindestens 230.000 Computern in 150 Ländern für zwei Monate nicht das entscheidende Sicherheitsupdate von Microsoft installiert

worden. Zu den Betroffenen zählten vor allem Krankenhäuser in Großbritannien, aber auch große Unternehmen wie FedEx, Renault, Nissan, die Deutsche Bahn sowie der chinesische Ölkonzern PetroChina. Sogar staatliche Stellen wie das russische Innenministerium, das rumänische Außenministerium und Internetdienstleister wie Telefonica und MegaFon sahen sich plötzlich digitaler Erpressung, zu zahlen in Bitcoin, ausgesetzt.

Im Oktober 2017 legte die vorwiegend auf den osteuropäischen Raum gerichtete Ransomware „Bad Rabbit" die russische Nachrichtenagentur Interfax sowie den Flughafen von Odessa, die Metro in Kiew sowie einige ukrainische Ministerien lahm. Die Malware tauchte aber auch in Russland, der Türkei, Japan und Südkorea sowie Deutschland und den USA auf. Genauso verrichteten „alte Bekannte" aus der Ransomware-Familie, etwa die Schadcodes „Cerber" und „Locky" (siehe Sicherheitsreport 2016/17) auch noch 2017 ihr schädliches Werk.

Lagen Internet-Würmer 2016 mit über 25 Prozent noch auf Platz 2 der von Cyberkriminellen eingesetzten Schadprogramme, wurden sie 2017 so gut wie gar nicht mehr weiterentwickelt. Mit gerade noch 4,29 Prozent gehörten sie im letzten Jahr zu einer schnell aussterbenden Gattung.

Trend 2018

Im ersten Quartal dieses Jahres zeigt sich die Entwicklung neuer Ransomware stark rückläufig. Der Anteil im Bezug zur Malware-Gesamterfassung sank von 1,78 auf 1,38 Prozent. Ein messbarer Wert, der allerdings keine Aussagen über die Entwicklung dieser Schädlingsgattung im gesamten Jahr 2018 erlaubt. Vermuten lässt sich jedoch, dass Cyberkriminelle durch die mit Ransomware gemachten Erfahrungen ein neues und lukrativeres, ebenfalls auf Krypto-Währungen basierendes Erwerbsmodel gefunden haben, das noch attraktiver ist. Aus diesem Grund widmet dieser Sicherheitsreport der Schädlingsgattung der Coinminer ein eigenes Kapitel.

Die Rate der Neuentwicklungen von Trojanern allgemein zieht um über 10 Prozent an. Damit ist mindestens jeder zweite im 1. Quartal 2018 programmierte Schadcode ein Trojaner. Noch deutlicher fällt die Entwicklung der gesondert erfassten Passwort- und Banking-Trojaner aus: Deren Anzahl verdoppelt sich fast von 4,5 auf 8,03 Prozent. Im Gegenzug sinkt die Verbreitung klassischer Viren weiter auf unter 20 Prozent des Gesamtanteils der erfassten Malware.

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.

KRYPTO-MINER
vor dem Durchbruch

Die Anonymität vieler Krypto-Währungen garantiert Cyberkriminellen optimale Geschäftsgrundlagen. Denn Bitcoin & Co erlauben das direkte Abkassieren von Opfern, ohne das Zwischenschalten von Handlangern. Das minimiert das Risiko bei gleichzeitiger Einsparung von „Personalkosten". Darum setzen auch kriminelle Vordenker auf die Blockchain. 2017 entwickelte die Malware-Industrie zunehmend Schadcode zum Schürfen digitaler Währungen unter Missbrauch fremder Ressourcen.

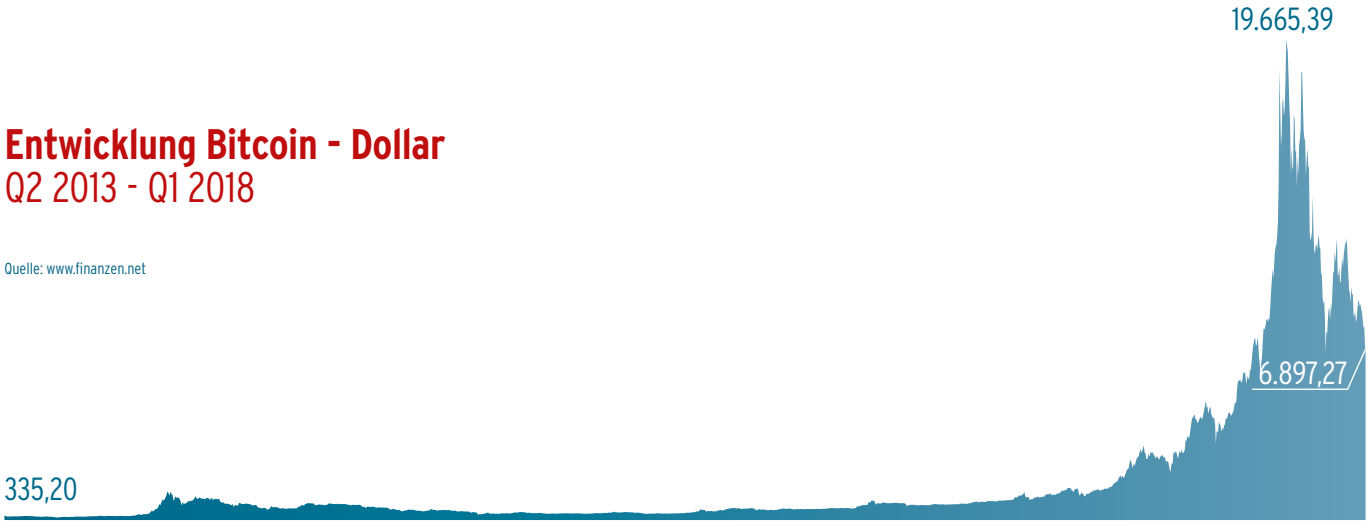
Anonymität ist attraktiv

Durch den erfolgreichen Einsatz von Ransomware sammelten Cyberkriminelle bereits positive Erfahrungen mit Krypto-Währungen. Denn der Einsatz digitaler Währungen, zu deren Grundprinzipien es gehört, anonym nutzbar zu sein, ist für Kriminelle per se schon attraktiv. Das Fehlen der Regulierung durch Banken oder andere gleichartige Instanzen ist ein weiterer Grundpfeiler aller aktuell über 4.500 existierenden Krypto-Währungen. Wirklich gehandelt werden davon zwar nur ungefähr 1.000, doch im Unterschied zum ersten 2009 gestarteten Kryptogeld Bitcoin lassen alle anderen einen nahezu komplett anonymen Austausch großer Summen zu. Als Startwährung mit der mit Abstand größten Marktkapitalisierung stehen große Bitcoin-Summen beim Wechsel in wahre Münze allerdings unter besonderer Beobachtung. Mit 153.225 Mio. US-Dollar macht die bekannteste digitale Währung derzeit über 37 Prozent des Gesamtvolumens aller aktuellen Krypto-Währungen aus. Bitcoin-Wechsel können nur auf ein reguläres Bankkonto erfolgen und sind damit personalisiert und wieder verfolgbar. Seit 2014 analysieren und überwachen Unternehmen wie Chainalysis Bitcoin-Transfers, dokumentieren diese und stellen unter anderem für die US-Steuerbehörde Zusammenhänge zwischen Blockchain-Adressen und realen Konten her.

Kriminelle springen darum auf andere, weniger beobachtete Cyber-Währungen mit weiter Verbreitung wie Litecoin, Ethereum, EOS, Tronix und Monero auf. Auch diese folgen dem Grundsatz der anonymen Finanzabwicklung. Das bedeutet, dass sowohl die Besitzer digitaler Coins als auch die Menge der von ihnen besessenen Krypto-Währung dank individueller Verschlüsselung anonym bleiben. Gleiches gilt für Transaktionspartner. Zwar sind alle innerhalb eines Währungssystems getätigten Transaktionen öffentlich ersichtlich, allerdings weiß niemand, wer diese tätigt.

Entwicklung Bitcoin - Dollar
Q2 2013 - Q1 2018

Quelle: www.finanzen.net

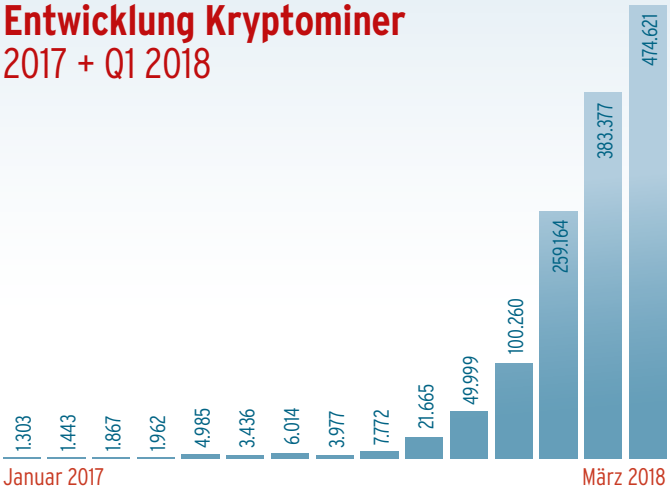


Stehlen oder Minen

Prinzipiell gibt es für Kriminelle zwei Wege, an die digitale Währung zu gelangen. Der erste besteht darin, fremde Rechner nach gespeicherten Coins zu durchsuchen und diese zu stehlen. Das Guthaben einer Krypto-Währung besteht ausschließlich aus einem entsprechenden Zahlencode. Der gibt Auskunft über die Anzahl der Coins innerhalb des Systems einer Krypto-Währung. Solche Zahlencodes können als geheimer privater Schlüssel gespeichert, aber beispielsweise auch in Strichcode übersetzt und ausgedruckt werden. Damit sind die Schlüssel für die Verfügung über ein Guthaben allerdings auch leicht aufzuspürende Beute für Computerkriminelle. Sie lassen sich ähnlich wie Passwörter mit Schadprogrammen ausspähen und abgreifen. Attacken sind wegen der geringen Verbreitung allerdings nur lohnend, wenn das Opfer bekannt ist, gezielt angegriffen werden kann und über eine ausreichende Menge schlecht geschützter Coins verfügt. Denn solch gezielte Angriffe erfordern einiges an Planung und sind entsprechend aufwendig.

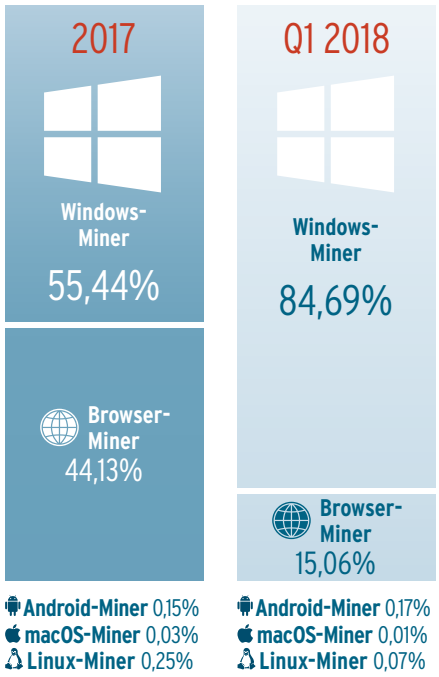
Der zweite Weg, auf Kosten anderer an Krypto-Währung zu gelangen, erfordert einen deutlich geringeren Aufwand und ist darum deutlich lukrativer: das Mining von Krypto-Währung durch den Missbrauch fremder Rechenressourcen. Die Rechenleistung fremder Hardware wird eingesetzt, um innerhalb der Krypto-Blockchain kryptographische Aufgaben zu lösen. Als „Belohnung" für das richtige Ergebnis gibt die entsprechende Blockchain Anteile der in ihr vordefinierten Währung aus. Beim Start einer Währungs-

Entwicklung Kryptominer
2017 + Q1 2018



Blockchain sind die Rechenaufgaben zum Schürfen noch relativ simpel und können auch mit geringer Rechenlast erledigt werden. Jede Krypto-Währung ist ein in sich geschlossenes System mit einer vorher festgelegten Coin-Menge und einem festgelegten Gesamtwert. Mit jedem Coin, der innerhalb eines solchen Währungssystems geschürft wird, steigt jedoch die Komplexität der Rechenaufgaben und somit die notwendige Rechenleistung. Nutzer können Pools bilden und die Rechenleistung ihrer Hardware koppeln, um gemeinsam zu schürfen. Teils wird aber auch in Grauzonen agiert, indem die Mining-Funktion zum Beispiel in kostenlosen Applikationen für Smartphones und Tablet-PCs versteckt wird. Auch Browser-Addons, mit denen Betreiber von Onlinediensten ihre Nutzer während der Verweilzeit auf der Website für sich schürfen lassen, finden zunehmend Verbreitung.

Kryptominer auf Betriebssystemen



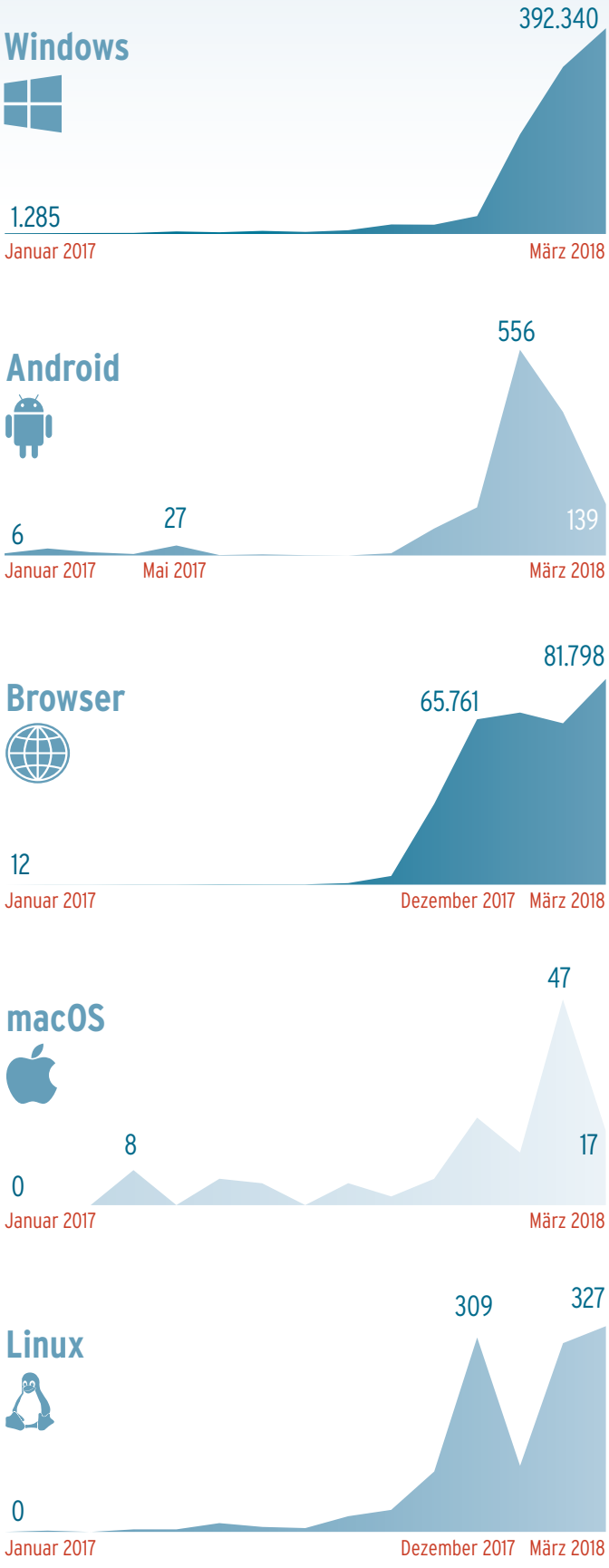
Und genau hier setzen auch die Cyberkriminellen an: Anstatt die Cyberwährung von ihren Opfern über Ransomware zu erpressen, gingen sie ab dem 4. Quartal 2017 zunehmend dazu über, die Rechenleistung infizierter Hardware zum Coinmining zu missbrauchen. Die Erfassungssysteme des AV-TEST Instituts messen seit September letzten Jahres einen signifikanten Anstieg der Samples von Coinmining-Malware, der bis ins 1. Quartal 2018 exponentiell zulegt. Lag die Zahl der Neuentwicklung von Mining-Malware Mitte des Jahres noch bei durchschnittlich 3.500 Samples pro Monat, verdoppelte sich deren Rate ab September und steigt seither quasi ungebremst auf bis zu 470.000 neue Samples pro Monat. Bis zum Abschluss dieses Reports lag die Gesamtsumme der von AV-TEST seit 2010 erfassten Mining-Samples bereits bei über einer Million.

Windows wird Mining-Plattform

Der Blick auf die Verteilung der Mining-Malware nach Betriebssystemen zeigt deutlich, dass sich die Kriminellen 2017 noch in der Entwicklung des Geschäftsmodells befinden. Zu diesem Zeitpunkt zielen über die Hälfte aller Coinminer auf die Infektion von Windows-Systemen (55,44 Prozent). Die andere Hälfte (44,13 Prozent) versucht, die Rechenleistung infizierter Hardware über Browser und andere Internetverbindungs-Software abzusaugen.

Das ändert sich im 1. Quartal 2018 drastisch, denn die Anzahl von Coinminern für Windows-Systeme steigt überproportional um knapp 30 Prozent auf 84,69 Prozent an. Damit legen sich Cyberkriminelle, wie auch bei anderer Malware, auf die für sie bewährten Windows-Systeme als Hauptangriffsziel fest. Ob es sich lediglich um einen Trend handelt, bleibt abzuwarten. Möglicherweise ist die zu erbeutende Rechenleistung gegenüber Plattformen wie Android oder unterschiedlichen IoT-Geräten ein Argument, auf Windows zu setzen. Allerdings ist hier aufgrund der hohen Akzeptanz von Antiviren-Software auch die Gefahr höher, dass neu programmierte Malware schnell erkannt wird. Es bleibt abzuwarten, ob kriminelle Software-Entwickler auf andere, weniger gut überwachte Betriebssysteme ausweichen werden, sich quasi ungeschützte Ressourcen von IoT-Geräten zunutze machen oder systemunabhängig mit Browser-Malware weiterarbeiten. Bei dieser Betrachtung darf nicht vergessen werden, dass Krypto-Währungen selbst für nicht kriminelle Ökonomen eigentlich noch Neuland darstellen. Bereits jetzt Malware für Krypto-Währungen einzusetzen spricht insofern für die Innovationsgeschwindigkeit der Cyberkriminellen. Aufgrund zumeist fehlender Regulierung in Bezug auf neue Technologien sind solche „neuen Märkte" für Kriminelle vor allem in deren Anfangsphasen von besonderem Interesse.

Entwicklung Kryptominer 2017 + Q1 2018



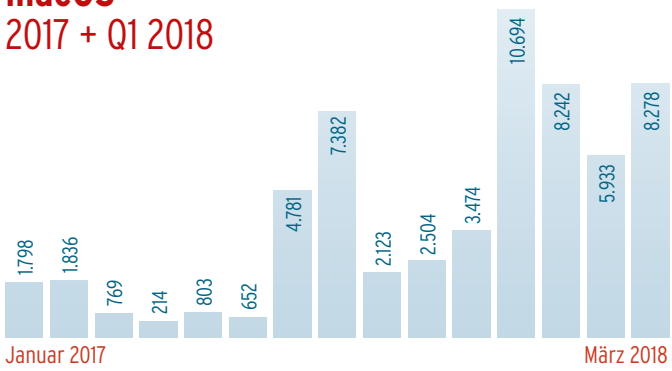
Sicherheitsstatus macOS

Einerseits sind Apple-Nutzer nur von einem verschwindend geringen Anteil neu programmierter Malware betroffen. Andererseits läuft auch nicht auf jedem Mac ein vernünftiges Virenschutzprogramm. Wie die Malware-Entwicklung für das Betriebssystem aus Cupertino zeigt, wäre das aber ratsam. Denn die Malware-Quote für das Apple-Universum steigt kontinuierlich an.

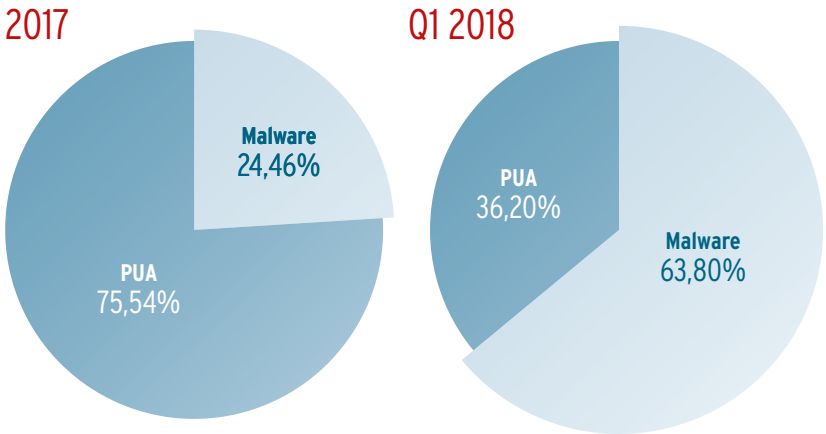
macOS-Malware verfünffacht

Im Sicherheitsreport des letzten Jahres verzeichneten die Messsysteme des AV-TEST Instituts eine dramatische Zunahme der Malware-Zahlen für macOS um 370 Prozent zum Vorjahr. Diese Entwicklung war 2017 nicht zu stoppen. Während 2016 insgesamt 6.959 neuprogrammierte Malware-Samples auf Apple-Rechner zielten, verfünffachte sich dieser Wert im zurückliegenden Jahr auf 37.030 neue Malware-Samples. Dabei steigt die Menge der für macOS entwickelten Schadprogramme seit zehn Jahren beständig an und erreicht zum Abschlusstermin dieses Reports einen Gesamtwert von insgesamt 78.929 Samples.

Malware-Entwicklung macOS
2017 + Q1 2018



Schädlingeverteilung macOS



Entwicklung macOS-Malware
2008 - Q1 2018

Malware schlägt PUA

Damit übertrifft neue Malware für Mac hinsichtlich der Neuentwicklung von Schädlingen im Dezember erstmals die Anzahl unerwünschter Spionage-Anwendungen (PUA). Stellten die Spionage-Tools der Werbeindustrie bis Dezember 2017 noch die hauptsächliche Bedrohung für Apple-Nutzer – und vor allem für deren Privatsphäre – dar, hat sich das Blatt seither gewendet und die Malware-Schreiber übernehmen jetzt das Ruder.

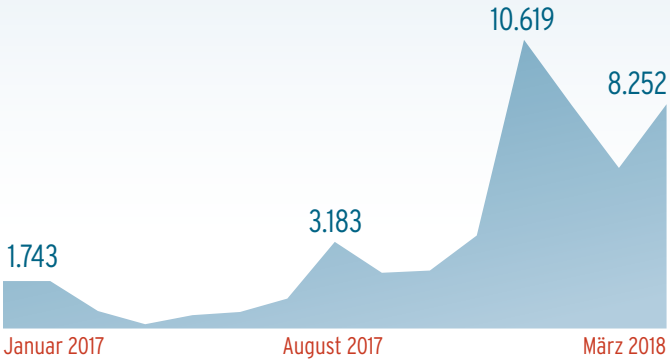
macOS unter Trojaner-Beschuss

In 2017 handelt es sich bei vier von zehn Schadprogrammen für macOS um Trojaner (40,93 Prozent). Ansonsten spielen schädliche Skripte mit 12,66 Prozent eine herausragende Rolle bei der durch die AV-TEST Systeme erfassten und analysierten Schadsoftware. Viren, Würmer und andere, etwa auf Windows-Systemen relevante Malware-Gattungen spielen für Mac-Rechner gar keine oder bestenfalls eine untergeordnete Rolle und sind im Prozentbereich nicht darstellbar. Die auf Windows-Systemen so verbreitete Ransomware findet auf Mac-Systemen quasi nicht statt.

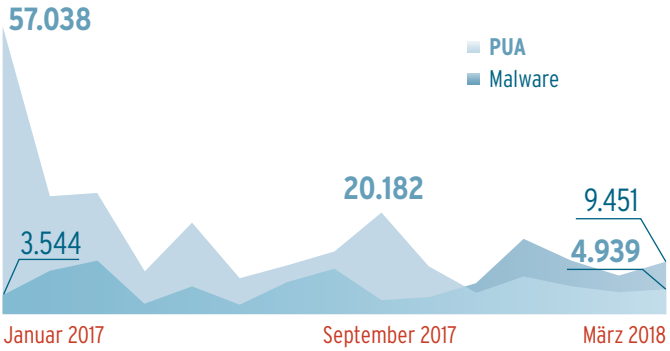
TOP 10 macOS-Malware 2017

1	FLASHBACK	35,75%
2	MACONTROL	22,30%
3	FBJACK	20,93%
4	MACKONTROL	6,46%
5	KERANGER	3,38%
6	HACKBACK	2,71%
7	FACELIKER	1,50%
8	MORCUT	0,96%
9	OLYX	0,83%
10	KRYPTIK	0,57%

Entwicklung Trojaner allg. für macOS 2017 + Q1 2018



Entwicklung der Schädlingsverteilung macOS 2017 + Q1 2018



Trend 2018

Die Dominanz von Trojanern bei macOS-Systemen setzt sich im 1. Quartal 2018 dramatisch fort, die Anzahl verdoppelt sich und erreicht über 86 Prozent der Gesamtsumme der für Apple geschriebenen Malware. Die Verbreitung neuer Skripte wird dadurch von 12,66 auf 0,04 Prozent zurückgedrängt. Die Anzahl neu geschriebener Malware (63,8 Prozent) übersteigt die neu entwickelter PUA-Samples (36,2 Prozent) im Verhältnis von 3:1 und schafft damit eine komplett veränderte Bedrohungssituation für den Apple-Kosmos.

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 ANDROID

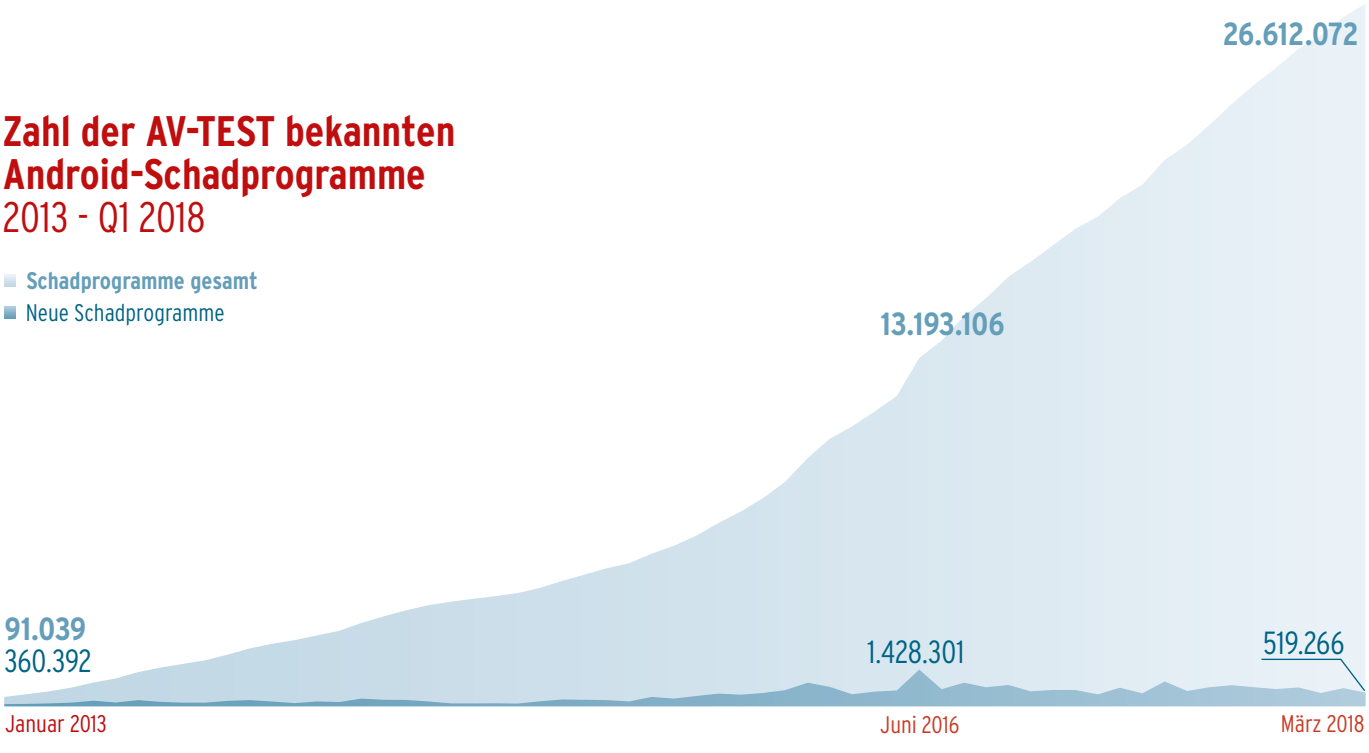
Android-Nutzer geraten zunehmend unter Feuer: Im Vergleich zum Vorjahr hat sich die Zahl von Schadprogrammen für Googles Betriebssystem mehr als verdoppelt. Doch nicht nur die Menge an Schadcode nimmt beständig zu, auch die Komplexität der Angriffe steigt. Zudem trafen die Entwickler mobiler Malware einige grundlegende Entscheidungen mit erheblichen Auswirkungen.

Android – das optimale Angriffsziel

Mit 6,53 Prozent zielte nur ein sehr kleiner Teil der Gesamt-Malware 2017 auf Android-Geräte. Im Verhältnis zu über 67 Prozent Windows-Malware sieht das verschwindend gering aus. Allerdings ist Android nach Windows das Hauptangriffsziel von Cyberkriminellen. Ein Grund dafür ist selbstverständlich die weite Verbreitung von Android-Geräten. Laut StatCounter laufen weltweit zwei von drei Smartphones mit Googles Betriebssystem. Ein weiterer Grund besteht darin, dass Android im Gegensatz zu Apples iOS ein offenes System darstellt. Das bedeutet, dass die Ressourcen für die App-Entwicklung offen für jedermann ersichtlich sind und dass neben Googles PlayStore auch andere Plattformen zur Verteilung von Android-Apps, und somit auch von Malware, verfügbar sind.

Hinzu kommt eine hohe Marktdiversität unterschiedlicher Hersteller mit einer großen Anzahl an unterschiedlichen Geräten. Dabei spielt den Cyberkriminellen in die Hände, dass viele dieser Geräte nicht mit der aktuellsten Android-Version versorgt werden und damit auch nicht auf dem aktuellsten Patch-Level laufen. Nach Google-Angaben war zum Zeitpunkt der Erstellung dieses Reports auf nicht einmal zwei Prozent der Geräte die aktuelle Version 8 aka „Oreo“ installiert. Und zu guter Letzt ist längst nicht auf jedem Android-Gerät eine Schutzsoftware installiert. In der Summe werden Angreifern somit optimale Möglichkeiten geboten, um mit Android-Malware

Zahl der AV-TEST bekannten Android-Schadprogramme
2013 - Q1 2018



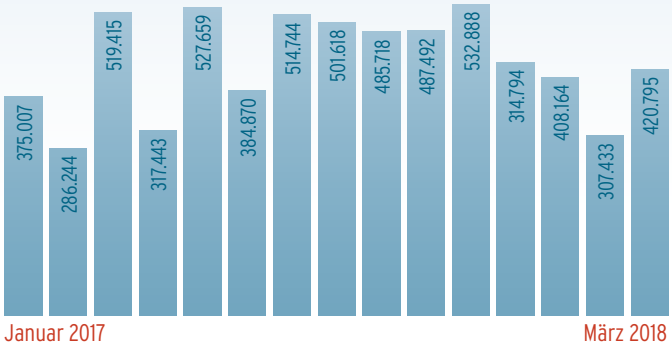
Geld zu verdienen, denn die Geräte bieten nahezu identische Funktionalität und Anbindung an entsprechende Onlinedienste wie Windows-PCs. Folglich steigt auch die Anzahl schadhafter Apps seit Einführung von Android stetig an. Zum Zeitpunkt der Fertigstellung dieses Reports lag die Anzahl der von AV-TEST erfassten Android-Malware-Samples bei exakt 28.335.604 Millionen. Interessant ist dabei, dass die Entwicklung neuer Malware seit Mai 2016, abgesehen von einigen Spitzen, kontinuierlich rückläufig ist.

Android-Ransomware auf dem Rückzug

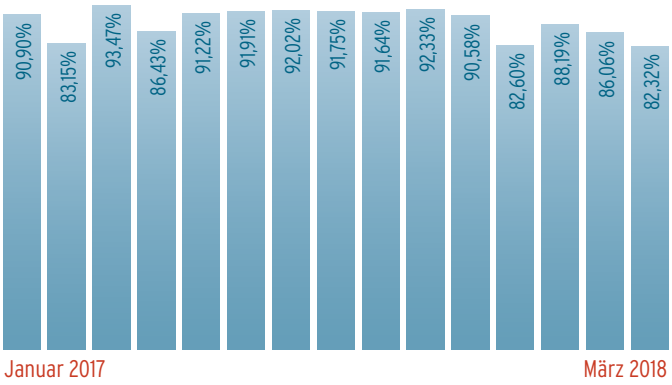
Wer 2017 von Android-Malware spricht, meint damit im Wesentlichen Trojaner. Mit über 90 Prozent aller Android-Schadprogramme sind sie das Allround-Werkzeug der Cyberkriminellen. Sie eignen sich sowohl zum Ausspähen von Daten als auch zum Nachladen weiteren Schadcodes. Das können beispielsweise höher spezialisierte Trojaner wie Ransomware sein. Und tatsächlich erfassten die AV-TEST Systeme ein spürbares Beben von über 2,5 Prozent des Malware-Gesamtanteils im Bereich dieser Schädlingsgattung im zweiten Quartal 2017. Danach flaute die Welle der registrierten Erpresser-Schadcodes wieder auf kaum messbare Werte ab.

Dies könnte bedeuten, dass sich Ransomware auf Mobilgeräten für Kriminelle nicht auszahlt. Ein Grund dafür ist sicherlich, dass Nutzer weitaus weniger und womöglich weniger wichtige Daten auf dem im Verhältnis zum PC doch recht geringen Speicherplatz der meisten Mobilgeräte lagern. Da sich die meisten Ransomware-Attacken bisher noch durch das Zurücksetzen der Geräte in den Werkszustand entschärfen lassen, dürfte die Zahlungsbereitschaft der Opfer deutlich geringer sein, als bei infizierten PCs. AV-TEST wird die Entwicklung von Android-Ransomware weiter verfolgen.

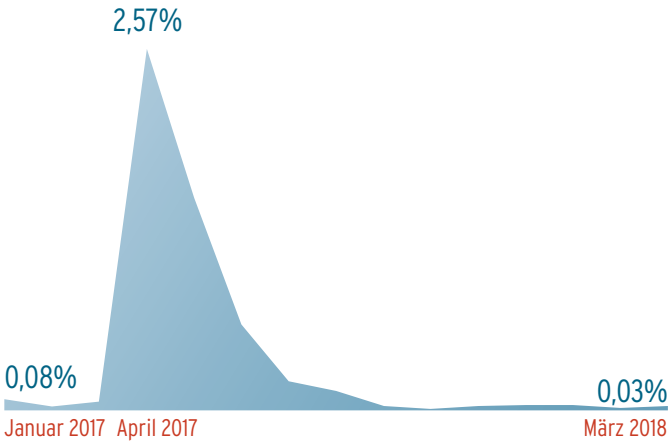
Malware-Entwicklung Android 2017 + Q1 2018



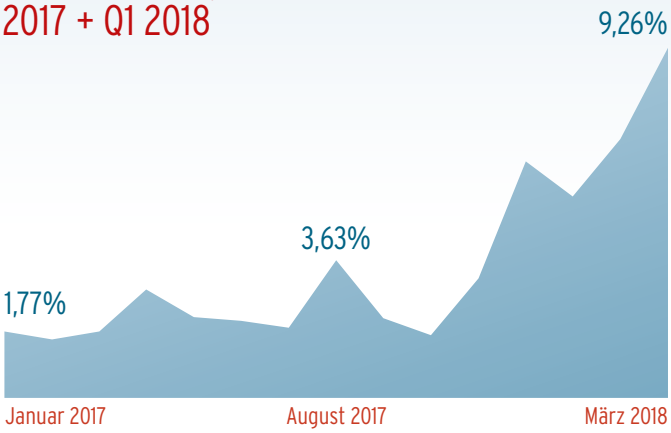
Entwicklung Trojaner allgemein 2017 + Q1 2018



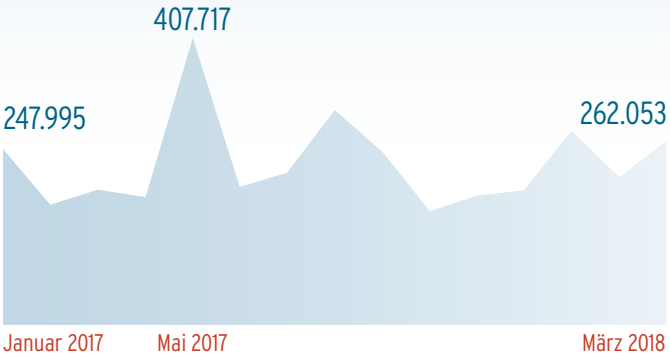
Entwicklung Ransomware 2017 + Q1 2018



Entwicklung Passwort-Trojaner
2017 + Q1 2018



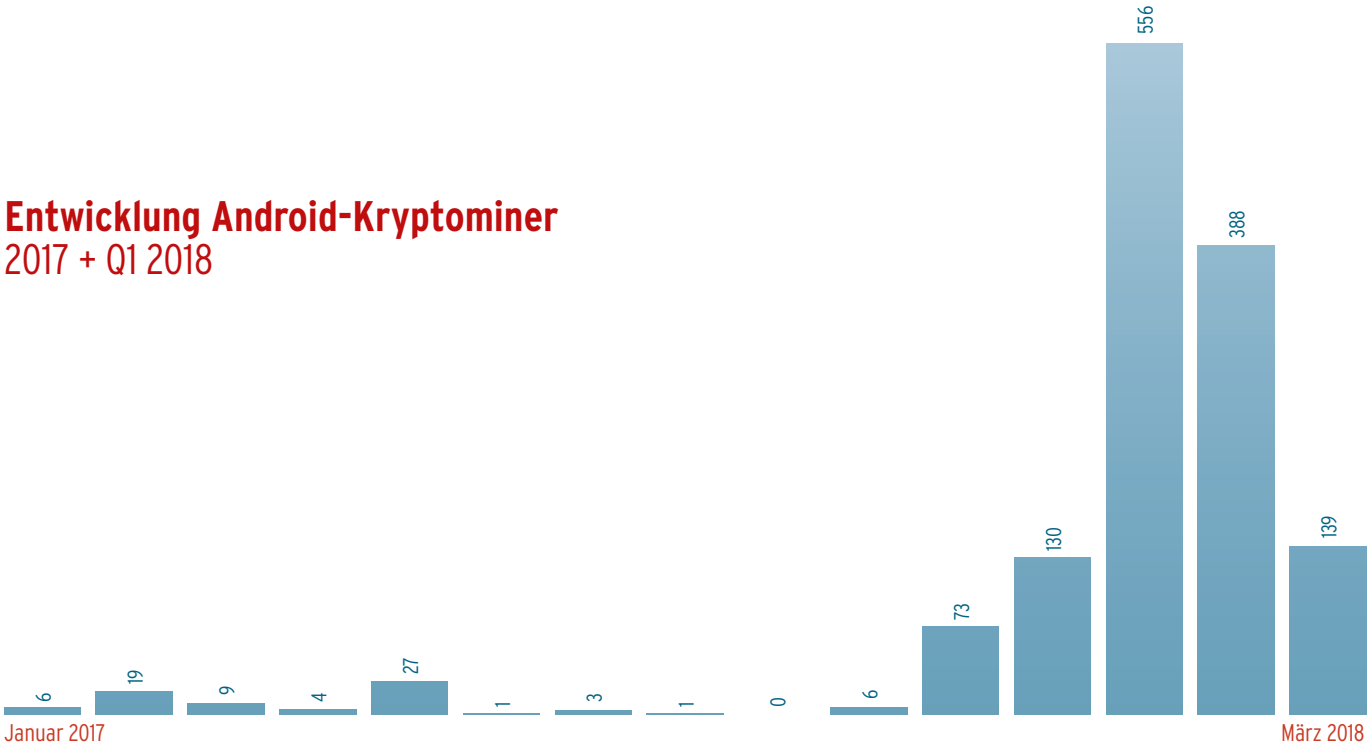
Entwicklung neuer PUA-Samples
2017 + Q1 2018



Zahl der Banking-Trojaner verdreifacht

Stattdessen zielten die Angreifer 2017 immer mehr und ganz direkt auf die Konten der Nutzer von Mobilgeräten. Banking- und Passwort-Trojaner legten im letzten Jahr einen entsprechenden Entwicklungsschub vor. Lag der Anteil dieser Trojaner-Gattung zu Beginn des Jahres noch bei unter 2 Prozent, hatte er sich gegen Jahresende bereits auf über 6 Prozent verdreifacht. Offensichtlich profitieren die Malware-Entwickler von dem steigenden Trend, Kontobewegungen und Einkäufe immer öfter über Smartphone und Tablet sowie entsprechende Apps zu erledigen.

Entwicklung Android-Kryptominer
2017 + Q1 2018



PUA hinter Malware

Ein weiterer signifikanter Vorgang im Laufe des vergangenen Jahres ist die Entwicklung neuer Spionage-Programme der Werbeindustrie. Hauptaufgabe dieser unerwünschten Anwendungen im rechtlichen Graubereich ist die Analyse von Nutzergewohnheiten und Standorten zur Individualisierung von Werbeeinblendungen. Zeitgleich zeichnen sich die meisten von den AV-TEST Systemen erfassten und ausgewerteten PUA-Samples durch die penetrante Einblendung von Werbung, etwa auf Home- und Lock-Screens, aber auch während der App-Nutzung aus. Hier gibt es für das Jahr 2017 Positives zu vermelden, denn die Anzahl der Neuentwicklungen von Werbe-Spionen geht messbar zurück. Brachte die Werbe-Mafia 2016 noch 4.222.713 neu entwickelte PUA-Samples auf den Markt, mussten sich Android-Nutzer 2017 „nur noch" von 2.702.098 neuen Spähprogrammen beschnüffeln lassen.

TOP 10 Android-Malware 2017

1	AGENT	35,07%
2	SHEDUN	14,76%
3	TRIADA	9,13%
4	LOCKSCREEN	7,82%
5	SMSPAY	4,68%
6	CONGUR	2,87%
7	BOOGR	2,36%
8	SMSSPY	1,45%
9	SMFORW	1,45%
10	FAKEINST	1,42%

Trend 2018

Eine klare Entwicklung des ersten Quartals ist die Konzentration der Android-Malware-Industrie auf einen neuen, lukrativen Markt. Denn die Malware-Erfassung der AV-TEST Systeme zeigt einen überdeutlichen Ausschlag bei der Entwicklung von Kryptominern auf Android-Basis. Während AV-TEST bereits 2014 die ersten Schadprogramme dieser Art orten konnte, stiegen die Sample-Zahlen Mitte 2016 und 2017 erstmals geringfügig an, was auf eine Experimentierphase mit der neuen Malware-Gattung hinweist. Bei diesen beiden Mess-Peaks wurde jedoch nie die Sample-Zahl von 50 Samples überschritten. Das sieht zu Beginn dieses Jahres völlig anders aus: Mit 556 Samples im Januar sowie 388 neuen Kryptominern im Februar nimmt die Entwicklung des Schürfens von Krypto-Währungen auf Mobilgeräten deutlich Fahrt auf. Offensichtlich stehen Cyberkriminelle in den Startlöchern, um die immer potenteren Prozessoren von Android-Geräten für illegales Coinmining anzuzapfen.

Während auch 2018 die Entwicklungsrate für Android-Malware, darunter ebenfalls die der Trojaner und der Ransomware, weiter sinkt, durchbricht die Rate der Banking- und Passwort-Trojaner gegen diesen Trend die Schallgrenze von 9 Prozent der Malware-Gesamterfassung. Android-Nutzer sind mit dem Einsatz von Security-Apps also weiterhin gut beraten.

AV-TEST
av-test.org

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 INTERNET-GEFAHREN

Verseuchte E-Mails, infizierte Websites, Attacken per Malware-Download: Die Untiefen der Online-Kommunikation bieten Cyberkriminellen zahlreiche Möglichkeiten, Schadprogramme auf die Rechner ihrer Opfer zu schleusen. Die Gefahrenanalyse von AV-TEST zeigt, welche Wege sie dafür bevorzugt nutzen.

Geprüfte Webseiten in 2017

Webseiten gesamt
ca. 1.850 Mio.

95 Millionen Websites überprüft

Für die Suchmaschinen-Analyse erfassten die AV-TEST Systeme 2017 insgesamt 95.547.507 Websites. Dabei erfolgte ebenfalls eine Analyse sowie ein Ranking infizierter Top-Level-Domains und der zur Malware-Verbreitung genutzten Datei-Formate. Es zeigte sich, dass Angreifer bei der Verbreitung von Malware nach wie vor auf ungeschützte http-Seiten bauen: 84,26 Prozent aller infizierten Websites arbeiteten mit dem nicht geschützten Übertragungsprotokoll. Allerdings nimmt die Zahl ausgeklügelter Angriffe, die auch über https-Seiten erfolgen, im Vergleich zum Vorjahr weiter zu. Während 2016 gerade 8 Prozent der Angriffe von https-Seiten ausgingen, waren es im Folgejahr bereits 15,74 Prozent. Ein Grund dafür kann in der ohnehin massiv steigenden Anzahl SSL-verschlüsselter Seiten gesehen werden. Beflügelt wird diese an sich wünschenswerte Entwicklung durch den massiv steigenden Einsatz kostenloser, automatisiert vergebener SSL-Zertifikate durch den Dienst „Let's Encrypt". Allerdings nutzen diesen Service nicht nur unbescholtene Privatleute und KMU, sondern sein Nutzen ist auch kriminellen Geschäftemachern nicht entgangen.

TOP 10 Malware-verseuchte Domains 2017

1	COM	52,92%
2	NET	10,32%
3	RU	4,48%
4	GE	3,58%
5	ORG	2,76%
6	SU	2,46%
7	TIPS	2,35%
8	BR	1,76%
9	CO	1,27%
10	ME	1,12%

Ransomware reist per Mail

2017 bedienten sich Cyberkriminelle eines großen Arsenals, um Malware entweder über Massenangriffe oder sehr gezielt auf die Geräte ihrer Opfer zu schmuggeln. Die großen Ransomware-Attacken des vergangenen Jahres nutzten die klassischen Übertragungswege für Schadprogramme ihrer Gattung, und so fanden beispielsweise „WannaCry" und „Locky" ihre Verbreitung durch große E-Mail- beziehungsweise Phishing-Kampagnen. Dieser Übertragungsweg blieb auch 2017 für Ransomware, sowie den Großteil der per Internet übertragenen Schadprogramme – der Hauptteil davon Trojaner – bestimmend. Schädlinge wie WannaCry und Petya verbreiteten sich auf infizierten Systemen zudem durch Lücken im Windows SMB-Netzwerkprotokoll weiter.

Mit 16 Prozent aller Spam-Mails arbeitete sich Vietnam in 2017 gegenüber dem Vorjahr auf den ersten Platz der Spam-Versender. Die USA behaupteten Platz zwei, während Indien seine bisherige Vormachtstellung an Vietnam verlor. Nach China auf Platz vier folgte bereits Deutschland mit einem wenig rühmlichen fünften Platz unter den von AV-TEST erfassten Spam-Nationen, mit 3,9 Prozent des globalen Anteils an unerwünschter und oft verseuchter E-Mail.

Gezielt infiziert per Update

Einen anderen Weg der Verbreitung suchten dagegen die Entwickler von Petya, indem sie gezielt Rechner mit Standort Ukraine durch die Infektion der für das Land typischen Buchhaltungs-Software „MeDoc" mithilfe verseuchter Programm-Updates infizierten. Eine ähnliche Attacke erfolgte von August bis September durch die Infektion der millionenfach genutzten Freeware „CCleaner" des damaligen Anbieters Piriform. Während des Zeitraums der Attacke könnte es über 2 Millionen Installationen der infizierten Software gegeben haben. Diese war aufgrund eines gültigen Zertifikats in den infizierten 32-Bit-Versionen CCleaner v5.33.6162 und CCleaner Cloud v1.07.3191 als Malware nur schwer zu erkennen. Wie das Talos Team von Cisco, das die Malware entdeckte, herausfand, nahmen im September 1,65 Millionen infizierte Rechner Kontakt mit dem Command-and-Control-Server der Malware auf.

TOP 10 Malware-verseuchte Dateitypen 2017

1	HTML	22,97%
2	PHP	8,90%
3	EXE	5,69%
4	ZIP	4,50%
5	RAR	2,29%
6	HTM	1,13%
7	ASP	0,31%
8	ASPX	0,25%
9	IZLE	0,23%
10	COM	0,10%

Exploit-Kits weiter stark aktiv

Exploit-Kits erfreuten sich auch 2017 großer Beliebtheit bei der Malware, denn sie sind im Internet leicht zu bekommen, weit verbreitet und ihr Einsatz ist extrem günstig. Den Erfolg von Exploit-Kits garantiert das professionelle, arbeitsteilige Vorgehen der gut organisierten kriminellen Banden, die in diesem Geschäftsbereich arbeiten. Während die einen die Malware-Verbreitungswerkzeuge in Untergrund-Foren vermarkten, halten andere Kriminelle die Exploit-Kits für Kunden immer auf dem neusten Stand und garantieren so „Crime-as-a-Service" mit einer Erfolgsgarantie für eine Mindestanzahl infizierter PCs.

Dementsprechend sind die Funktionen der Malware-Bau- und Verbreitungskästen ständig up-to-date: Neue Angriffsvektoren und Ziele sowie das ständige Anpassen auf die neusten Exploits und Detektionsmethoden von Virenscannern versprechen Kriminellen für ihre Malware-Kampagnen hohe Reichweiten. 2017 dominierten die Exploit-Kits „RIG", „Magnitude", „Terror" und „Neutrino" den Markt und verbreiteten unter anderem Ransomware, Coinminer und Banking-Trojaner. Sehr oft nutzen die Angreifer dabei bekannte Lücken der Software Adobe Flash. Für die Malware-Verbreitung setzten Cyberkrimelle auch im letzten Jahr im großen Umfang selbsterstellte Websites mit Inhalten ein, die sich in Suchmaschinen großer Nachfrage erfreuten. Die Erfassungssysteme des AV-TEST Instituts überwachten darum über das gesamte Jahr die fünf größten Suchmaschinen.

TOP 10 Spamversender 2017

1	VIETNAM	16,0%
2	VEREINIGTE STAATEN VON AMERIKA	11,5%
3	INDIEN	9,8%
4	CHINA	6,6%
5	DEUTSCHLAND	3,9%
6	IRAN	3,9%
7	MEXIKO	2,8%
8	INDONESIEN	2,8%
9	BRASILIEN	2,7%
10	RUMÄNIEN	2,6%

Trend 2017

Das erste Quartal 2018 zeigt eine deutliche Steigerung von Angriffen, die über https-Seiten erfolgen: Mit über 27 Prozent nehmen Angriffe über verschlüsselte Webseiten stark zu. Die Top 10 der mit Malware verseuchten Dateitypen bleibt dagegen nahezu identisch.

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.

Sicherheitsstatus IoT

IP-Kamera, smarte Beleuchtung und Smart-TVs: Es gibt kaum noch Haushalte, in denen nicht mindestens ein mit dem Internet vernetztes Gerät steht. Zudem koppeln immer mehr Hersteller bisher unvernetzte mit eigens dafür entwickelten Onlinediensten. Dabei spielt es oft keine Rolle, ob solche Online-Features sinnvoll sind oder nicht. Und nur selten spielen bei deren Entwicklung Sicherheitserwägungen eine Rolle. Damit bringen Hersteller Millionen ihrer Kunden unnötig in Gefahr.

Kampf um den Markt der Zukunft

Bereits die Zahlen vorsichtiger Schätzungen zur Entwicklung des Internet of Things zaubern Marketingchefs das Leuchten in die Augen: Laut Gartner-Vorhersagen werden Unternehmen innerhalb der nächsten zwei Jahre ca. 1.477 Milliarden Dollar in IoT-Geräte und Dienstleistungen investieren. Die Chancen, im gleichen Zeitraum im Verbrauchersegment Geld zu verdienen, liegen sogar noch darüber, denn den Markt für Endanwenderprodukte schätzt das Marktforschungsunternehmen noch profitabler ein: 1.534 Milliarden Dollar sollen Privathaushalte bis 2020 für IoT-Geräte ausgegeben. Tritt diese Vorhersage ein, werden rund um den Globus über 830 Millionen Wearables und 20,8 Milliarden vernetzte Geräte verkauft und im Einsatz sein.

Solche Zahlen begeistern nicht nur Unternehmen, sondern auch Cyber-kriminelle. Und so entsteht eine brisante Mischung: Auf der einen Seite stehen Produkthersteller ohne Expertise in IT-Sicherheit, die möglichst schnell immer mehr Produkte auf den boomenden Markt werfen wollen. Auf der anderen Seite lauert die Cyber-Mafia mit einem großen Arsenal bereits funktionierender und erprobter Schadprogramme auf die Masse an Geräten und Online-Services, die ihnen jede Menge Schwachstellen zur Verbreitung von Schadcodes bieten. Insofern beflügelt ein Markt den andern. Das Risiko und die Kosten tragen die Nutzer.

IoT-Malware legt stark zu

Unter der erfassten Malware befinden sich Schadcodes zur Ausnutzung der Rechenleistung internettauglicher Geräte für DDoS-Attacken, nach Vorbild von Mirai, wie etwa der Schädling „Gafgyt“ alias „Bashlite“, der mit 21,52 Prozent Platz 1 der IoT-Malware Top 10 belegt. Dieser Linux-Trojaner, dessen erste Erkennung durch die AV-TEST Systeme auf Januar 2012 datiert, nutzt unter anderem die Shellshock-Lücken der Unix-Shell Bash. Damit ist der Schädling in der Lage, jedes ungepatchte, Unix-basierte Betriebssystem zu infizieren. Verläuft die Infektion erfolgreich, verbreitet sich Gafgyt wie ein Internetwurm im angeschlossenen Netzwerk. Der Source-Code der Malware wurde bereits 2015 veröffentlicht. Seither ist auch eine deutliche Zunahme an Gafgyt-Aktivität messbar. Der Schädling zwingt vor allen IP-Kameras und digitale Videorecorder in sein Botnetz, welches dann unter anderem für DDoS-Attacken eingesetzt wird; damit ist er Mirai sehr ähnlich.

Mirai weiterhin aktiv

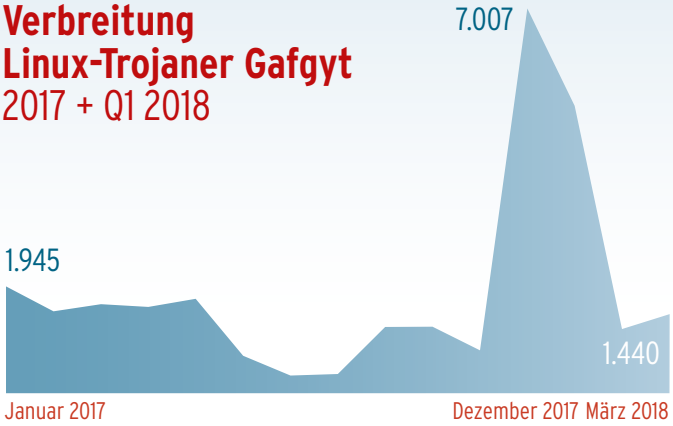
Die 2016 über die IoT-Malware Mirai geführten Attacken verknüpften zeitweise über 500.000 infizierte IP-Kameras und digitale Videorekorder zu einem der bisher größten Botnetze der Welt. Über Denial-of-Service-Attacken wurden dabei weite Teile des Internets lahmgelegt. Drei amerikanische Studenten hatten die Malware ursprünglich entwickelt, um die Server konkurrierender Minecraft-Spieler aus dem Netz zu schießen. Später wurde das per Mirai erzeugte Botnetz für DDoS-Erpressungen gegen große Provider und Dienstanbieter genutzt. Mit dieser ersten großen Attacke erzeugten die drei Studenten ein vorübergehendes öffentliches Bewusstsein für die Gefahr durch ungeschützte IoT-Geräte. Durch das Veröffentlichen des Mirai-Quellcodes im Internet schufen sie allerdings eine zusätzliche Gefahr.

Nach wie vor kommt der erfolgreiche Schadcode in modifizierten Fassungen zum Einsatz, wie die Zahlen der AV-TEST-eigenen Honeypot-Systeme beweisen. Für Kriminelle bleibt der Schadcode weiterhin attraktiv, da für viele IP-Kameras sowie andere gefährdete IoT-Geräte nach wie vor weder Security- noch Firmware-Updates zur Verfügung stehen, teilweise nicht einmal eine entsprechende Update-Funktion.

Eindringliche Warnung

Ähnlich Mirai und Gafgyt verbreitet sich seit dem ersten Quartal 2017 der IoT-Schädling „Hajime". Auf befallenen Geräten mit Display warnt die IoT-Malware sogar mit einer eigens programmierten Meldung: „Nur ein White Hat (Hacker), der einige Systeme sichert. Bleiben Sie scharf!" Die Verbreitung von Hajime erfolgt seit April letzten Jahres in zunehmenden Wellen. AV-TEST wird auch die Entwicklung dieses Eindringlings in IoT-Systeme weiterhin überwachen.

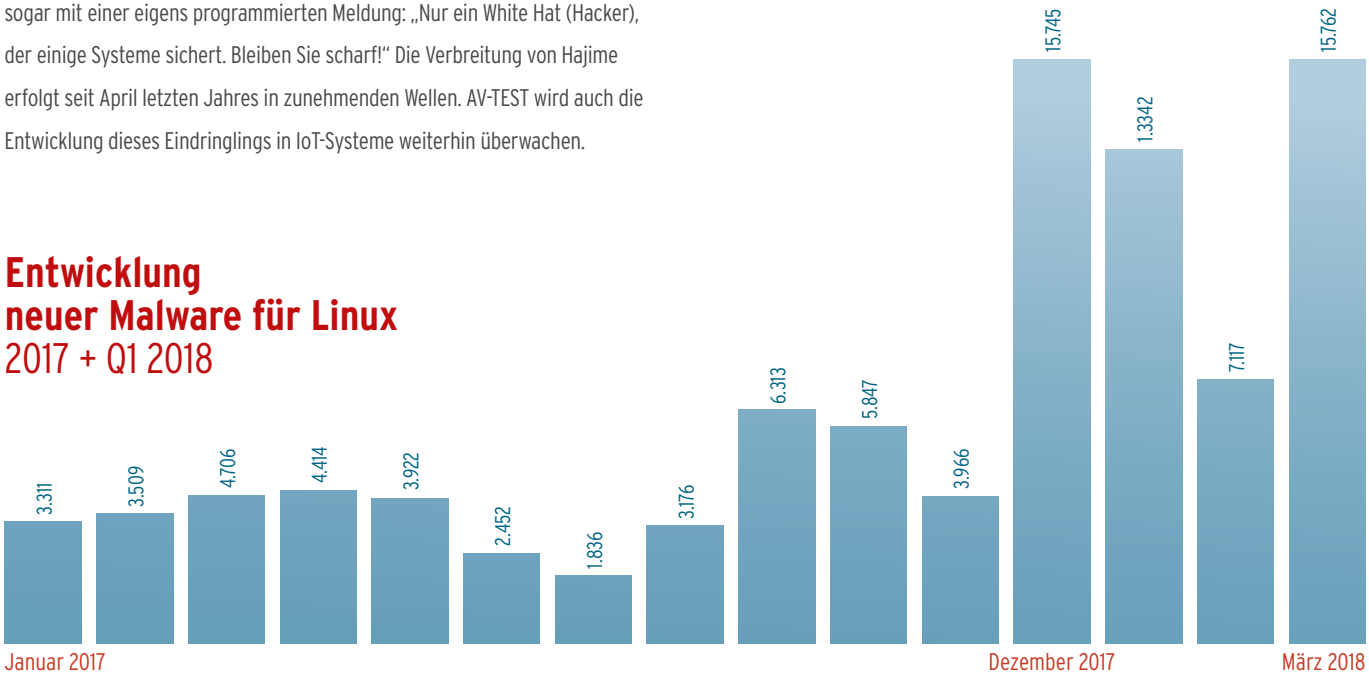
Verbreitung Linux-Trojaner Gafgyt
2017 + Q1 2018



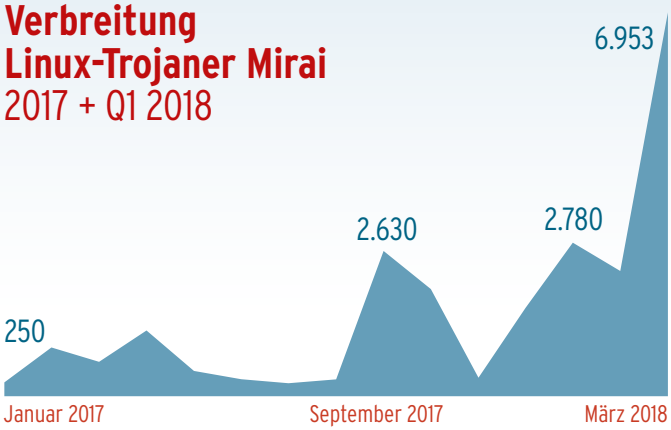
IoT: Das Coinmining-Eldorado

Neben dem Aufbau großer Botnetze für DDoS-Erpressung rückt mit Millionen ungeschützter IoT-Geräte ein weiterer krimineller Businessplan in das Visier der Cyberkriminellen. Denn was liegt näher, als die weitestgehend ungeschützte und immer weiter steigende Rechenleistung von IoT-Produkten zum Errechnen von Krypto-Währungen einzusetzen. Für IoT- und Smart Home-Infrastrukturen können Angreifer Schadprogramme auf Linux-Basis zum Einsatz bringen, um die Leistung von Geräte-CPUs für sich arbeiten zu lassen. Während Coinminer anfangs noch die volle CPU-Leistung für das Schürfen von Bitcoin und Co. nutzten und Geräte bis zum Ausfall an ihre Leistungs-

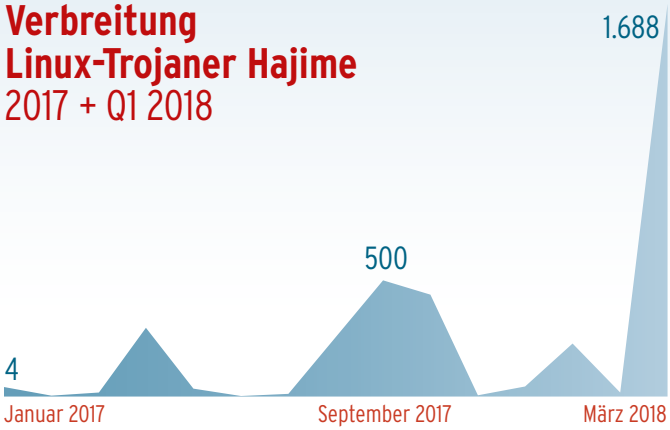
Entwicklung neuer Malware für Linux
2017 + Q1 2018



Verbreitung Linux-Trojaner Mirai 2017 + Q1 2018



Verbreitung Linux-Trojaner Hajime 2017 + Q1 2018



grenzen führten, überwacht und reguliert die neue Generation von Coinminern die genutzte CPU-Leistung und verhindert so den Ausfall des infizierten Wirt-Systems. Zudem führt diese Strategie dazu, dass mit Coinminern infizierte Geräte weniger leicht zu erkennen sind und damit für einen längeren Zeitraum zur Verfügung stehen. Der signifikant messbare Einsatz Linux-basierter Coinminer setzte im zweiten Quartal 2017 ein. Seit September steigt die Sample-Zahl dieser Malware-Gattung nicht nur für IoT-Geräte unaufhörlich und wuchs bis Dezember auf das Achtfache an.

TOP 10 IoT-Malware 2017

1	GAFGYT	21,52
2	MIRAI	17,12
3	VIT	13,57
4	LOTOOR	5,82
5	AGENT	5,42
6	TSUNAMI	3,34
7	SHELLBOT	2,21
8	SETAG	2,16
9	SH	2,08
10	HAJIME	1,90

Trend 2018

Auch im ersten Quartal dieses Jahres verzeichnen die AV-TEST Systeme signifikante Zuwächse von Malware für IoT-Systeme. Über 300 neue Varianten der lukrativen Schädlingsgattung entwickelte die Malware-Industrie seither pro Monat. Derzeit ist davon auszugehen, dass diese Entwicklung in absehbarer Zeit auf hohem Niveau stagnieren wird, denn Cyberkriminelle können auf eine wachsende Zahl meist ungeschützter IoT-Geräte zugreifen. Dementsprechend besteht für sie kein Entwicklungsdruck. Allerdings wird die qualitative Entwicklung der Coinminer weitergehen und es werden zunehmend Samples mit ausgefeiltem CPU-Management zu sehen sein.

Insgesamt wird die Entwicklung von Malware für Linux-basierte Systeme 2018 enormen Zuwachs erfahren. Das lassen die Messwerte quasi aller Malware-Gattungen, die für Smart Home- und andere IoT-Systeme zum Einsatz gebracht werden können, bereits erahnen.

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 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 35 Servern mit einer Speicherkapazität von mehr als 2.000 Terabyte. Zum Veröffentlichungsdatum dieses Jahresreports beinhaltete die AV-TEST Datenbank 771.077.699 Schadprogramme für Windows und 28.335.605 Schadprogramme für Android!

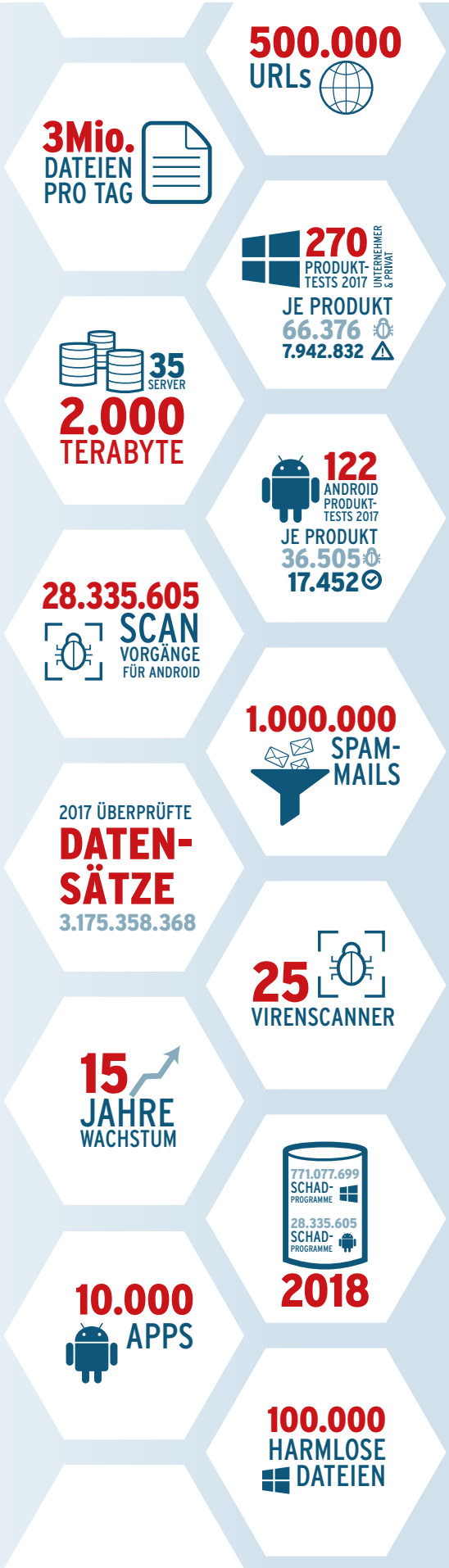
AV-TEST Qualitätssiegel für Antiviren-Produkte

- Das Siegel AV-TEST CERTIFIED erhalten Produkte für den Heimanwenderbereich nach den hohen Zertifizierungsstandards des AV-TEST Instituts.
- Das Prüfzertifikat AV-TEST APPROVED ist Produkten aus dem Unternehmensbereich vorbehalten.

Überprüft werden alle marktrelevanten Produkte für die Betriebssysteme Windows, MacOS und Android.

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. 2017 wurden so über 270 Produkttests allein für Privatanwender- und Unternehmensprodukte durchgeführt. Dabei wurden pro Produkt 66.376 Malware-Attacken gefahren sowie 7.942.832 einzelne Datensätze für Fehlalarmtests eingesetzt und ausgewertet. Im gesamten Jahr 2017 waren das 3.175.358.368 von den Testexperten zu überprüfende Datensätze. In den monatlichen Android-Tests überprüften die Tester über das Jahr insgesamt 122 Produkte. Dabei musste sich jede überprüfte Sicherheits-App gegen 36.505 spezielle Android-Schädlinge zur Wehr setzen. Zur Gegenprobe erfassten die Experten zudem über 17.452 Scans sicherer Apps pro Produkt, um die Anfälligkeit für Fehlalarme zu überprüfen. Im Labor wurden in Tests von Sicherheitsprodukten für Android also allein 6.582.754 Scan-Vorgänge analysiert und reproduzierbar ausgewertet. 2.359.358 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.

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