ZAHLEN UND FAKTEN

SECURITY REPORT 2016/17

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Der AV-TEST Sicherheitsreport

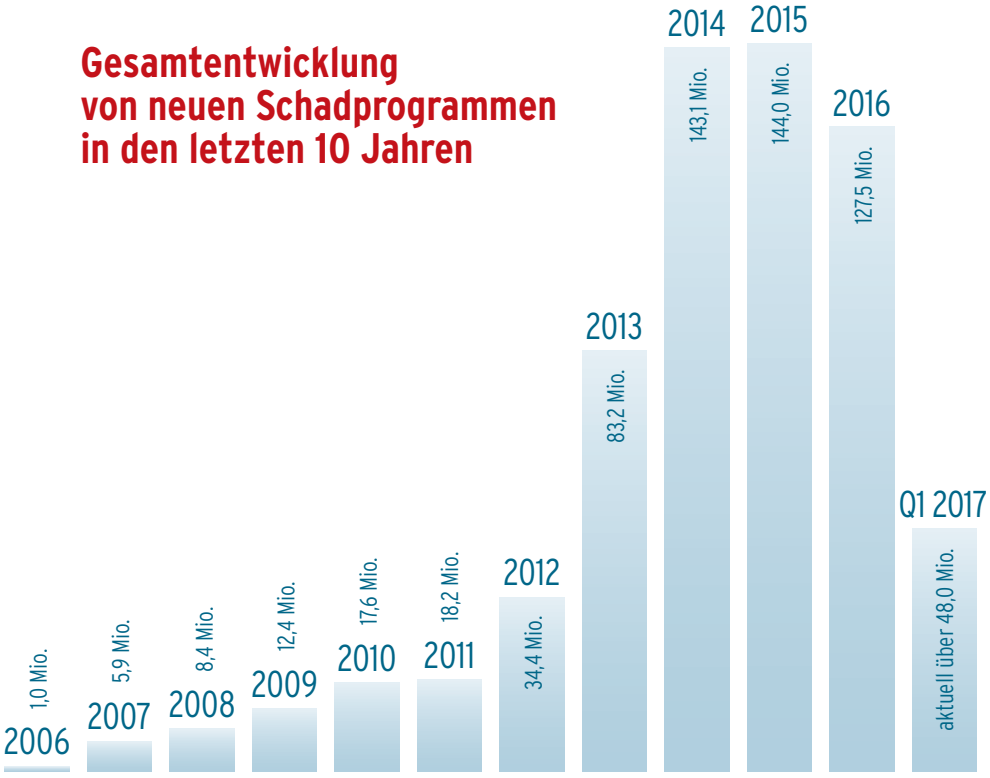
Die beste Nachricht gleich zu Beginn: Im Vergleich zum Vorjahr verzeichnen die Erkennungssysteme von AV-TEST für das Jahr 2016 einen Rückgang bei der Entwicklung von Schadprogrammen. Das ist insgesamt zwar ein erfreulicher Trend, allerdings längst kein Grund zum Feiern, wie die Zahlen des diesjährigen Sicherheitsreports des AV-TEST Instituts belegen.

Rückläufige Malware-Zahlen

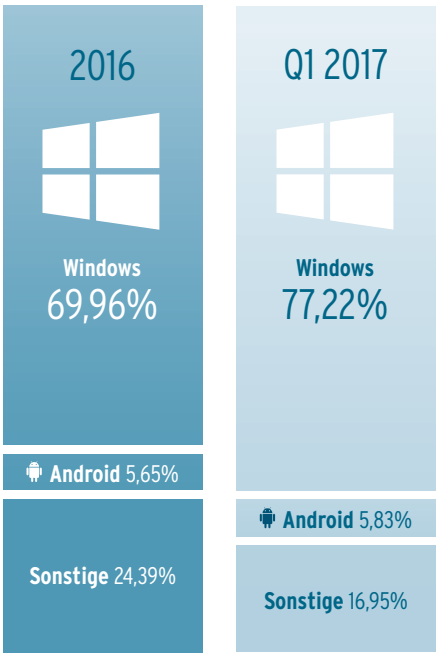
Positiv zu vermerken bleibt, dass die im Jahr 2016 rückläufige Malware-Entwicklung zumindest quantitativ für Entlastung sorgte. So mussten Erkennungssysteme im Vergleich zu 2015 immerhin 14 Prozent weniger Malware-Samples aufspüren und abwehren. In Summe waren das genau 11.725.292 neu entwickelte Schadprogramme weniger als im Vorjahr. Allerdings sollte dabei nicht vergessen werden, dass die Menge neu entwickelter Malware 2016 immer noch die zweithöchste seit Beginn der Messungen durch die Systeme von AV-TEST ist. Zudem lag 2015 eine sprunghafte Entwicklung von Schadprogrammen und im Vergleich zu 2014 quasi eine Verdopplung der Sample-Zahlen vor. Die Gesamtzahl an Schadprogrammen für alle Betriebssysteme übersteigt aktuell 640 Millionen.

Ohne den positiven Trend für 2016 kleinreden zu wollen, bleibt weiterhin festzustellen, dass es solche kurzfristigen rückläufigen Entwicklungen seit Beginn der Messungen 1984 bereits einige Male gab, insgesamt sechs Mal, ohne den klaren, langfristigen Trend – hin zu mehr Malware – ernsthaft zu beeinflussen. 2016 verzeichneten die AV-TEST Analysesysteme trotz rückläufiger Zahlen im Schnitt immer noch 350.000 neue Schadprogramme pro Tag, also etwa vier neue Schädlinge pro Sekunde. Eine Einschätzung der Bedrohungslage lässt sich durch die Analyse allein quantitativer Faktoren nicht sinnvoll vornehmen. Doch dazu mehr im Rahmen dieses Reports.

Gesamtentwicklung von neuen Schadprogrammen in den letzten 10 Jahren



Malware-Erkennung nach Betriebssystem



Klasse statt Masse?

Doch nicht nur hinsichtlich rückläufiger Zahlen im Gesamtbereich der Malware ist das vergangene Jahr bemerkenswert. Auch innerhalb der von AV-TEST erfassten Schädlingsklassen sowie bei den Entwicklungen der Angriffsziele stellt das Jahr 2016 einen deutlich messbaren Umbruch dar, und es zeichnen sich deutliche Trends ab:

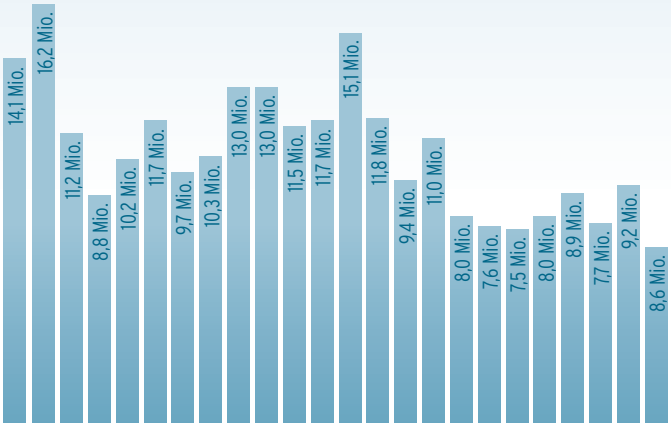
Die Menge des ausschließlich für Windows-Systeme programmierten Schadcodes nimmt ab. Angreifer entwickeln zunehmend Schadprogramme für andere Betriebssysteme. Im Vergleich zum Vorjahr steigt deren Anzahl um knapp 10 Prozent, während die Anzahl reiner Windows-Schädlinge um knapp 13 Prozent sinkt.

Windows bleibt das meistangegriffene Betriebssystem. Im Jahr 2016 zielten nach wie vor sieben von zehn neu programmierten Schadprogrammen auf die Microsoft-Plattform.

Apple-Geräte geraten immer mehr unter Feuer: Gegenüber dem Vorjahr hat sich die Menge der Malware für macOS verdreifacht.

Auch Nutzer von Android-Geräten sehen sich einer schnell wachsenden Menge von Malware gegenüber: Im Vergleich zum Vorjahr hat sich die Zahl von Schadprogrammen, die auf die Vielzahl an Geräten mit Googles Betriebssystem zielen, mehr als verdoppelt.

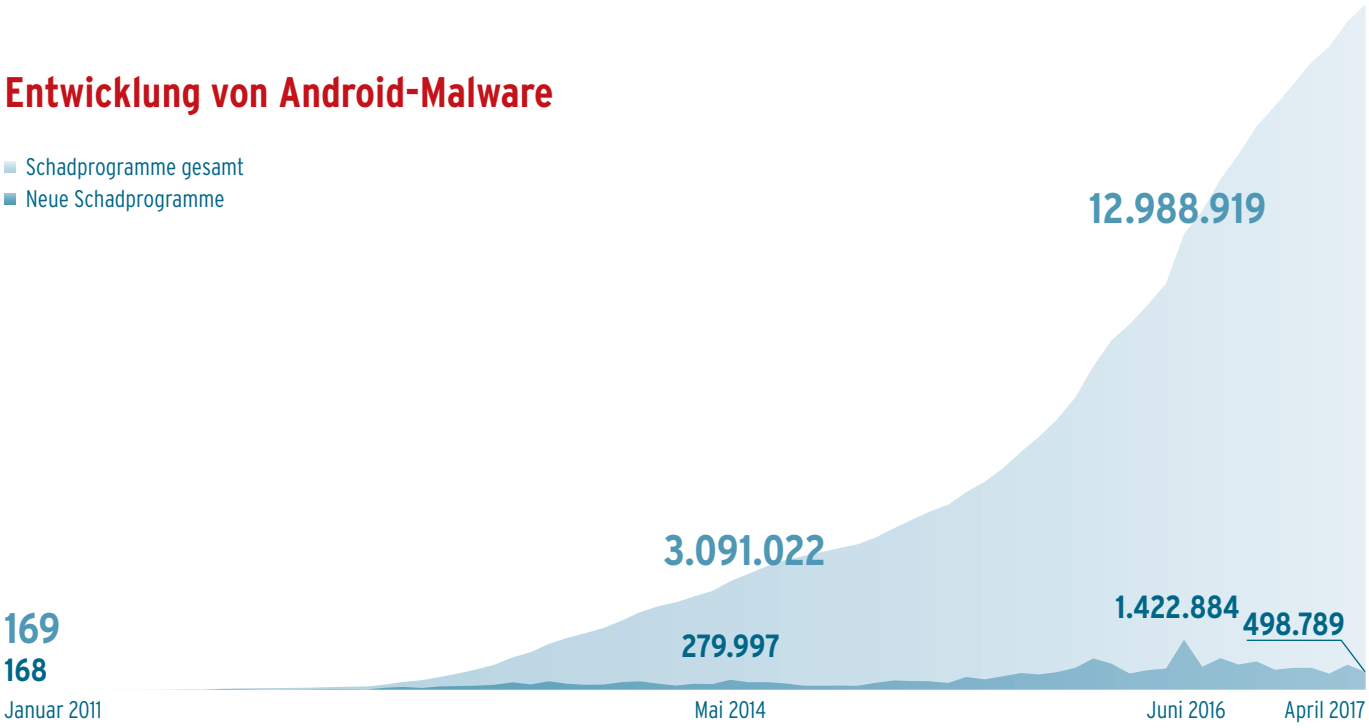
Auftreten neuer Malware-Samples insgesamt



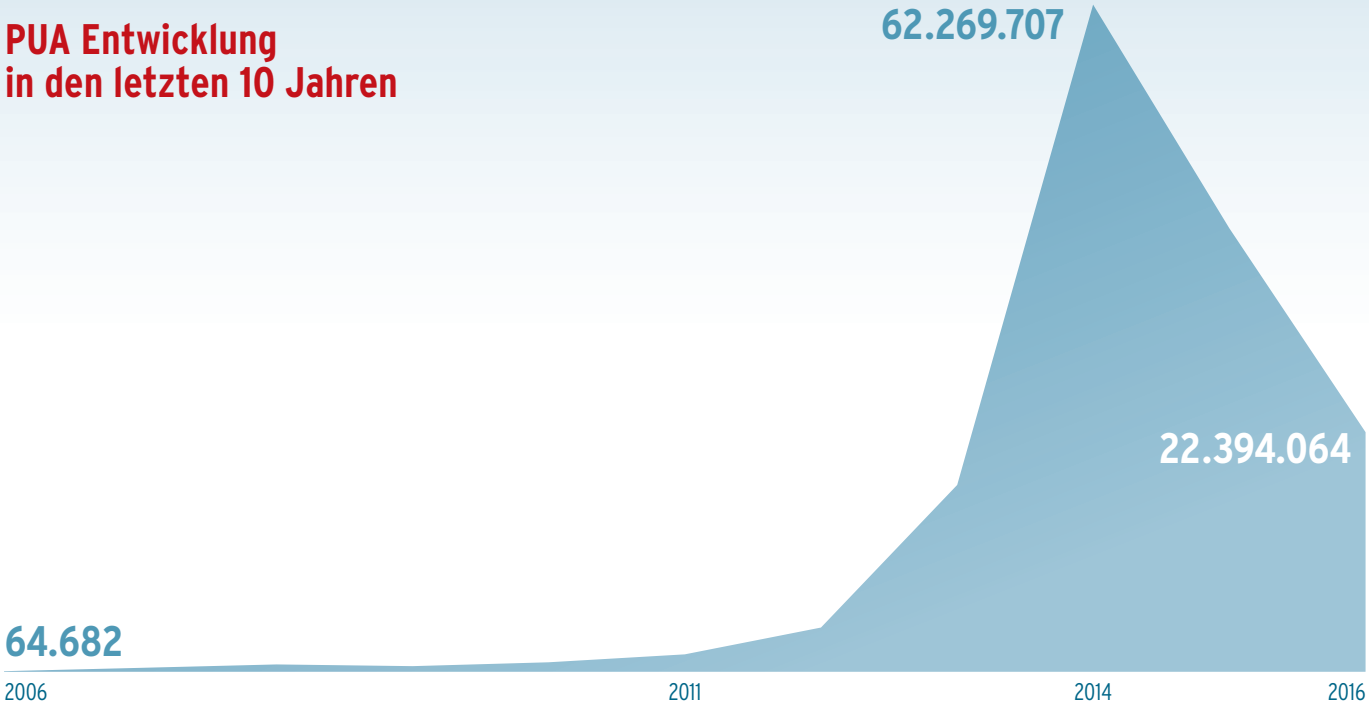
Auch für Linux-Systeme standen die Zeichen 2016 auf Sturm: Die Anzahl angreifender Schadprogramme verdreifachte sich im Vergleich zum Vorjahr.

Aufgrund der stark gestiegenen Zahlen Potentiell Unerwünschter Anwendungen (PUA), mit denen die Werbeindustrie vor allem in den Jahren 2014 und 2015 das Surfverhalten von Nutzern ausspionierte, widmeten die AV-TEST Forscher dieser Schädling-Gattung im letzten Sicherheitsreport ein eigenes Kapitel. Allerdings halbierte sich die Zahl neuer PUA-Samples im Jahr 2016 im Vergleich zum Vorjahr auf nur noch 22.394.064 neu erfasste Samples.

Entwicklung von Android-Malware



PUA Entwicklung in den letzten 10 Jahren



Trend 2017

Dieser Sicherheitsreport umfasst nicht nur den Datenstand für das Jahr 2016, sondern berücksichtigt zudem die Messwerte der - AV-TEST Analysesysteme für das erste Quartal 2017. So lassen sich schon jetzt erste mit Daten untermauerte Trends für das laufende Jahr erkennen.

Die Q1-2017-Zahlen bestätigen einen Trend, der Apple-Nutzern nicht gefallen wird. Die bereits 2016 erkennbar zunehmenden Angriffszahlen steigen weiter – und zwar deutlich: So verdoppelte sich die Gesamtzahl von Schadprogrammen für macOS innerhalb der ersten vier Monate dieses Jahres! Ebenfalls eine deutliche Zunahme verzeichnen Angriffe auf Linux-Systeme, die oft ebenso ungeschützt ins Internet angebunden werden wie Rechner unter macOS. Für Angreifer offenbar ein lohnendes Ziel.

Umkehren wird sich nach erster Prognose dagegen der hoffnungsvolle Trend für Windows-Nutzer. Denn die sinkende Angriffsrate von 2016 wird durch die neuen Messwerte der AV-TEST Systeme nicht bestätigt. Im ersten Quartal 2017 steigt die Zahl der Schadprogramme wieder an, aktuell um etwas mehr als sieben Prozent im Verhältnis zum Jahreswert des Vorjahres.

Der Trend zur Abnahme der Anzahl an PUA-Samples bestätigt sich im ersten Quartal dieses Jahres. Im April erfassten die AV-TEST Systeme gerade noch 724633 Samples. Einen derart niedrigen Wert gab es zuletzt im März 2013. Trotz des massiven Rückgangs ist es für Entwarnung noch zu früh und die Experten des AV-TEST Institutes werden die PUA-Entwicklung weiter beobachten.

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

Sicherheitsstatus WINDOWS

Auch 2016 blieben die Betriebssysteme von Microsoft Hauptangriffsziel krimineller Online-Attacken. Allerdings sank die Zahl der Angriffe im Vergleich zum Vorjahr um 13 Prozent. Warum? Die Analyse der Messdaten von AV-TEST gibt die Antwort.

Über 600 Millionen Gegner für Windows

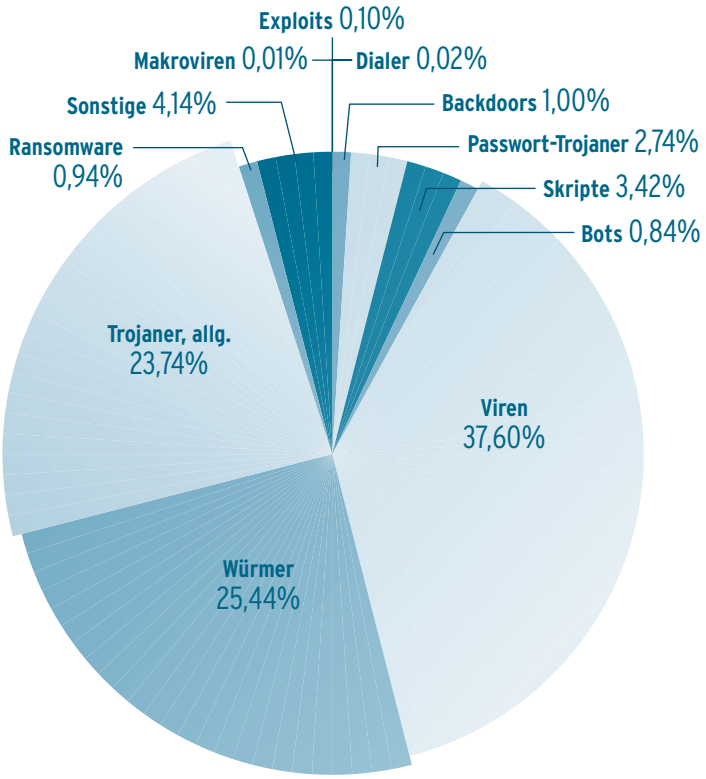
Trotz eines deutlichen Rückgangs der von den AV-TEST Systemen ermittelten Anzahl an Malware-Samples besteht für Windows-Nutzer kein Grund zur Entwarnung. Windows ist und bleibt das meistattackierte Betriebssystem. Zwar verringerte sich die Anzahl von Malware-Samples 2016 im Vergleich zum Vorjahr um 15 Prozent. Allerdings stieg die Fieberkurve im ersten Quartal 2017 wieder um sieben Prozent an. Zum Zeitpunkt des Abschlusses dieses Reports Ende Juni 2017 zielten bereits über 600 Millionen der von AV-TEST erfassten Schadprogramme auf das vielgenutzte Betriebssystem aus Redmond. Ohne einen guten Virenschutz ist das Internet längst nicht mehr sicher.

Viren, Würmer und Trojaner

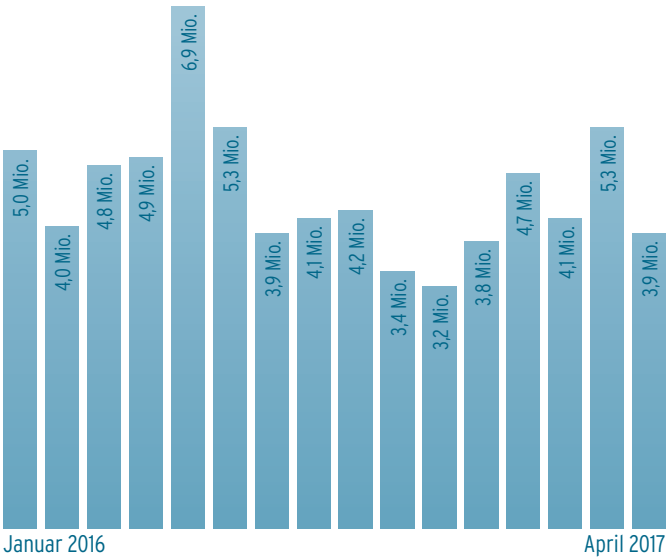
Ein Blick auf die Entwicklung von Windows-Malware zeigt genau, welche Arten von Schadprogrammen für Cyberkriminelle 2016 am lukrativsten waren. Denn wie jedes andere Produkt im Markt müssen auch Schadprogramme Gewinne für ihre Entwickler abwerfen. Nur bei Malware mit einem entsprechenden Return of Investment lohnt sich die Weiterentwicklung, also das Investieren von Zeit und Geld. Der wirtschaftliche Erfolg von Schadsoftware lässt sich anhand einiger Kennzahlen ablesen.

Bereits die bloße Häufigkeit des Auftretens eines Schadcodes kann Auskunft darüber geben, wie erfolgreich dieser ist. So dominierten 2016 klassische Viren den Malware-Markt für Windows. Mit mehr als 37 Prozent war rund jede dritte

Malware-Verteilung unter Windows 2016



Entwicklung neuer Malware für Windows 2016 + Q1 2017



Malware ein Vertreter dieser Gattung. Ein Grund dafür liegt natürlich in der Art ihrer Verbreitung: Als nicht selbstständige Programmroutinen, die sich erst bei Aktivierung durch das Opfer reproduzieren, indem sie immer weitere Programmdateien infizieren, ist ihnen die explosionsartige, oft unkontrollierbare Vermehrung bereits im Programmcode vorbestimmt. Allerdings erleichtert diese Art der Verbreitung Scan-Engines die Erkennung solchen Schadcodes. Damit Viren erfolgreich sind, müssen sie also in Massen auftreten, denn eine kontrollierte Verbreitung, wie bei anderen Schadprogrammen, ist ihnen verwehrt.

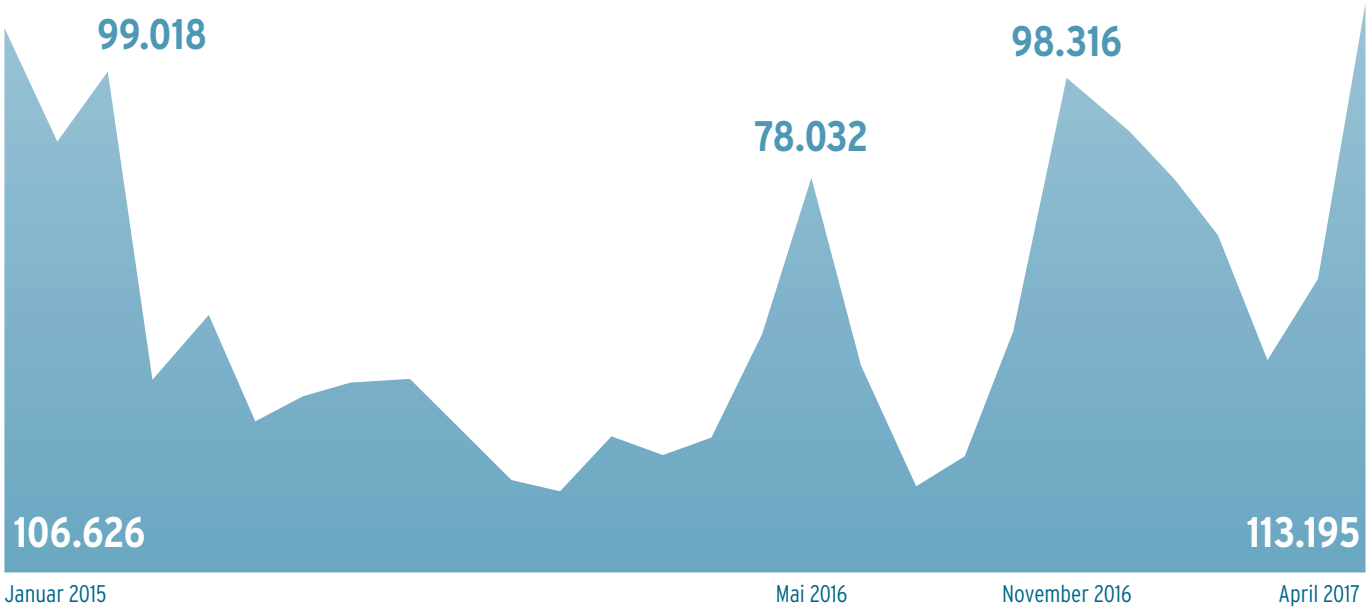
Ebenfalls massenhaft traten 2016 Würmer auf. 25,44 Prozent aller erfassten Schädlinge waren dieser Malware-Gattung zuzuordnen. Cyberkriminelle schätzen den sich selbst verbreitenden Schadcode vor allem wegen seiner hohen Verbreitungsgeschwindigkeit und der Vielzahl möglicher Funktionen. Computerwürmer können quasi jeden möglichen Weg zur Infektion von Systemen nutzen. So verbreiten sie sich über infizierte USB-Sticks, innerhalb von Netzwerken sowie per Drive-by- oder Direkt-Download und per E-Mail. Auf befallenen Rechnern laden sie beliebigen Schadcode nach, etwa Trojaner.

Auch Trojaner waren 2016 mit über 23 Prozent stark vertreten. Und zu der ohnehin stark verbreiteten Malware-Gattung müssen zudem noch 2,74 Prozent Passwort-Trojaner sowie 0,94 Prozent Ransomware addiert werden. Denn beide Malware-Familien der Gattung „Trojaner" werden in diesem Report aufgrund ihrer Bedeutung gesondert erfasst.

Ransomware: die High-Tech-Malware

Dass auch 2016 das „Jahr der Ransomware" war, lässt sich nicht über die Verbreitungszahlen erkennen. Mit nicht einmal einem Prozent am Gesamtanteil der Malware für Windows erscheinen die Erpresser-Trojaner eher wie eine Randerscheinung. Dass man mit einer solchen Einschätzung schon im Vorjahr ziemlich falsch lag, erklärt sich über die Wirkweise sowie den 2016 verursachten Schaden dieser Trojaner-Gattung. Um für seine Entwickler die gewünschten Gewinne zu erwirtschaften, ist keine mit klassischen Viren vergleichbare Streuung nötig, denn bei Ransomware handelt es sich um „High-Tech-Malware", die sich ihre Opfer vor allem zielgerichtet im Business-Umfeld sucht. So erfolgt etwa der Versand mit Ransomware verseuchten E-Mails fast ausschließlich werktags, wie die Messwerte der AV-TEST Systeme beweisen.

Entwicklung Ransomware Windows 2015 – Q1 2017



Hoch komplexe Verschlüsselung

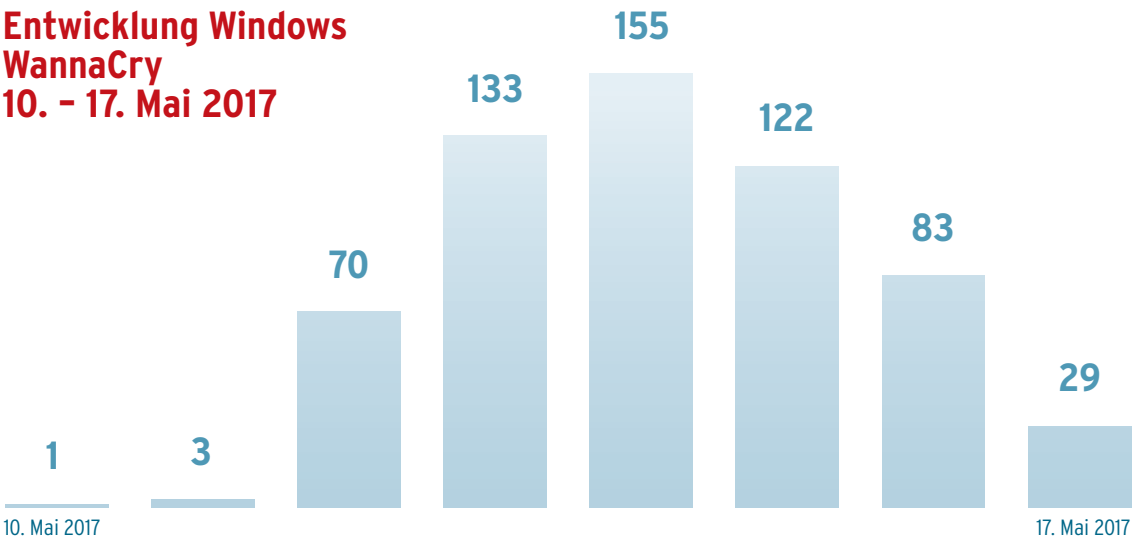
Die Schädlinge verschlüsseln Dateien oder komplette Rechner mit hoch komplexen Verschlüsselungsverfahren auf dem letzten Stand der Technik. Dabei kommen hohe Schlüssellängen zum Einsatz, wie beispielsweise beim RSA-Verfahren Schlüssel zwischen 1024 bis 4096 Bit, bei ECDH bis 192 Bit und bei AES bis 256 Bit – damit sind diese Schlüssel so gut wie nicht zu knacken. Zudem nutzen Erpressertrojaner eine ausgeklügelte Server-Infrastruktur zur Errechnung, Verwaltung und Vergabe der Schlüssel, mit denen Opfer gegen Lösegeld Dateien und Rechner entschlüsseln können. Zur Abwicklung der Online-Erpressung kommt quasi jede verfügbare Online-Währung samt ihrer anonymen Server-Infrastruktur zum Einsatz. So lassen sich sowohl massenhaft geringe Erpressungssummen zwischen 100 und 500 Euro über Währungen wie UCash und PaySafeCard eintreiben und waschen. Aber auch große Summen, wie etwa bei der Online-Erpressung des Krankenhauses Hollywood Presbyterian Medical Center in Los Angeles im Februar 2016 sind leicht einzutreiben. Die Erpressungssumme von 15.000 Euro kassierten die Cyberkriminellen bequem, anonym und kostenlos über Bitcoin.

Hoch komplex und hoch flexibel

Doch auch die gezielte Verbreitung zeigt die Leistungsfähigkeit von Ransomware: Mit zielgerichteten Angriffen nahmen Cyberkriminelle 2016 kritische Branchen aufs Korn; insbesondere öffentliche Verwaltungen, das Gesundheitswesen und der Einzelhandel wurden Opfer gezielter Ransomware-Kampagnen, die meist per E-Mail-Attachment ausgelöst wurden. Wie treffsicher Kriminelle mit Ransomware agieren können, zeigt etwa die Attacke durch die Ransomware GoldenEye Anfang Dezember 2016. Die als Bewerbungs-E-Mail getarnte Malware griff in der ersten Welle nahezu ausschließlich Personalabteilungen von Unternehmen an.

Dass sich Ransomware auch für Masseninfektionen eignet, bewiesen eindrucksvoll die WannaCry-Attacken im Mai dieses Jahres mit mehr als 230.000 infizierten Windows-Rechnern in über 150 Ländern. Dieser Fall zeigt, wie hoch die Entwicklungsstandards solcher Malware sind, den Kriminelle als Service vermieten. So infizierte WannaCry Computer über Zero-Day-Exploits, mit denen der US-Geheimdienst NSA vorher weltweit Rechner bespitzelte. Durch einen Einbruch der Hacker-Gruppe „The Shadow Brokers“ gelangten diese von der NSA gehorteten Windows-Schwachstellen frei verfügbar ins Internet und wurden für den Schadcode der Ransomware WannaCry genutzt. Zwar bot Microsoft zeitnah Patches für die betroffenen Betriebssysteme an, jedoch werden Betriebssystem-Updates von Privatleuten wie Unternehmen oft ebenso stiefmütterlich behandelt wie das regelmäßige Erstellen von Backups. So stellten sich unter anderem große Teile des britischen Gesundheitswesens, darunter etliche Krankenhäuser, der große spanische Provider Telefonica sowie die Deutsche Bahn als zu leicht angreifbar heraus.

Entwicklung Windows WannaCry
10. – 17. Mai 2017



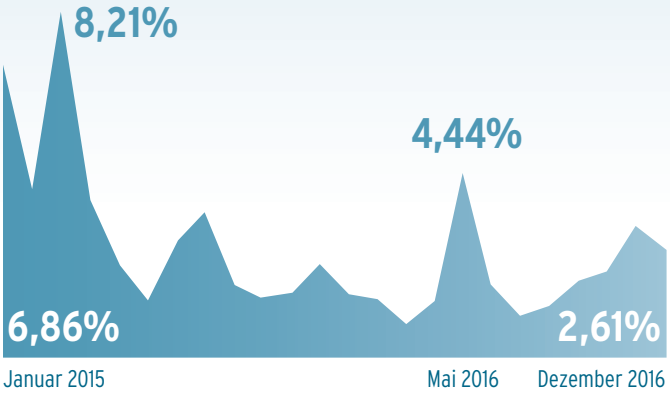
Attacken auf das Bankensystem SWIFT

Auch Passwort- und Banking-Trojanern zeigten 2016 eine interessante Entwicklung. Zwar ging die Verbreitung (2,74%) dieser extrem spezialisierten Malware im Vergleich zum Vorjahr (3,02%) insgesamt leicht zurück, sie steht aber in keinem Verhältnis zu dem verursachten Schaden. Der war besonders Anfang des Jahres erheblich. Bereits im Februar 2016 verlor die Bangladesh Central Bank über 81 Millionen Dollar durch eine Malware-Attacke. Ebenfalls im Februar erfolgte ein ähnlicher Angriff auf die New York Federal Reserve. Doch dabei blieb es nicht.

Wie die von AV-TEST gemessene Verbreitung von Passwort- und Banking-Trojanern zeigt, waren im ersten Quartal des letzten Jahres besonders viele Samples ähnlichen Schadcodes aktiv. Einige davon wurden mit großer Sicherheit für Attacken auf das Banking-Netzwerk Swift (Society of Worldwide Interbank Financial Telecommunication) genutzt. Über entsprechende Malware verschafften sich Kriminelle Zugriff auf Bankenrechner, die mit dem Zahlungssystem verbunden waren. Dies bestätigte der belgische Dienstleister dann später auch in einer Warnung an seine Kunden, 3.000 Finanzinstitute rund um den Globus. Die Angreifer hätten im Swift-System die Identität befugter Nutzer annehmen und in deren Namen tätig werden können, hieß es in dem Schreiben. Welche Banken betroffen waren und wie hoch die Schadenssummen waren, darüber schwieg sich das Brüsseler Unternehmen aber aus. Ende April gab Swift ein entsprechendes Sicherheits-Update heraus.

Der monetäre Erfolg von Banking-Trojanern ist offensichtlich: Im Verhältnis zum Aufwand lohnt sich der Angriff auf wenige Swift-Nutzer natürlich deutlich mehr als massenhafte Angriffe auf Privat-PCs oder Rechner kleiner Firmen.

Entwicklung Windows Passwort-Trojaner 2015/16



TOP 10 Windows-Malware 2016

1	ALLAPLE	7.628.795
2	VIRUT	5.689.139
3	RAMNIT	5.020.383
4	VIRLOCK	3.092.764
5	AGENT	2.890.132
6	PARITE	1.811.675
7	SALITY	1.514.886
8	LAMER	1.422.229
9	MIRA	1.364.763
10	SMALL	1.284.994

Die Top 10 der Windows-Schädlinge

Da Viren, Würmer und Trojaner 2016 zu den meistverbreiteten Schädlingen zählten, verwundert es kaum, dass sich auch die Top 10 der Windows-Malware aus diesen Gattungen rekrutieren.

Auch in diesem Jahr verteidigt der seit 2006 im Internet aktive Windows-Wurm Allaple Platz 1 auf der Rangliste der meistverbreiteten Malware. Er verbreitet sich erfolgreich beim Besuch infizierter Websites. Einmal in ein Windows-System eingedrungen, verteilt er sich selbst in kennwortgeschützten Netzwerken von Rechner zu Rechner, wobei er als polymorpher Schädling ständig seinen Programmcode verändert, was die Erkennung der Malware erschwert. Seine unterschiedlichen Samples machten über 15 Prozent der gesamten Malware-Erkennung für Windows-Systeme aus!

Bei Virut, Ramnit, Parite, Sality, Lamer und Small handelt es sich um Computerviren im klassischen Sinne. Sie infizieren massenhaft Dateien und verbreiten sich über unterschiedliche Kanäle, darunter infizierte Websites, PDF-Downloads und auch infizierte Dateien auf portablen Speichermedien wie USB-Sticks.

Auf Platz 4 steht mit Virlock ein wirklich ausgeklügeltes Stück Programmcode unter den Top 10. Die Ransomware wird ständig weiterentwickelt und gehört zu den wenigen Programmen, die sowohl einzelne Dateien als auch komplette Systeme verschlüsseln kann. Zudem funktionieren Varianten von Virlock nicht ausschließlich wie Ransomware, sondern können Dateien befallen und sich so wie ein Virus weiterverbreiten. Auf diese Weise machte Virlock 2016 Cloud-Speicher unsicher, indem sich die Software über infizierte Dateien verbreitete, die von mehreren Anwendern per Cloud synchronisiert wurden.

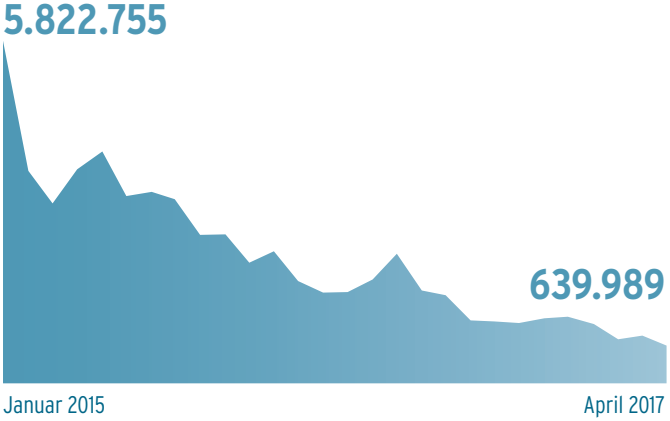
PUA: Windows-Spionage auf dem Rückzug

Zum Abschluss des Kapitels eine positive Entwicklung: Das Ausspähen von Windows-Nutzern über Schnüffelprogramme durch die Werbe-Industrie wurde 2016 spürbar zurückgefahren. Und dieser Trend setzt sich im ersten Quartal dieses Jahres fort. Noch deutlicher wird diese Entwicklung, wenn man die Daten des Jahres 2015 mitbetrachtet: Sahen sich Windows-Nutzer, die ihre Privatsphäre schützen wollten, im Januar 2015 noch sechs Millionen neuen Samples von Potenziell Unerwünschten Anwendungen gegenüber, sank deren Rate bis April 2017 auf unter ein Sechstel.

Trend 2017

Im ersten Quartal dieses Jahres zeichnet sich ein klarer Trend zu mehr klassischen Viren für Windows ab, deren Anteil an der Malware-Verteilung gegenüber 2016 von 37 auf 46 Prozent steigt. Auch die Anzahl der Windows-Trojaner legt in Q1 deutlich zu und klettert von 23 auf über 30 Prozent. Dieser Entwicklung folgt auch die Zahl der ermittelten Ransomware-Samples, die um ein Drittel auf 1,55 Prozent anwächst. Diese Entwicklung geht auf Kosten der Internetwürmer, die mit einem prozentualen Rückgang von 25 auf sechs Prozent klar zu den Verlierern im Malware-Markt gehören.

Entwicklung PUA Windows 2015 – Q1 2017



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

Sicherheitsstatus macOS

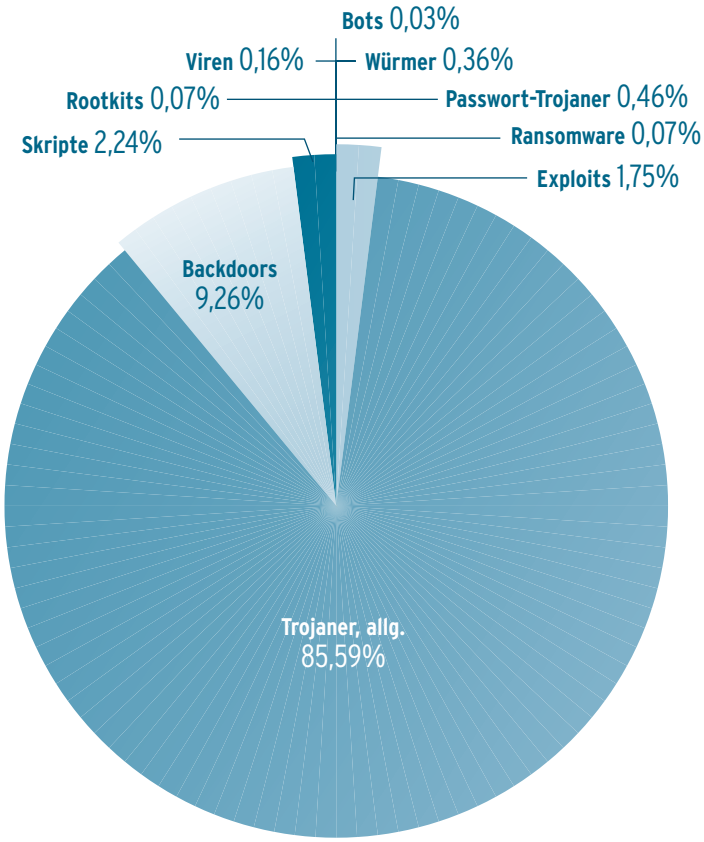
Den Nimbus der absoluten Sicherheit ist Apples Betriebssystem schon seit Jahren los, und nicht einmal absolute Mac-Fans gehen noch ungeschützt ins Internet. Das ist auch gut so, denn die Anzahl von Malware für Rechner aus Cupertino explodierte 2016

Keine sichere Bank

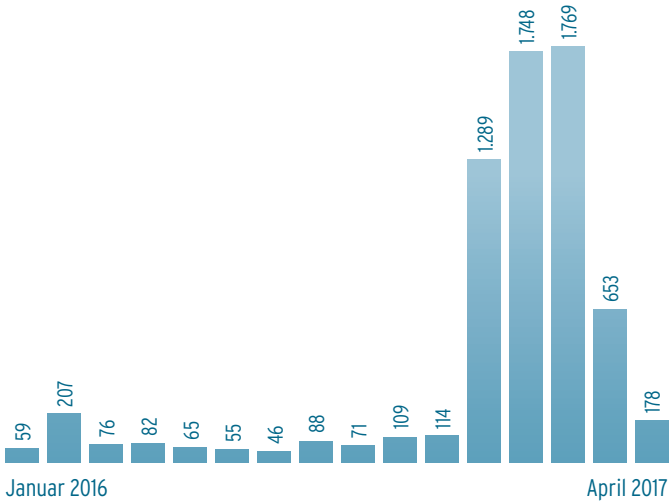
Bei einer Steigerungsrate von über 370 Prozent im Vergleich zum Vorjahr ist es nicht übertrieben, von einem explosionsartigen Anstieg zu sprechen. Allerdings muss man dabei auch die Gesamtzahl an Schadprogrammen im Auge behalten, mit denen Kriminelle versuchen, Mac-Nutzer abzuzocken: Waren es 2015 überschaubare 819 unterschiedliche Schädlinge, die auf macOS zielten, mussten Apple-Nutzer ihre Geräte 2016 bereits vor 3033 Malware-Samples schützen.

Das hört sich im Verhältnis zu Hunderten Millionen Schadprogrammen für Windows nach wie vor harmlos an. Es beschreibt aber einen gefährlichen Trend, denn die massenhafte Steigerung von Malware-Samples für macOS bedeutet nichts anderes, als dass dieser Markt für Kriminelle zunehmend interessanter wird. Mit anderen Worten: Die ruhigen Zeiten für Apple-Nutzer sind spätestens jetzt vorbei, wenn das nicht bereits 2014 mit der Massen-infektion von Macs mit dem Flashback-Trojaner der Fall war. Allerdings vertrauen einige Mac-Nutzer nach wie vor auf ein trügerisches Sicherheits-versprechen, dass auch durch Werbeaussagen von Apple befeuert wurde.

Malware-Verteilung 2016 macOS



Malware-Entwicklung macOS 2016



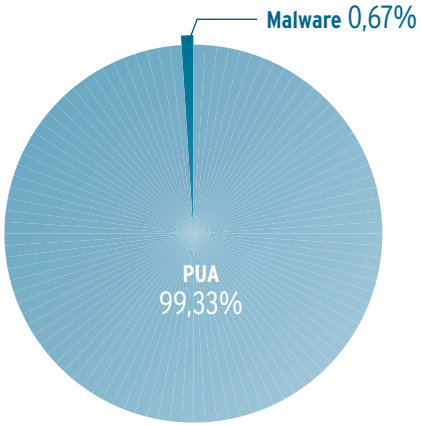
Cyberkriminelle in der Entwicklungsphase

Der Anstieg der Anzahl von Malware-Samples begann im Dezember 2016. Davor bewegte sich die Schädlingszahl quasi auf dem Niveau des Vorjahres. Das bedeutet, dass sich Cyberkriminelle seitdem in der Experimentierphase befinden und ausloten, welche Malware und welcher Aufwand sich für die Infektion des Betriebssystems aus Cupertino lohnt. Diese Annahme bestätigt auch die Verteilung der unterschiedlichen Malware-Samples beziehungsweise deren Entwicklung.

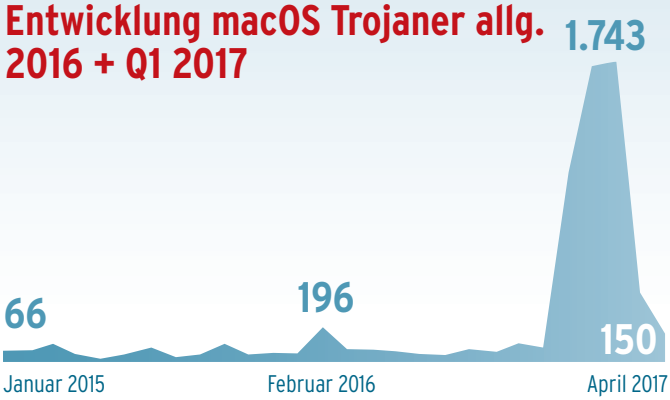
Anders als bei Windows-Rechnern halten Cyberkriminelle klassische Viren für den Einsatz auf Mac-Systemen offensichtlich nicht für sinnvoll. So fällt der Anteil dieser Malware-Gattung mit 0,16 Prozent äußerst gering aus. Das kann unter anderem daran liegen, dass die Software-Architektur des Betriebssystems sich anders als Windows nicht sonderlich für die Verbreitungsmuster dieser Malware eignet.

Interessanter für das Ausloten wirtschaftlich verwertbarer Daten scheinen Kriminellen dagegen Backdoors zu sein. In den Experimentierstuben für Mac-Malware machten die Hintertür-Programme, die heimlichen Zugriff auf fremde Systeme erlauben, 2016 gleich 9,26 Prozent der Gesamt-Malware-Summe aus. Größer war damit 2016 nur noch die überragende Anzahl an Trojanern, denen Kriminelle offensichtlich den größten Erfolg auf macOS zutrauen: 86,12 Prozent aller Apple-Schädlinge gehören dieser Gattung an – verschwindend gering ist allerdings noch der Anteil an Erpressertrojanern (0,07%) und Passwort-Trojanern (0,46%).

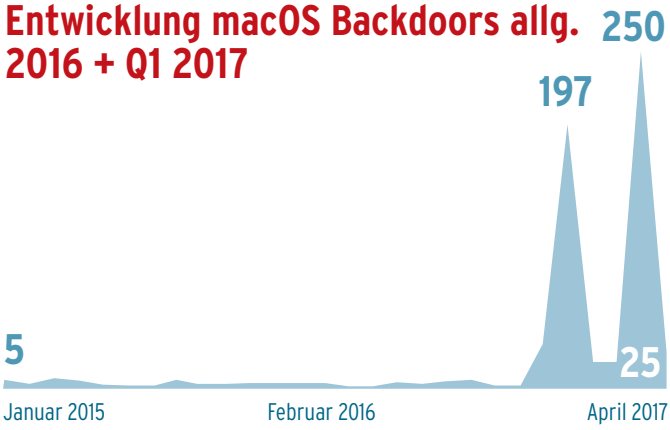
Schädlingsverteilung macOS 2016



Entwicklung macOS Trojaner allg. 2016 + Q1 2017



Entwicklung macOS Backdoors allg. 2016 + Q1 2017



Trend 2017

Um diese Entwicklung besser analysieren zu können, hilft ein Blick auf die Zahlen des ersten Quartals 2017. Sie zeigen ein wellenartiges Auftreten großer Mengen von Bots mit Spitzen am Ende des letzten und Anfang dieses Jahrs sowie gleiche Muster bei Trojanern. Auch das spricht dafür, dass sich Kriminelle gerade in der Erprobungsphase entsprechender Malware befinden und prüfen, welcher Schadcode die wirtschaftlich relevantesten Ergebnisse liefert. Hier könnte bereits das zweite Quartal eine deutliche Entwicklung zeigen. Eine ganz klare Erkenntnis lassen die Zahlen für Quartal 1 2017 allerdings auch schon zu: Die Attacken auf macOS nehmen weiter zu. Im Verhältnis zum Vorjahr steigert sich die Zahl der Malware-Samples erneut, diesmal um über 140 Prozent auf die Gesamtsumme von 4348.

Top 10 der Mac-Malware

Mit Flashback führt ein alter Bekannter die Rangliste für Mac-Malware an. Das seit September 2011 bekannte Schadprogramm ist offensichtlich nicht totzukriegen und wird ständig weiterentwickelt. Ursprünglich als Adobe-Flash-Installationsdatei getarnt, schummelte sich der Trojaner später als Drive-by-Download durch ungepatchte Java-Sicherheitslücken im Browser auf den Computer. Nach wie vor erfreut sich Flashback starker Verbreitung, mehr als jede vierte im letzten Jahr von den AV-TEST Systemen registrierte Mac-Malware war ein Flashback-Sample.

Zwar ist der Anteil von Erpressertrojanern in der Gesamtsumme der Mac-Malware verschwindend gering. Über den Erfolg eines Schadprogramms sagt das allein aber noch nichts aus. Bestes Beispiel ist Platz 3 der Schadprogramme 2016, eine der ersten Ransomwares für Apple-Rechner. Bereits im letzten Sicherheitsreport wies AV-TEST auf KeRanger hin, der im ersten Halbjahr 2016 bereits als Neuzugang Platz 8 der Malware-Top 10 belegte.

TOP 10 macOS-Malware 2016

1	FLASHBACK	633
2	MACONTROL	254
3	KERANGER	195
4	XCODEGHOST	163
5	HACKBACK	140
6	JAHLAV	112
7	GETSHELL	105
8	OPINIONSPY	64
9	MORCUT	64
10	OLYX	46

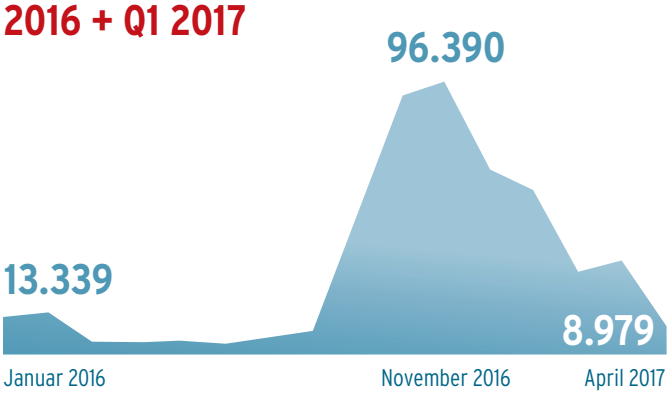
Der Schädling, der auf OS-X-Nutzer zielt und Dokumente verschlüsselt, enterte Mac-Rechner unter anderem als getarnte BitTorrent-Software Transmission. Perfide: Nach der Infektion lässt KeRanger drei Tage verstreichen, bevor die Malware mit der Verschlüsselung von Dokumenten startet.

Mac-User ausgespäht

Offensichtlich sind die Daten von Mac-Nutzern für die Werbeindustrie besonders lukrativ. Zumindest lässt der Anteil der PUA an der Gesamtmenge der Schädlinge für Apples Betriebssystem keinen anderen Schluss zu. Denn in der Gesamtverteilung machte die massiv wachsende Anzahl an Malware-Samples für macOS nicht einmal ein Prozent aus. Mit über 99 Prozent bestand der Großteil der Schädlinge klar aus PUA-Samples.

Ein Blick auf die Entwicklung der Spionage-Tools der Werbeindustrie offenbart einen dramatischen Anstieg der Samplezahlen im vierten Quartal des Jahres 2016. In der absoluten Hochphase im November kratzte die Anzahl neuer von den AV-TEST Analysesystemen gemeldeter Samples knapp an der Hunderttausender-Marke. Seither fällt sie aber genauso drastisch ab, um sich auf den Normalwert von unter 20.000 neuen Samples pro Monat einzupegeln. Es ist von einer Versuchsphase zur Anpassung der Schädlinge auf neue Erkennungsmuster der Schutzfunktionen von macOS auszugehen.

Entwicklung macOS PUA 2016 + Q1 2017



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

Sicherheitsstatus ANDROID

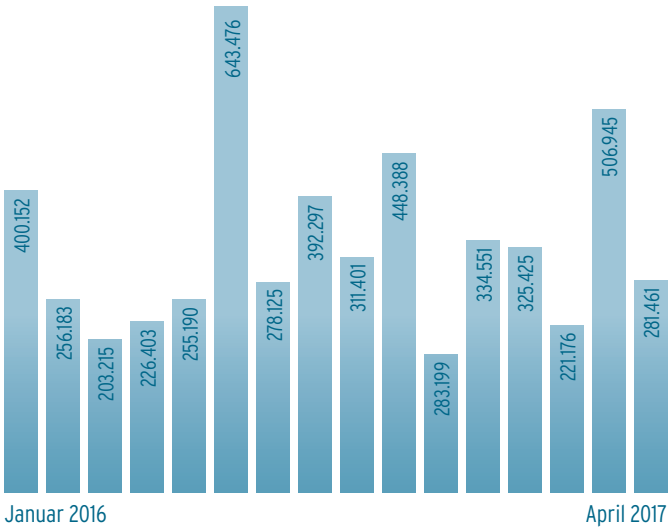
Die Zahlen sprechen eine klare Sprache: Wer mit Angriffen auf Mobilgeräte Geld machen will, greift Android-Geräte an. Für andere Mobilplattformen lohnt sich die Entwicklung von Schadprogrammen schlichtweg nicht. Der Anteil an der Malware-Gesamtentwicklung für iOS, Windows Mobile und andere rutscht darum unter noch darstellbare Prozentmengen, während sich die Zahl der neuen Schädlinge für Android im Vergleich zum Vorjahr verdoppelt.

Wellenartige Angriffe

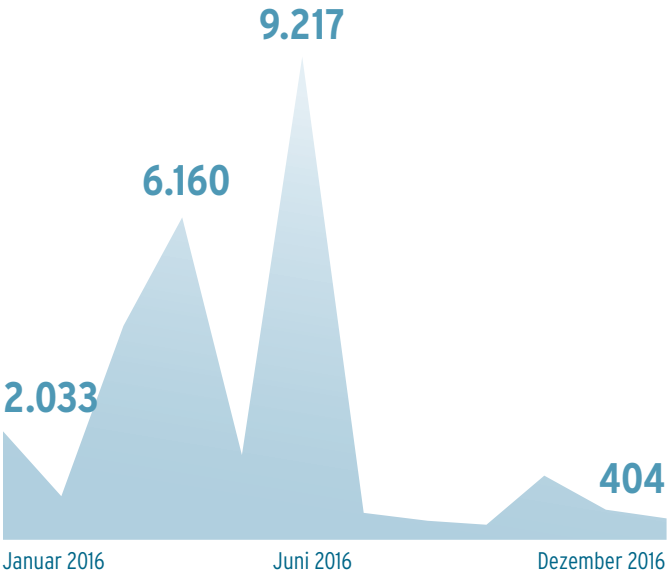
Bei der Betrachtung der Malware-Entwicklung von 2015 zu 2016 fällt – neben der Verdoppelung der ermittelten Sample-Menge auf über 4 Millionen neue Schadprogramme für Android im Jahr 2016 – vor allem eines auf: Ab Jahresbeginn 2016 pushten Kriminelle Malware in Wellen in den Markt, was auf Tests neuer Malware beziehungsweise neuer Verbreitungswege, etwa auf das Ausprobieren neuer Android-Lücken, hindeutet. Die Peaks dieser Entwicklung liegen 2016 im Januar, August und Oktober. Den größten Ausschlag liefert Mitte des Jahres allerdings der Juni. In diesem Monat messen die AV-TEST-Systeme extreme Aktivität und mit exakt 643.476 neuen Schadprogrammen für Android den bisherigen Höchstwert seit Veröffentlichung des Google-Betriebssystems.

Und tatsächlich bietet Android Kriminellen zu diesem Zeitpunkt zahlreiche Lücken, durch die sich Malware einschleusen lässt. Dementsprechend ist Google gezwungen zu reagieren. Der Patchday im Juli übertrifft alle bisherigen bei Weitem: Über 100 Lücken schließt Google mit zwei kurz aufeinanderfolgenden Sicherheitsupdates, etwa ein Drittel der Lecks sind sicherheitskritisch und betreffen unter anderem die Krypto-Bibliotheken OpenSSL und BoringSSL sowie USB-Treiber. Mit dem bisher größten Android-Patch schloss Google zwar massenhaft bekannte Lücken, für den Juni 2016 zeigten die Erfassungssysteme von AV-TEST allerdings insgesamt 9.217 Exploits für alle Android-Versionen insgesamt, ebenfalls ein beeindruckender Höchstwert.

Malware-Entwicklung Android 2016 + Q1 2017



Entwicklung Android Exploits 2016



Trojaner als Hauptwerkzeug

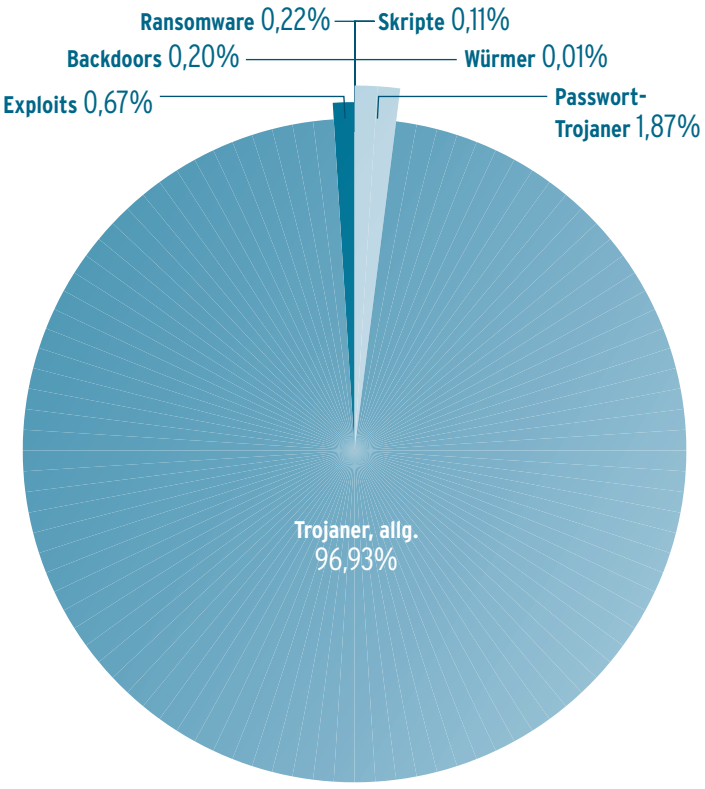
Mit Abstand am häufigsten nutzten Kriminelle im Jahr 2016 mit Trojanern infizierte Apps. Bei einem Anteil von über 97 Prozent lässt sich mit Fug und Recht davon sprechen, dass andere Malware-Gattungen bei Angriffen auf Mobilgeräte 2016 quasi keine Rolle spielten.

Mit nur 0,22 Prozent Anteil an der Gesamtmenge der Android-Malware waren Erpressungstrojaner zwar zahlenmäßig gering vertreten, und ihre Zahl war 2016 mit 8.822 gegenüber dem Vorjahr (12.521) rückläufig. Dennoch stellte Ransomware 2016 eine nicht zu unterschätzende Gefahr für Mobilgeräte dar. Und wie die Entwicklung im ersten Quartal 2017 zeigt, steigt die Zahl der Ransomware-Samples wieder sprunghaft an. Wie auch bei Windows und macOS lassen die Verbreitungszahlen bei Ransomware nur geringfügige Schlüsse auf den Erfolg von Malware-Angriffen zu.

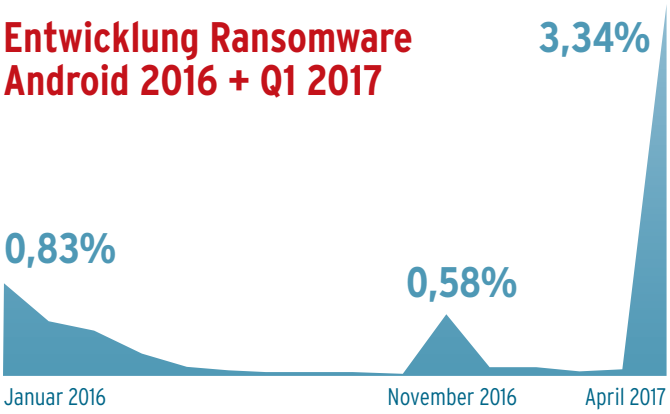
So enterte mit „Lockscreen" 2016 erstmals eine Android-Ransomware die Malware-Top 10. Der Schädling verbreitete sich sowohl über infizierte Apps aus Quellen abseits Googles Play Store als auch über Drive-by-Downloads. Auf infizierten Geräten sperrte die Malware den Homescreen und verlangte je nach Kampagne Lösegeld für die Freischaltung des Geräts. In den ersten Versionen war die Malware noch verhältnismäßig leicht zu überlisten, denn die immer gleiche Freischalt-PIN war im Programmcode der Malware ersichtlich. Neuere Versionen von Lockscreen, die im Laufe des Jahres auftauchten, erfuhren diverse Upgrades. Unter anderem waren einzelne Samples in der Lage, sich Adminrechte über das Root-Verzeichnis von Geräten zu besorgen und die bisherige Nutzer-PIN direkt in den Geräteeinstellungen zu verändern.

Auch eine andere Familie der Gattung „Trojaner" machte 2016 von sich reden, denn auch bei den Passwort-Trojanern zeigten die Warnsysteme von AV-TEST eine wellenförmige Entwicklung an. Die hatte den ersten von zwei markanten Ausschlägen im ersten Quartal des Jahres und übertraf diesen anschließend noch im vierten. Zu diesem Zeitpunkt wütete unter anderem die Android-Malware Gooligan. Der Android-Trojaner verbreitete sich durch über 80 infizierte Apps aus unsicheren Dritt-App-Stores und infizierte im großen Stil Geräte, auf denen die Android-Versionen Ice Cream Sandwich, Jelly Bean und KitKat (Version 4) sowie Lollipop (Version 5) liefen.

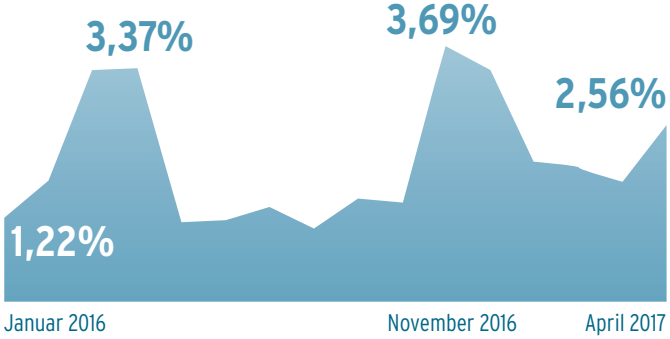
Malware-Verteilung Android 2016



Entwicklung Ransomware Android 2016 + Q1 2017



Entwicklung Passwort-Trojaner Android 2016 + Q1 2017



Die Top 10 der Android-Schädlinge

Wie im letzten Jahr ungeschlagen auf Platz 1 der Top 10 waren Trojaner der Familie „Agent". Ein Grund dafür ist die Art ihrer Verbreitung. Wie auch Shedun müssen diese Trojaner nicht mehr warten, bis unbedarfte Nutzer sie als infizierte App selbst auf ihre Geräte laden. Auch der Agent-Trojaner infiziert Android-Smartphones und Tablets per Drive-by-Download. Einmal auf dem Gerät, kann Agent anderen Schadcode nachladen, die Sicherheitseinstellungen herabsetzen und private Daten an Server im Internet verschicken.

Wie viele andere Android-Schädlinge auch erlebte das Schadprogramm auf Platz 2 der Malware-Top 10 im Juni 2016 seinen fragwürdigen Höhepunkt. Die Rede ist von Trojaner Shedun alias HummingBad, der Mitte des Jahres an die 10 Millionen Geräte rund um den Globus infizierte, indem er sich unter anderem per Drive-by-Download über infizierte Porno-Websites verbreitete. Betroffen waren zum Großteil Geräte, auf denen KitKat und Jelly Bean lief. Auf diesen Geräten wurde Pop-up-Werbung eingespielt. Deutlich schlimmer war jedoch, dass sich die Malware im Hintergrund Zugang zu Google-Konten verschaffte und diese für automatisierten Klick-Betrug missbrauchte.

TOP 10 Android-Malware 2016

1	AGENT	2.004.880
2	SHEDUN	417.945
3	FAKEINST	136.544
4	SMSSPY	134.384
5	LOCKSCREEN	131.782
6	OPFAKE	109.833
7	TROJANSMS	77.185
8	SMSTHIEF	63.279
9	LOTOOR	58.731
10	SMFORW	55.723

Trend 2017

Für Android verzeichnen die Erkennungssysteme von AV-TEST steigende Zahlen in den Bereichen Banking-Trojaner und Ransomware. Der Anteil der Letzteren an der Gesamt-Malware wuchs auf das Dreifache des vorjährigen Werts. Gemessen am Gesamtanteil der Schadprogramme, sinkt die Anzahl von Trojanern zwar geringfügig. Mit über 96 Prozent bleiben sie aber auch 2017 die schärfste Waffe von Cyber-Kriminellen, die es auf Mobilgeräte abgesehen haben.

AV-TEST av-test.org

Die AV-TEST GmbH überprüft im Zweimonatsturnus regelmäßig alle auf dem Markt relevanten Schutz-Lösungen 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

Welche Strategien verfolgen Kriminelle bei der Verbreitung von Malware? Wer das weiß, kann Gefahren aus dem Netz gezielt abwehren. Die Erkennungssysteme von AV-TEST erfassen Malware-Attacken rund um dem Globus bereits seit Langem. Hier ist die Gefahrenanalyse für 2016

Massenhaft Spam

Beim Blick auf die Malware-Verteilungsstrategien von Online-Kriminellen offenbart unterschiedliche professionelle Ansätze: Größtenteils setzten Cyber-Gauner beim Streuen ihrer Schadprogramme auf die seit Langem erfolgreichen, klassischen Verbreitungskanäle. Insbesondere über groß angelegte E-Mail-Kampagnen wurden im Jahr 2016 ans Internet angebundene Geräte mit Schadcode infiziert. Internationale Spam-Kampagnen waren darum oft nicht nur nervig, sondern auch höchst gefährlich. Im Vergleich zu E-Mails mit verseuchtem Schadcode im Anhang setzten die Gauner häufig auf digitale Nachrichten, die arglose Nutzer mit eingebetteten Links auf Malware-verseuchte Internetseiten lockten. Aktuelle Grafiken aus ständig aktualisierten Messdaten finden Sie auf den Statistikseiten des AV-TEST Instituts.

Unter den Ländern, die 2016 zu den größten Verbreitern „schlechter Nachrichten" gehörten, war auch Deutschland. Immerhin 3,1 Prozent allen Spams, darunter auch Malware-verseuchte Post, ging von Deutschland aus, was in den Top 10 der Spam-versendenden Länder Platz 8 ergibt. Deutlich davor stehen jedoch die „Spam-Meister" Indien, die USA sowie Vietnam, die 2016 bereits über ein Drittel des globalen Spams zu verantworten hatten.

Geprüfte Webseiten in 2016

Webseiten gesamt
ca. 1.100 Milo.

Top 10 Spamversender 2016

1	INDIEN	12,0%
2	VEREINIGTE STAATEN VON AMERIKA	11,9%
3	VIETNAM	11,8%
4	CHINA	5,6%
5	BRASILIEN	4,8%
6	POLEN	3,4%
7	IRAN	3,3%
8	DEUTSCHLAND	3,1%
9	MEXIKO	3,0%
10	RUSSISCHE FÖDERATION	2,2%

Exploit-Kits, Hacks und Malvertising

Für die Malware-Verbreitung über gängige Exploit-Kits erstellten Kriminelle auch 2016 massenhaft eigene, infizierte Internetseiten. Zwar verschwanden Mitte des Jahres die bis dato meistgenutzten Malware-Baukästen Angler und Nuclear von der Bildfläche, was zumindest zeitlich mit einem deutlichen Rückgang der von AV-TEST gemessenen Gesamt-Malware-Zahlen korrelierte. Doch die beiden viel genutzten Baukästen wurden im umkämpften Markt der Exploit-Kits schnell durch Konkurrenz-Produkte wie RIG, Magnitude, Sundown und andere ersetzt, mit denen sich ebenso komfortabel groß angelegte Malware-Kampagnen, darunter auch mit vielen Ransomware-Samples, automatisieren lassen. Oft nutzten die Exploit-Kits 2016 Lücken der Adobe-Programme Flash Player und Reader sowie des Internet Explorers von Microsoft automatisiert aus. Je nach eingesetztem Exploit-Kit variierten die Mietpreise. Mit 1500 Dollar pro Woche war das Exploit-Kit Neutrino mit Abstand das teuerste Angriffswerkzeug der Malware-Mafia. Deutlich günstiger war der Einsatz von RIG mit etwa 200 Dollar pro Woche.

Auch 2016 nutzten Kriminelle zur Verbreitung ihrer Schadcodes zudem Online-Angriffe und Website-Hacks viel besuchter Internetseiten und Online-Portale. Die mit knapp 80 Prozent häufigsten Angriffe verzeichneten dabei ungepatchte Online-Auftritte, die mit WordPress erstellt wurden. An zweiter Stelle – mit etwa 15 Prozent aller Angriffe – standen Seiten, die mit Joomla! erstellt wurden. Die Angriffe erfolgten dabei meist auf Lücken ungepatcher Versionen, und oft suchten die Angreifer den Weg auf die Rechner ihrer Opfer über veraltete Plug-ins.

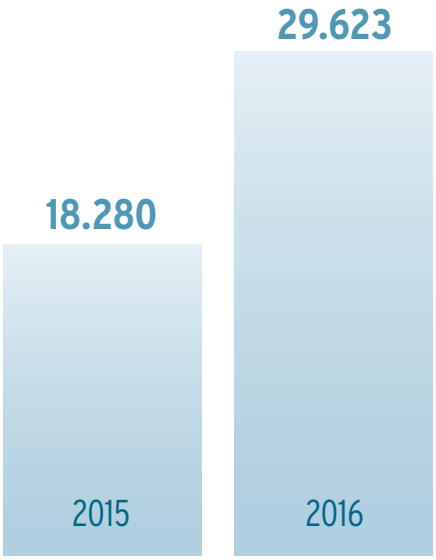
Immer häufiger nutzen Kriminelle auch legale Vermarktungswerkzeuge der Internetwirtschaft. Ein seit 2007 ständig wachsender Trend ist dabei das Malvertising, also das Buchen von Anzeigenfläche auf großen und viel genutzten Internetseiten. Dabei ist den Anzeigenverkäufern der Werbeindustrie meist nicht bewusst, dass einige ihrer Kunden über gebuchte Banner, Pop-ups, Verlinkungen und versteckte iFrames Schadcode übertragen.

160 Millionen Websites im Malware-Check

In einem umfangreichen Test überprüfte das AV-TEST Institut 2016 über 80 Millionen Websites und fand unter ihnen genau 29.632 Internetangebote, die Malware transportierten. Ein Jahr zuvor ergab die gleiche Untersuchung mit gleichem Testumfang lediglich 18.280 verseuchte Seiten. Das entspricht einer massiven Steigerung von über 60 Prozent gegenüber dem Vorjahr!

Die genauen Analysen der AV-TEST-Erfassungssysteme schlüsseln über das ganze Jahr 2016 gut auf, von welchen Internetseiten dabei die größte Gefahr ausgeht. Dazu gehören definitiv Internetseiten, die nicht per SSL geschützt sind. Knapp 92 Prozent aller verseuchten Internetseiten waren HTTP-Seiten.

Schädlinge in geprüften Webseiten



Trend 2017

Das erste Quartal 2017 spiegelt diese Entwicklung übrigens deutlich wider: Der Anteil gefährlicher HTTPS-Seiten ging im Vergleich zum Vorjahr um knapp 3 Prozent auf 4,9 Prozent zurück.

TOP 10 Malware-Domains 2016

1	COM	52,35%
2	SU	7,11%
3	ORG	5,04%
4	NET	4,94%
5	RU	4,05%
6	TO	4,04%
7	CO	3,24%
8	UA	1,73%
9	TR	1,37%
10	US	1,04%

Die gefährlichsten Websites

Die Gefahr, sich beim Surfen mit Malware zu infizieren, ist auf Websites mit der Top-Level-Domain (TLD).COM klar am höchsten: Mit über 52 Prozent gehören .COM-Seiten also zu den gefährlichsten Seiten im Netz. Der Grund dafür ist klar: Sie sind Nutzern am geläufigsten und haben mit Abstand die weiteste Verbreitung. Zudem können sie von jedem rund um den Globus günstig und schnell erworben und angemeldet werden. Zwar hat die Wahl der Domain keinen messbaren Vorteil in Bezug auf das Suchmaschinen-Ranking der Website, allerdings ist der positive psychologische Effekt einer gängigen TLD beim Endanwender kaum zu unterschätzen. Nutzer klicken im Zweifel eher auf eine Internetadresse mit gängiger TLD. Das Vertrauen, selbst wenn es in die Irre führt, ist einfach höher. Das beweist auch das klar sinkende Interesse von Cyberkriminellen an anderen TLDs.

Die gefährlichsten Dateien

Die meistgenutzten Dateiformate zur Verbreitung von Malware werden mit über 33 Prozent klar von den ausführbaren Dateien im .EXE-Format angeführt. Mit mehr als zehn Prozent Abstand folgen komprimierte Dateien mit der Endung .ZIP, die sich nicht nur im direkten Download, sondern auch ideal per E-Mail verteilen lassen (21%). Auf Platz 3 steht das HTML-Format (20%).

TOP 10 File Extensions Malware Q1 2017

1	HTML	39,23%
2	EXE	26,27%
3	ZIP	13,95%
4	RAR	7,85%
5	PHP	6,60%
6	HTM	2,38%
7	ASP	1,84%
8	IZLE	1,74%
9	ASPX	0,10%
10	MP4	0,05%

Trend 2017

Die Messungen für das erste Quartal 2017 deuten einen Wechsel der Verbreitungsstrategie für Malware an: Im Vergleich zum Vorjahr steigt die Gefahr, sich per Drive-by-Download zu infizieren. Mit 39 Prozent steigt die Zahl der infizierten HTML-Seiten sprunghaft um fast ein Drittel und verdrängt sogar die ausführbaren Dateien auf den zweiten Platz. Bei den Domains bestätigt sich dagegen die Entwicklung von 2016 weg von Länder-Domains hin zur gängigen .COM-Seite. Die Zahl der als infiziert gemeldeten .COM-Seiten steigt um sieben Prozent.

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

Sicherheitsstatus IoT

Die Vorzüge der Online-Vernetzung von Dingen des täglichen Gebrauchs sind immens. Sie haben bereits massiven Einfluss auf unser tägliches Leben. Diese Entwicklung lässt sich nicht zurückdrehen. Umso erschreckender ist die mangelhafte Sicherheit der angebotenen Geräte. Das AV-TEST Institut ist mit jahrelanger unabhängiger Forschungsarbeit sowie vierjähriger Zertifizierungspraxis weltweit Pionier auf dem wichtigen Gebiet der IoT-Sicherheit.

Milliarden Geräte ohne Basisschutz

Laut Schätzungen der Finanzexperten von Gartner werden bis 2020 über 20 Milliarden Geräte mit dem Internet gekoppelt sein, die meisten davon, geschätzte 14 Milliarden, in Privathaushalten. Das setzt massive Investitionen in Hardware voraus. Hier prognostiziert Gartner bis 2020 Unternehmensausgaben von etwa 1477 Milliarden Dollar. Verbraucher sollen im gleichen Zeitraum 1534 Milliarden Dollar für internetbasierte Geräte lockermachen. Doch am profitabelsten sind bereits jetzt die angekoppelten Onlinedienste.

Über solche Cloud-Anwendungen werden zukünftig Milliarden Geräte per Internet gesteuert, Daten und Informationen von und über ihre Nutzer erfasst und verarbeitet werden. Doch bereits heute senden, empfangen, speichern und verarbeiten die unterschiedlichsten IoT-Geräte je nach Einsatzgebiet die unterschiedlichsten Nutzerdaten: Smart-Home-Basen steuern über ein breites Spektrum an Sensoren komplette Haushalte: Das Angebot reicht von der Kamera über Einbruchs-, Feuer-, Wasser- und Heizungssensoren sowie smarte Lampen bis hin zu Türschlössern, die per App-Fernsteuerung Zutritt zu den eigenen vier Wänden gewähren. Mittlerweile bauen sogar Versicherungen Prämienmodelle für Policen auf Basis dieser Sensorik auf.

Security by Design? Fehlanzeige!

Im Rahmen ihrer Zertifizierungspraxis müssen die IoT-Experten von AV-TEST allerdings immer wieder feststellen, dass die Sicherheit von IoT-Geräten stark zu wünschen übrig lässt. So entwickelt sich IoT-Technik immer schneller und dringt in immer weitere Bereiche unseres täglichen Lebens vor, ohne dass die Sicherheit der Geräte Schritt hält. Dabei erhöht das schon jetzt kaum überschaubare Spektrum eingesetzter Geräte die Zahl an Angriffsmöglichkeiten erheblich, denn bei der Entwicklung der meisten Geräte wird auf sichere und gut implementierte Verschlüsselungsverfahren und Web-Schnittstellen sowie sauber umgesetzte Autorisierungsverfahren und Anmeldeprozesse verzichtet.

Statt bereits bei der Entwicklung der internetbasierten Geräte auf deren Sicherheit im Netz zu achten, liegt der Fokus auf schneller Marktdurchdringung. Internetsicherheit ist bisher häufig nicht Teil des Produktdesigns, sondern wird oft als Hemmnis für schnelle Go-to-Market-Strategien empfunden. Das liegt auch daran, dass immer mehr IT-fremde Hersteller ohne Verständnis für Online-Gefahren Geräte produzieren, die mit dem Internet verbunden sind.

Augenöffner Mirai-Botnetz

Ein Augenöffner bezüglich der Unsicherheit im Internet der Dinge waren gegen Ende des letzten Jahres sicherlich die weltweit geführten Attacken des Mirai-Botnetzes. Von den Erkennungssystemen von AV-TEST im August 2016 erstmals erfasst, schossen Attacken der IoT-Malware im Oktober bereits große Onlinedienste in den USA und Europa aus dem Netz, indem sie deren Server mit Adressanfragen überlasteten. Für die DDoS-Angriffe wurde die über ein Botnet gesammelte Rechenleistung Hunderttausender gekaperter Router, Drucker, Webcams und Video-Recorder genutzt. Ende November fuhren Kriminelle mit anderen Varianten der gleichen Linux-Malware wuchtige Attacken gegen DSL-Router von Telekomkunden. 900.000 Geräte wurden schachmatt gesetzt. Im Oktober tauchte der Mirai-Code frei verfügbar im Internet auf. Seither ermittelten die AV-TEST Systeme eine zunehmende Zahl von Samples mit Spitzen Ende Oktober, November und Anfang Dezember.

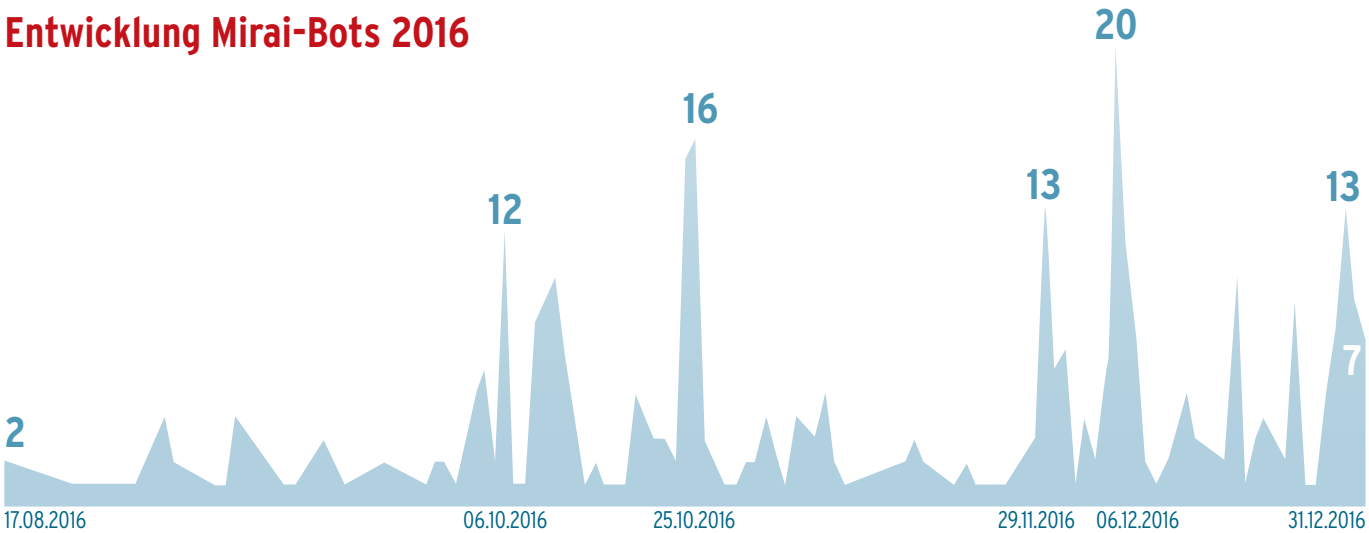
Aufgrund von Programmierfehlern konnte das Mirai-Botnetz bisher nicht seine volle Durchschlagskraft entwickeln. Es zeigt aber deutlich, wie hoch die Gefahr ist, die von ungeschützten Geräten im Netz ausgeht. Also von Geräten, die sich in privaten Wohnungen befinden oder etwa als Wearables sogar Einfluss auf die Gesundheit von Millionen Nutzern haben können.

IoT-Malware? Nichts Neues!

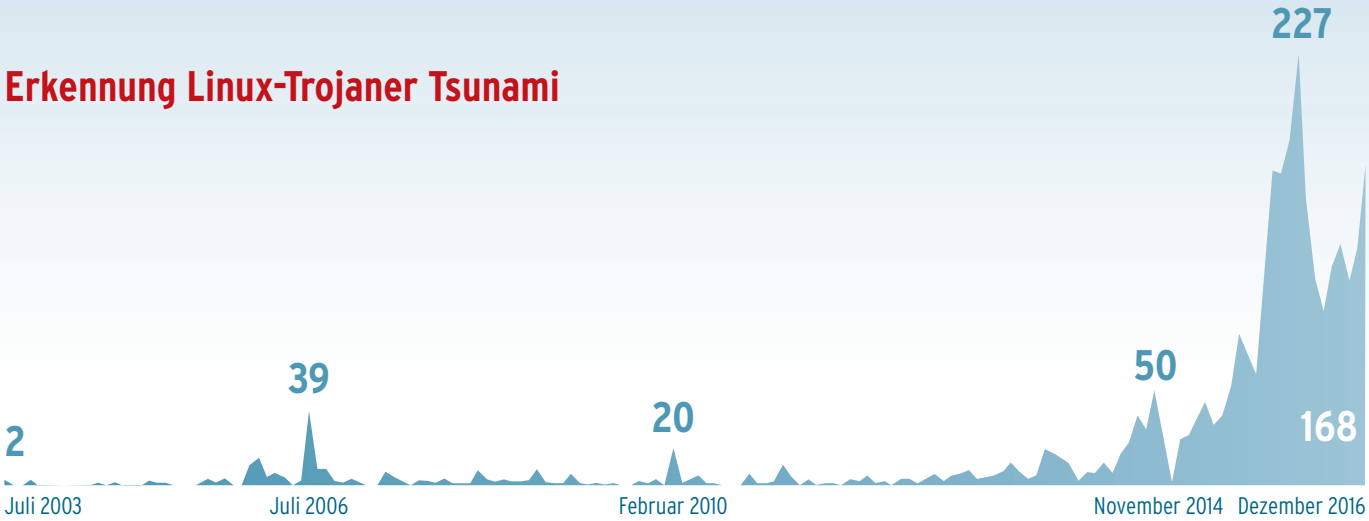
Ohne unnötig Angst zu schüren: Die Angriffe des Mirai-Botnetzes waren sicherlich erst der Beginn. Aufgrund von Programmierfehlern und der öffentlichkeitswirksamen Angriffsvariante DDoS waren die Schadprogramme dieses Typs verhältnismäßig leicht zu orten. Wirksamen Schutz gegen die Mirai-Infektionen bot jedoch so gut wie keines der IoT-Geräte. Denn weder ließen sich diese über Sicherheits-Updates und Patches nachträglich abdichten, noch besitzen sie ein in der Entwicklung eingeplantes Schutzkonzept gegen Malware-Infektionen. Und so stehen die von Mirai attackierten Geräte weiterhin auf der Abschussliste anderer IoT-Malware, die es bereits lange vor Mirai gab. Dazu gehören etwa die Schädlinge der Bashlite-Familie, die es 2016 ebenfalls auf unter Linux laufende IoT-Geräte abgesehen hatten.

Andere Linux-Malware, wie etwa die Backdoor Tsunami, treibt bereits seit einigen Jahren ihr Unwesen und kann von Kriminellen leicht für Angriffe auf IoT-Geräte modifiziert werden. Den Tsunami-Schadcode erfassten die Erkennungssysteme von AV-TEST erstmalig im Jahr 2003. Obwohl es zu diesem Zeitpunkt faktisch noch gar keine IoT-Geräte gab, beherrschte die Linux-Backdoor bereits Angriffsfunktionen, mit denen sie sich heute noch für quasi nicht abwehrbare Angriffe auf Router eignet: So kann Tsunami etwa weiteren Schadcode auf infizierte Geräte nachladen und Geräte so für Kriminelle fernsteuerbar machen. Doch auch für DDoS-Angriffe lässt sich die alte Malware nutzen. Ähnliche Angriffsmuster zeigen auch der seit 2013 bekannte Wurm Darlloz sowie viele andere Linux- und Unix-Schauprogramme, die AV-TEST seit Jahren erfasst und analysiert. IoT-Malware ist also alles andere als eine neue Bedrohung. Neu ist lediglich die ständig steigende Anzahl und massenhafte Verbreitung von IoT-Geräten, die ohne wirksamen Schutz online gehen.

Entwicklung Mirai-Bots 2016



Erkennung Linux-Trojaner Tsunami



Verbindung Mensch–Maschine

Menschen lassen einige dieser IoT-Geräte lassen sehr dicht an sich heran oder tragen sie sogar ständig am Körper: Denn nirgendwo ist die Akzeptanz von IoT aktuell höher als im Bereich Sport, Fitness und Gesundheit. Von der Arztsuche-App mit Pollenwarner für Allergiker über den Fitness-Tracker, der sich ein Online-Konto mit dem Blutdruckmesser und der Cardio-Waage teilt, bis hin zu Geräten, die medizinische Werte wie Blutzucker erfassen und online an den behandelnden Arzt weiterleiten. Laut einer aktuellen Studie des Digitalverbands Deutschland Bitkom e. V. nutzt mittlerweile jeder zweite Smartphone-Nutzer Gesundheits-Apps.

Statt ePrivacy Ausverkauf von Nutzerdaten

IoT-Geräte und angebundene Onlinedienste nehmen einen immer höheren Stellenwert ein. Und dank zunehmendem Komfort, etwa durch Sprachsteuerung wie Amazons Echo, Googles Home Assistent, Apples Siri und weiteren Systemen wird diese Technik zunehmend barrierefrei und für alle Generationen einfacher nutzbar. Allerdings fallen dabei auch viele bisher schützende Hürden, etwa wenn es um die Erfassung, Speicherung, Weitergabe und Nutzung von Daten geht. Wie Studien von AV-TEST ergaben, waren bei 80 Prozent der eHealth-Apps Datenschutzerklärungen entweder gar nicht vorhanden, nicht korrekt oder nicht verständlich. Und statt die Privatsphäre von Nutzern entsprechend der rechtlichen Regeln zu akzeptieren, versilbern Anbieter die Daten, die sie über ihre Apps mithilfe von Datenerfassungs-Werkzeugen und Tracking-Instrumenten von Drittanbietern aus der Werbeindustrie erfassen, an Werbenetzwerke. AV-TEST hat diese automatisierte Datenweiterleitung nachgewiesen.

Sicherheit als Feature und Wettbewerbsvorteil

Die Angriffe durch das Mirai-Botnet waren nicht die einzigen und werden nicht die einzigen bleiben. Darum empfiehlt das AV-TEST Institut, für IoT-Geräte und Services entsprechende Mindestsicherheitsstandards und Prüfmodelle als Basisschutz vorzuschreiben. Die vom AV-TEST Institut entwickelten Test- und Zertifizierungsverfahren setzen genau hier an: Sie prüfen grundlegende Kontrollen im Bereich Authentifizierung sowie die Gewähr sicherer Online-Schnittstellen, der sicheren und gesetzeskonformen Erfassung, Speicherung, Übertragung und Verarbeitung von Daten sowie des praktischen Datenschutzes. Dabei erweist sich etwa die Verschlüsselung bei der Datenübertragung zwischen Geräten, Apps sowie Cloud-Diensten als eine entscheidende Komponente. Die Sicherheit von IoT-Geräten und gut umgesetzter Schutz von Nutzerdaten wird ein zunehmender Wettbewerbsvorteil. Kunden erkennen sichere und datenschutzrechtlich unbedenkliche Geräte und Services am IoT-Zertifikat für Smart Home- und eHealth-Produkte.

AV TEST
av-test.org

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

Teststatistiken

Mit selbst entwickelten 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.

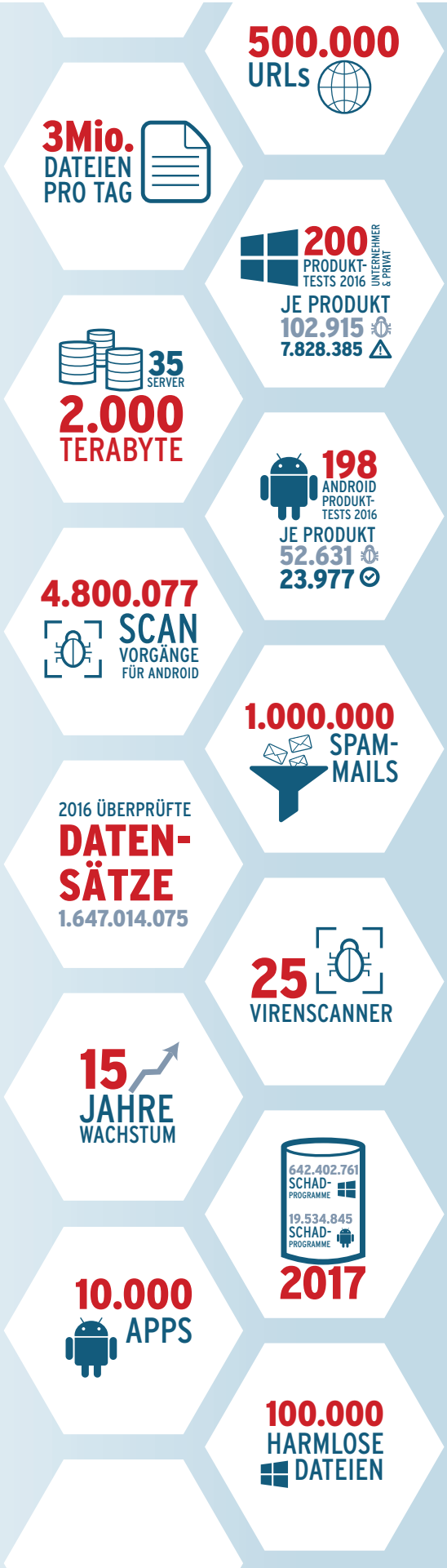
Millionen Malware-Samples für Ihre Sicherheit

Mehr als 3 Millionen Dateien scannt allein das System „VTEST Multiscanner" pro Tag. VTEST ist ein 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 ebenfalls automatisiert. So erweitert VTEST ständig eine der größten Datenbanken für Schadprogramme weltweit. Deren Datenbestand wächst seit über 15 Jahren kontinuierlich auf über 35 Servern mit einer Speicherkapazität von mehr als 2000 Terabyte. Zum Veröffentlichungsdatum dieses Jahresreports beinhaltete die AV-TEST Datenbank 642.402.761 Schadprogramme für Windows und 19.534.845 Schadprogramme für Android!

Zur gezielten Malware-Analyse bringt AV-TEST die Eigenentwicklung „Sunshine" zum Einsatz. Das Analysesystem ermöglicht das kontrollierte Ausführen potenziellen Schadcodes auf sauberen Testsystemen und erfasst 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 10.000 Android-Apps.

Die von den AV-TEST-Systemen erfassten Daten werden unter anderem für die monatlichen Tests von Sicherheitsprodukten für Windows eingesetzt. 2016 wurden so über 200 Produkttests allein für Privatanwender- und Unternehmensprodukte durchgeführt. Dabei wurden pro Produkt 102.915 Malware-Attacken gefahren sowie 7.828.385 einzelne Datensätze für Fehlalarmtests eingesetzt und ausgewertet. Im gesamten Jahr 2016 waren das 1.647.014.075 von den Testexperten zu überprüfende Datensätze. In den monatlichen Android-Tests überprüften die Tester über das Jahr insgesamt 198 Produkte. Dabei musste sich jede überprüfte Sicherheits-App gegen 52.631 spezielle Android-Schädlinge zur Wehr setzen. Zur Gegenprobe erfassten die Experten zudem über 23.977 Scans sicherer Apps pro Produkt, um die Anfälligkeit für Fehlalarme zu überprüfen. Im Labor wurden in Tests von Sicherheitsprodukten für Android also allein 4.800.077 Scan-Vorgänge analysiert und reproduzierbar ausgewertet.

Die besten Schutzlösungen zeichnet AV-TEST jedes Jahr mit den Awards des Instituts aus. Die prämierten Produkte setzen neue Standards in den Testbereichen Schutzwirkung, Geschwindigkeit, Benutzbarkeit und Reparaturleistung für Endanwender sowie Unternehmen.



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