ZAHLEN UND STATISTIKEN

SECURITY REPORT 2015/16

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

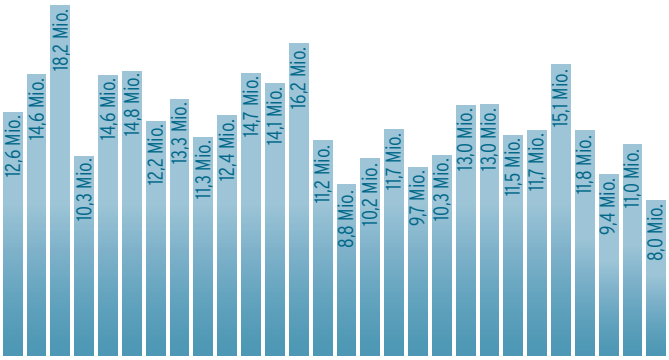
Der AV-TEST Sicherheitsreport

Cyber-Kriminelle denken unternehmerisch, und das müssen sie auch. Denn auch in ihrem Geschäft wird der Wettbewerb ständig härter. Unterm Strich muss sich der von ihnen betriebene Aufwand – von der Malware-Programmierung über deren Verteilung bis zur Monetarisierung – finanziell lohnen. Und selbst, wenn sie alle anderen Gesetze missachten, denen des Marktes müssen auch sie sich unterwerfen, wollen sie erfolgreich sein. Das bestätigen auch die Zahlen des diesjährigen Sicherheitsreports von AV-TEST.

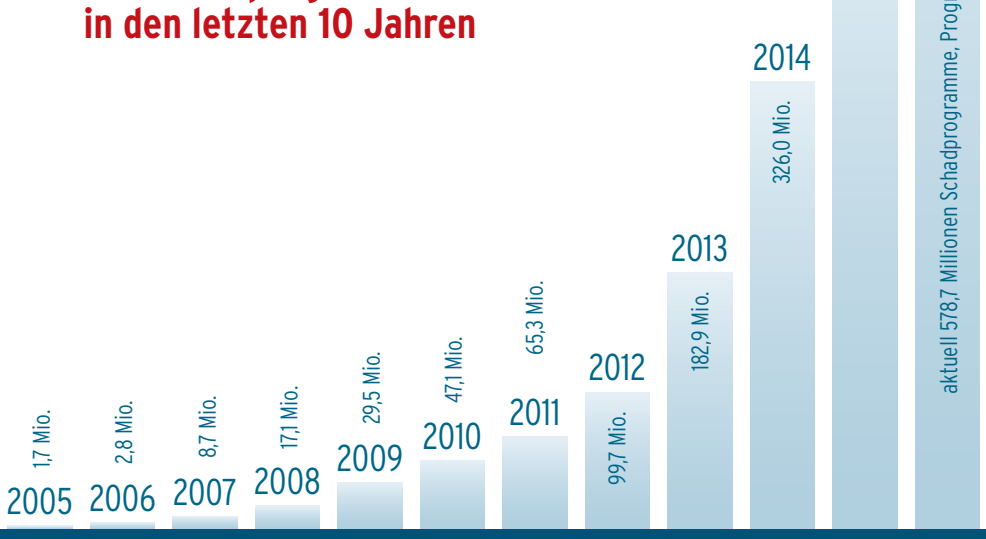
600 Millionen gegen Windows

So folgt die Entwicklung und Verbreitung von Schadprogrammen eindeutig ökonomischen Grundsätzen. Einer davon lautet: „Die Masse macht's." Dem Grundsatz folgend steigt die Anzahl der in Umlauf gebrachten Schadprogramme seit den ersten Messungen durch das AV-TEST Institut im Jahr 1984 beständig an. Bei Abschluss dieses Reports lag die Anzahl bekannter Schadprogramme für Windows-PCs in der AV-TEST-Datenbank bei 578.702.687, Tendenz stark steigend. Aktuell kommen jeden Monat etwa 12 Millionen neue Windows-Schädlinge „auf den Markt". Und so ist davon auszugehen, dass noch vor Ablauf dieses Jahres die Schallmauer von 600 Millionen Schadprogrammen für das Redmonder Betriebssystem durchbrochen wird.

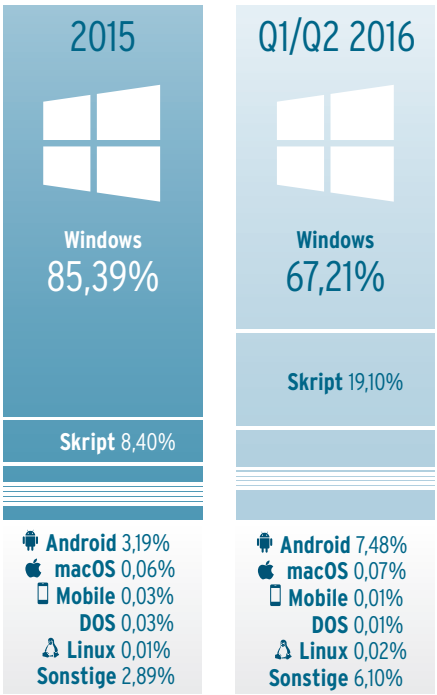
Auftreten neuer Malware insgesamt



Gesamtentwicklung von Schadprogrammen in den letzten 10 Jahren



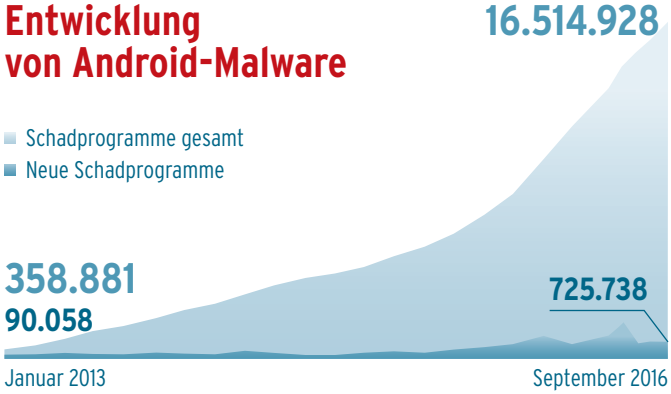
Malware-Erkennung nach Betriebssystem



Android zunehmend unter Feuer

Auch bei der Wahl des Angriffsziels folgen Kriminelle streng der ökonomischen Mengenlehre: Folglich zielten 2015 mit 85 Prozent die absolute Mehrheit der Schadprogramme auf das weltweit meistgenutzte Betriebssystem Windows. An zweiter Stelle, mit knapp über drei Prozent aber bereits weit abgeschlagen, rangiert die meistgenutzte Mobil-Plattform Android. Und mit gerade mal 0,06 Prozent belegten 2015 Betriebssysteme von Apple Platz drei der Beliebtheitsskala von Malware-Attacken. Selbstverständlich standen auch Linux sowie Betriebssysteme für Mobilgeräte unter Feuer. Der Anteil von Schadprogrammen für diese Plattformen war allerdings verschwindend gering – was jedoch keine Rückschlüsse auf die Gefährlichkeit der damit gefahrenen Angriffe zulässt.

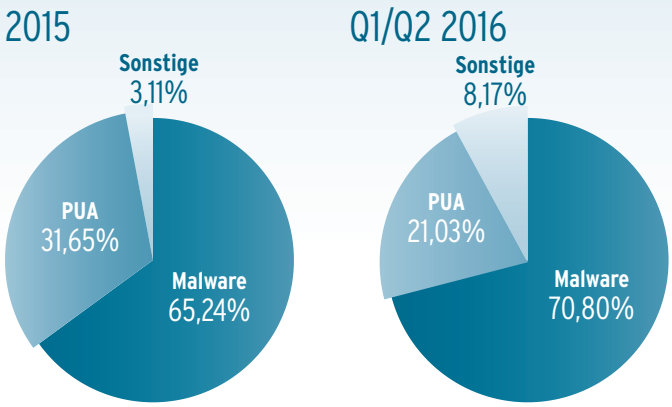
Entwicklung von Android-Malware



Trend 2016

Die Messwerte der AV-TEST-Erkennungssysteme zeigen im laufenden Jahr eine deutliche Entwicklung weg von Windows, hin zu Android. So verringert sich die Anzahl der Schädlinge für das Microsoft-System im Vergleich zum Vorjahr von 85 auf 67 Prozent. Android wird für Kriminelle dagegen deutlich attraktiver. Der Anstieg von 3 auf 7,4 Prozent klingt harmloser, als er tatsächlich ist, handelt es sich doch um eine Verdopplung der Malware-Zahlen. Und so erfassten die AV-TEST-Systeme Mitte Juni dieses Jahres bereits 12.998.160 Schadprogramme für Android. Allein im Vormonat Mai kamen knapp eine Million neuer schädlicher Anwendungen hinzu. Es ist also sicherlich ein Trend, der beobachtet werden sollte, denn offensichtlich weiten Kriminelle ihre Tätigkeit im Bereich Android massiv aus.

Schädlinge gesamt



PUA: Angriff der Industrie

Doch Schadprogramme waren 2015 nicht die einzige Bedrohung für Internetnutzer. Während Angriffe durch Malware eindeutig auf das Konto von Kriminellen gehen, droht steigende Gefahr für die Privatsphäre aus einer ganz anderen Ecke: Neben steigenden Schädlingszahlen stellte das AV-TEST Institut 2015 auch eine extreme Zunahme von PUA fest. Solche Potenziell Unerwünschten Anwendungen kommen oft Huckepack mit dem Download nützlicher Programme und Apps auf das Gerät. PUA wird seitens der Werbeindustrie eingesetzt, um etwa private Informationen wie das Nutzungs- und Bewegungsverhalten zu tracken und ungewollte, personalisierte Werbung einzublenden. Zudem agiert PUA meist verdeckt und ohne Zustimmung des Nutzers. Inwieweit solch industrielle Schnüffel-Tools durch Virenschutz-Programme als Malware identifiziert und geblockt werden sollen, ist nach wie vor arg umstritten. In den Erkennungssystemen von AV-TEST machte PUA 2015 knapp ein Drittel der Online-Gefahren aus. Da Angriffe auf die Privatsphäre von Nutzern auf allen Plattformen stark zunehmen, widmet AV-TEST der PUA-Entwicklung in diesem Sicherheitsreport ein eigenes Kapitel.

Trend 2016

In der ersten Hälfte dieses Jahres verzeichneten die AV-TEST-Systeme einen Rückgang von PUA. Lag die Erfassungsrate im Vorjahr noch bei 31 Prozent, sank sie bisher auf 20 Prozent. Allerdings handelt es sich dabei lediglich um einen Trend. Und da sowohl bei der Erkennung durch AV-Hersteller sowie bei der Selbstverpflichtung der Werbeindustrie bisher keine klare Linie erkennbar ist, wird AV-TEST weiterhin ein wachsames Auge auf die PUA-Verbreitung haben.

Sicherheitsstatus WINDOWS

Das Microsoft-Ökosystem verzeichnet mit Abstand die meisten Angriffe und höchsten Schädlingszahlen aller Betriebssysteme. Mehr dazu auf den folgenden Seiten.

Hauptangriffsziel Windows

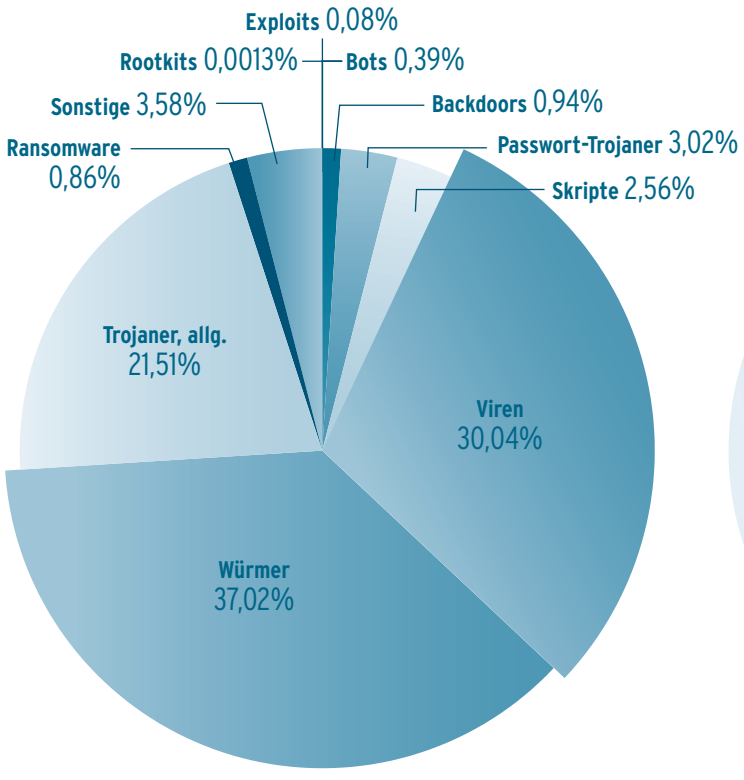
Als strategisches Ziel standen Windows-Systeme im Jahr 2015 nicht zuletzt wegen der hohen Verbreitung besonders im Fadenkreuz krimineller Angreifer. Dabei richteten sich mit 99,69 Prozent quasi alle durch die Erkennungssysteme von AV-TEST erfassten Attacken gegen die 32-Bit-Versionen des vielgenutzten Betriebsprogramms. Da Malware, die auf 32-Bit-Systemen funktioniert, auch 64-Bit-Versionen erfolgreich angreifen kann, ist spezielle 64-Bit-Malware eine absolute Seltenheit (0,31 Prozent).

Trend 2016

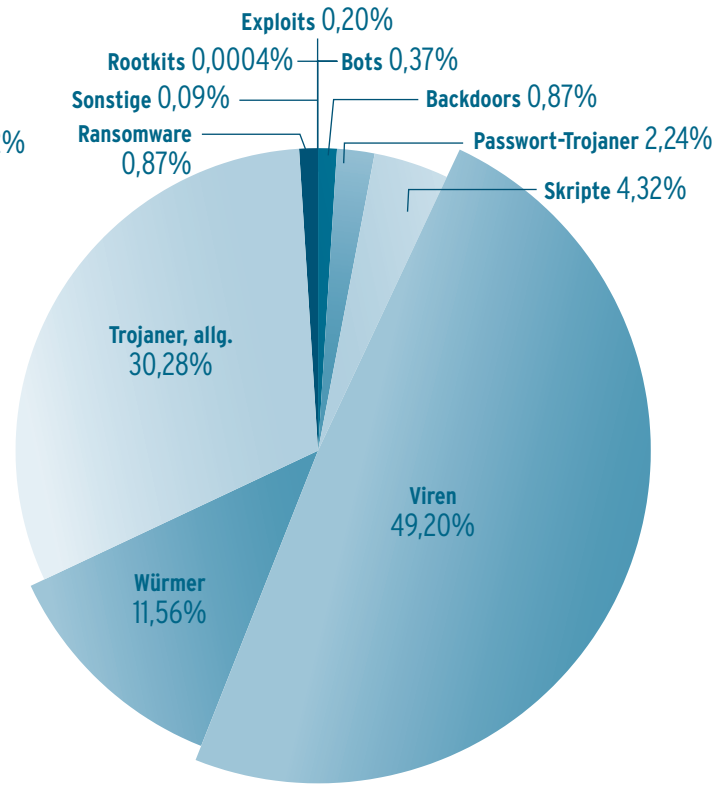
Auch die erste Jahreshälfte bestätigt diese Entwicklung: Windows bleibt nach wie vor Hauptangriffsziel, allerdings fast ausschließlich 32-Bit-Versionen (99,7 Prozent). Das Aufkommen spezieller 64-Bit-Windows Malware nimmt weiter ab.

Malware-Verteilung unter Windows

2015



Q1/Q2 2016



2015 war der Wurm drin

Bei Malware-Attacken auf Windows-Nutzer setzten kriminelle Angreifer 2015 besonders häufig Würmer ein. Über ein Drittel aller Malware-Erkennungen entfiel auf diese Schädlingsgattung. Würmer verbreiten sich selbst und entern PCs meist über infizierte Websites. Aber auch per Mail, P2P-Netzwerke, über Chat-Programme und sogar mittels Bluetooth-Verbindung können sie die Rechner ihrer Opfer kapern. Aufgrund ihres hohen Verbreitungspotentials wurden sie oft zum Infiltrieren großer Netzwerke eingesetzt, die sie im Anschluss mit beliebig nachladbarem Schadcode im Sinne der Angreifer nutzbar machten.

An zweiter und dritter Stelle folgten klassische Computer-Viren sowie das große Heer spezialisierter Trojaner, darunter Banking-Trojaner und die 2015 weit verbreitete Ransomware. Zusammen mit den Würmern machten diese Schädlingsgattungen bereits 92 Prozent der Gesamtzahl der Schadprogramme aus, die 2015 auf Internetnutzer lauerten. Mit Ausnahme schädlicher Skripte, mit denen Angreifer Websites so manipulierten, dass diese automatisch Schadcode-Attacken auf besuchende Windows-PCs durchführten (2,56 Prozent), blieben alle anderen Arten von Malware im Bereich von unter ein Prozent.

Trend 2016

Bis Mitte dieses Jahres sinkt die Zahl der für Angriffe eingesetzten Internetwürmer im Vergleich zum Vorjahr mit einer Entwicklung von über 37 auf knapp 11 Prozent merklich. Im Gegenzug steigt allerdings die Verbreitung klassischer Viren und Trojaner stark an. So nimmt allein die Virenverbreitung im Vergleich zum Vorjahr um 19 Prozent zu!

Top 10: Würmer und Ransomware mit Topwerten

In den Top 10 der meistverbreiteten Schadprogramme des Jahres 2015 sind somit ausschließlich Würmer, Viren und Trojaner zu finden.

Den unrühmlichen Platz 1 als weltweit aktivster Schädling 2015 belegt der Internetwurm „Allaple“. Dieser Schädling treibt bereits seit 2006 sein Unwesen: Über infizierte Websites kapert er PCs über ungepatchte Windows-Lücken und kann über einfache Brute-Force-Attacken sogar Angriffe auf Server mit schwachem Kennwortschutz fahren. Er gehört zu den polymorphen Schädlingen. Das bedeutet, dass er mit jeder zur Verbreitung selbst angelegten Kopie seinen Code verändert. Damit stellt er einfache Virenscanner auf eine harte Probe. Neben der Verbreitung von Schadcode hatte Allaple einst einen klaren Auftrag: Über infizierte Systeme führte er DoS-Attacken auf Websites estländischer Internetanbieter durch. Während der Programmierer des Schadcodes, ein 44-jähriger Este, bereits 2010 entlarvt, verurteilt und für 2,5 Jahren in Haft geschickt wurde, macht sein Wurm nach wie vor das Internet unsicher.

Auf Platz 2 der Top 10 der meist verbreiteten Schädlinge macht sich ebenfalls ein Internetwurm breit. Allerdings verbreitete sich „Sytro“ 2015 fast ausschließlich per E-Mail von infizierten Systemen. Und das geschah massenhaft, denn er verfügt über eine eigene SMTP-Engine. Der Mail-Wurm wurde zum ersten Mal Ende 2006 gesichtet.

„Virut“ und „Elkern“ auf den Plätzen 3 und 5 sind für Virenexperten ebenfalls alte Bekannte: Während sich der klassische HTML-Virus Virut bereits seit dem Jahr 2007 über infizierte Websites seinen Weg durch Browser-Lücken auf PCs bahnt, zerstört Elkern bereits seit 2001 Dateien auf infizierten Computern, die er über infizierte Datenpakete aus Onlinetauschbörsen gekapert hat.

Auf Platz 4 taucht mit „Ramnit“ ein Schädling auf, der zu Beginn 2010 erstmals auf dem Radar der Virenexperten der AV-TEST Labors erschien. Der Virus nutzt ganz verschiedene Wege, um sich per Internet zu verbreiten. Dazu gehören die Infektion per FTP-Download, Angriffe über infizierte Websites, portable Speichermedien, und auch in Kombination mit PUA kann er sich auf den Rechner schmuggeln. Seine Mission: die Jagd nach Einwahldaten für Online-Banking-Konten und nach Kreditkartendaten. Dabei überlässt der ausgefeilte Schädling fast nichts dem Zufall. Er durchsucht typische Programmordner und Speicherbereiche nach Kennwortdateien, überwacht

TOP 10 Windows-Malware 2015

1	ALLAPLE	17.315.842
2	SYTRO	5.318.628
3	VIRUT	4.898.268
4	RAMNIT	3.974.655
5	ELKERN	3.557.383
6	VIRLOCK	2.889.200
7	VB	2.007.596
8	AGENT	1.865.219
9	EXPIRO	1.768.984
10	VOBFUS	1.745.899

TOP 10 Windows-Malware Q1/Q2 2016

1	ALLAPLE	4.245.912
2	VIRUT	3.623.871
3	RAMNIT	2.976.489
4	VIRLOCK	1.534.457
5	AGENT	1.477.927
6	PARITE	1.147.433
7	SALITY	1.079.641
8	MIRA	882.365
9	LAMER	739.099
10	ZEGOST	616.975

Internetbesuche auf Banking-Portalen, um bei Überweisungsvorgängen Gelder über eine Man-in-the-Browser-Attacke abzuzweigen. Wird Ramnit fündig, schickt er die brisanten Informationen über eine heimlich aufgebaute Internetverbindung an seine Auftraggeber.

Mit „Virlock" ist auch eine Ransomware in den Top 10 der meistverbreiteten Schadprogramme 2015 vertreten. Dieser Verschlüsselungstrojaner ist der einzige Schädling der Top 10, dessen Geburtsstunde bzw. Ersterkennung in das Jahr 2015 fällt. Virlock gehört ebenfalls zu den polymorphen Schädlingen, und so erschwert auch sein sich ständig verändernder Code Schutzprogrammen die Jagd erheblich. Abgesehen davon gelten für Schutzprogramme bei der Erkennung von Ransomware ohnehin verschärfte Regeln: Bei Crypto-Schädlingen wie Virlock ist vor allem Schnelligkeit gefragt. Denn einmal auf einem infizierten System aktiv, beginnt der Schädling sofort mit der Verschlüsselung bestimmter Dateien und Ordner, darunter EXE-Dateien, Archivdateien, Audio-, Video- und Bilddateien sowie dem Ordner „Eigene Dateien". Je schneller ein Schutzprogramm reagiert, desto weniger Zeit bleibt dem Schädling, wichtige Dateien in Geiselhaft zu nehmen. Reagiert es zu langsam, ist der PC-Schutz möglicherweise selbst betroffen, denn Virlock verschlüsselt nicht nur EXE-Dateien, sondern auch Zertifikate.

Trend 2016

Das erste Halbjahr zeigt neben Platzwechseln einige Veränderungen der Malware Top 10. Außer Parite, einem ebenfalls ständig seinen Programmcode verändernden Virus, tauchen noch vier weitere neue Akteure in den Top 10 auf.

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

Hardware, auf der ein Apple-Betriebssystem läuft, gilt per se als sicher. Doch der Schein trügt. Zwar gibt es deutlich weniger Malware als für Windows, doch schutzbedürftig sind Mac-User dennoch.

Mac als Festung: eine Illusion

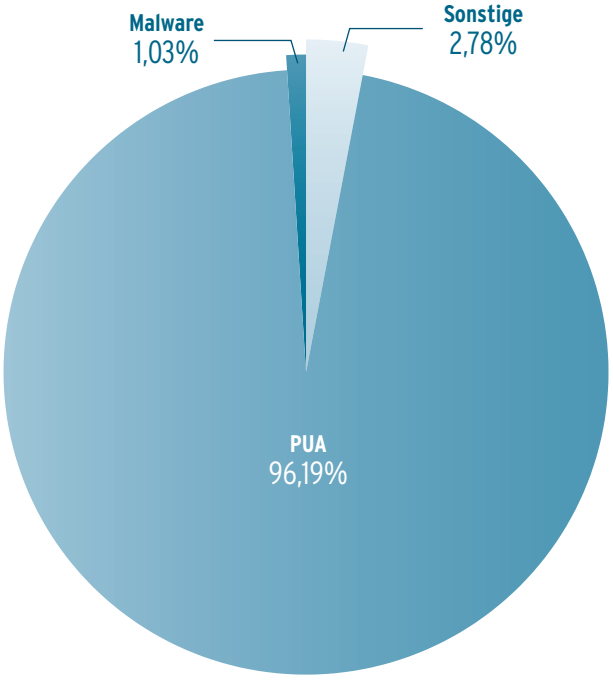
„Es ist eine ziemlich sichere Wette, dass Ihr Mac nicht mit einem Virus infiziert werden kann. Viel eher könnten andere sicherheitsrelevante oder technische Probleme auftauchen, die aber nichts mit Malware-Bedrohungen zu tun haben." Dieses offizielle Apple-Statement tragen viele Nutzer des Hard- und Software-Herstellers fast mantraartig vor, wenn Malware-Bedrohungen für Apple-Systeme zur Sprache kommen. Und so lautet das Fazit vieler Nutzer: Ich nutze Mac, Virenschutz brauche ich nicht. Dieses Motto gilt selbst dort, wo Macs im geschäftlichen Bereich eingesetzt werden, möglicherweise eine Fehleinschätzung.

Mac-Bedrohung: klein aber oho

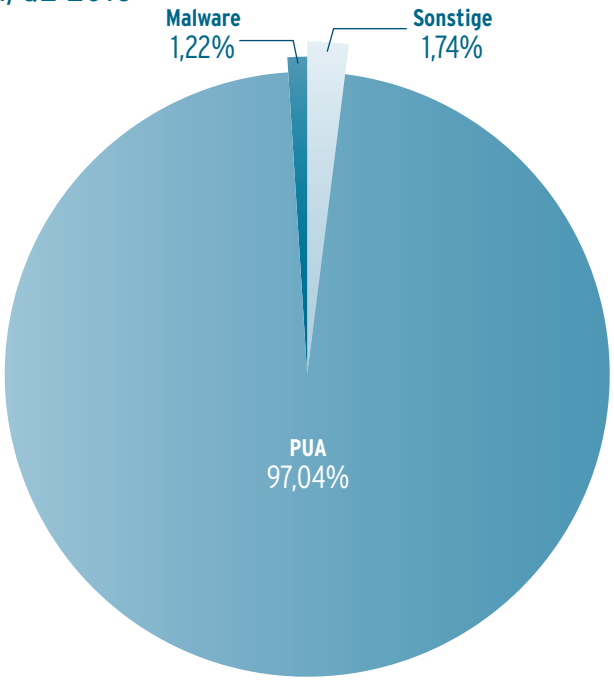
Tatsächlich ist die Anzahl der von den AV-TEST-Scansystemen identifizierten Schadprogramme für Apples Mac-Plattform im Vergleich zu Windows verschwindend gering. Gerade mal 819 Schädlinge hatten es 2015 auf Mac-Nutzer abgesehen. Doch wie bei Windows und Android sagen diese quantitativen Messwerte nichts über die Angriffsqualität der zum Einsatz gebrachten Schädlinge aus. Im Gegenteil lässt sich die These aufstellen, dass Angreifer keine Vielzahl an Malware programmieren müssen, um an wichtige Daten von Mac-Nutzern zu kommen, da diese ihre Rechner ohnehin so gut wie nie mit AV-Produkten schützen. Wie häufig Mac-Nutzer tatsächlich durch Malware attackiert werden, lässt sich nicht mit Sicherheit sagen.

Schädlinge macOS

2015



Q1/Q2 2016



Fakt ist allerdings, dass Apple die mutige Aussage, „ein Mac kann nicht infiziert werden“ spätestens bei der „Flashback-Infektionswelle“ im Jahr 2014 zurücknehmen musste. Damals kaperte der Trojaner Flashback etwa 600.000 Mac-Rechner über eine Java-Lücke des unangreifbar geglaubten macOS X und zwang sie als Sklavenrechner in ein Botnetz.

Für ältere, nicht gepatchte Mac-Versionen war Flashback 2015 immer noch eine Gefahr, wie die AV-TEST-Systeme zeigen: In den Top-Ten der Malware-Bedrohungen steht der Trojaner auf Platz 8.

Auf Platz 2 rangierte der Trojaner „Jahlav“, der sich im ersten Quartal dieses Jahres auf Platz 1 der Mac-Bedrohungen vorarbeitet. Der Schädling kann auf infizierten Macs beliebigen Schadcode aus dem Internet nachladen und im Hintergrund unbemerkt Prozesse starten. Jahlav kommt als Video-Codec per Download auf den Mac.

TOP 10 Mac-Malware 2015

1	AGENT	116
2	JAHLAV	89
3	GETSHELL	67
4	XCODEGHOST	65
5	MORCUT	63
6	MACNIST	52
7	YISPECTER	39
8	FLASHBACK	23
9	OPINIONSPY	18
10	TUNEUPMYMAC	16

Trend 2016

Auch in diesem Jahr sind keine überbordenden Angriffswellen auf Mac-Rechner zu erwarten. Fakt ist allerdings das Vorhandensein von Malware für macOS und somit die Notwendigkeit von Virenschutz-Maßnahmen.

TOP 10 Mac-Malware Q1/Q2 2016

1	JAHLAV	102
2	XCODEGHOST	84
3	GETSHELL	60
4	MALWARE	28
5	TINYV	23
6	ACEDECEIVER	20
7	WIRENET	18
8	KERANGER	17
9	OCEANLOTUS	14
10	FLASHBACK	13

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/ MOBILE

Wer über Bedrohungen für Smartphones und Tablets spricht, spricht auch automatisch über Android. Googles Betriebssystem lässt sich für Kriminelle am effektivsten ausnutzen.

Marktbedeutung weckt Interesse

Wie bereits gezeigt, zielen 85 Prozent der Schadprogramme auf die Betriebsplattform Windows ab. Das heißt allerdings keinesfalls, dass Nutzer anderer Betriebssysteme sich keine Gedanken um die Sicherheit ihrer Daten machen müssten. Einerseits mag der Prozentsatz am Gesamtaufkommen von Malware mit knapp über drei Prozent für Android auf den ersten Blick verschwindend gering erscheinen. Andererseits erfassten die AV-TEST Systeme für die meistgenutzte Mobilplattform Android bei Erstellung dieses Reports fast 17 Millionen Schadprogramme. Dabei begannen Kriminelle die Entwicklung von Malware für das quelloffene Google-System erst im Jahr 2013 recht zögerlich mit ein paar infizierten Apps. Anfangs begnügten sie sich damit, über versteckte Einwahlprogramme (Dialer) Kleinstbeträge abzugreifen.

Schädlinge Android versus Mobil

Android 2015
99,18%

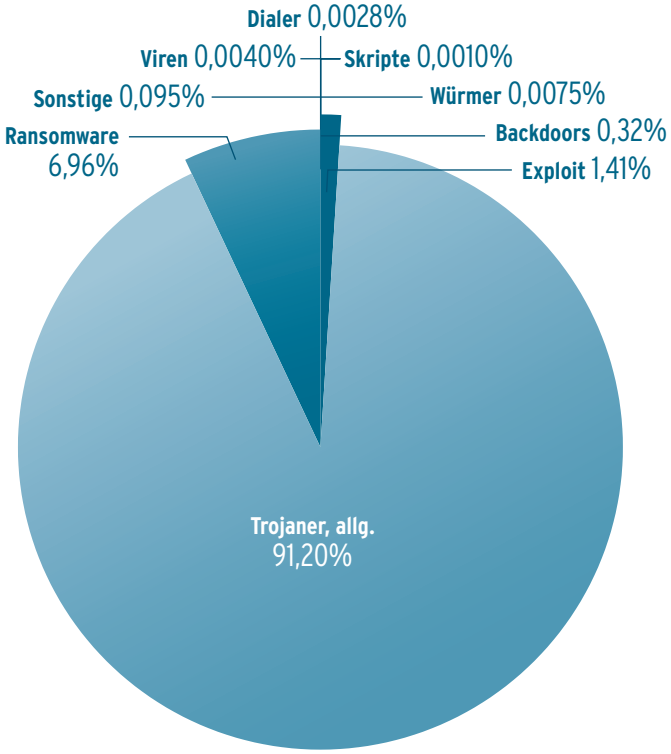
Android Q1/Q2 2016
99,87%

Mobile 2015
0,82%

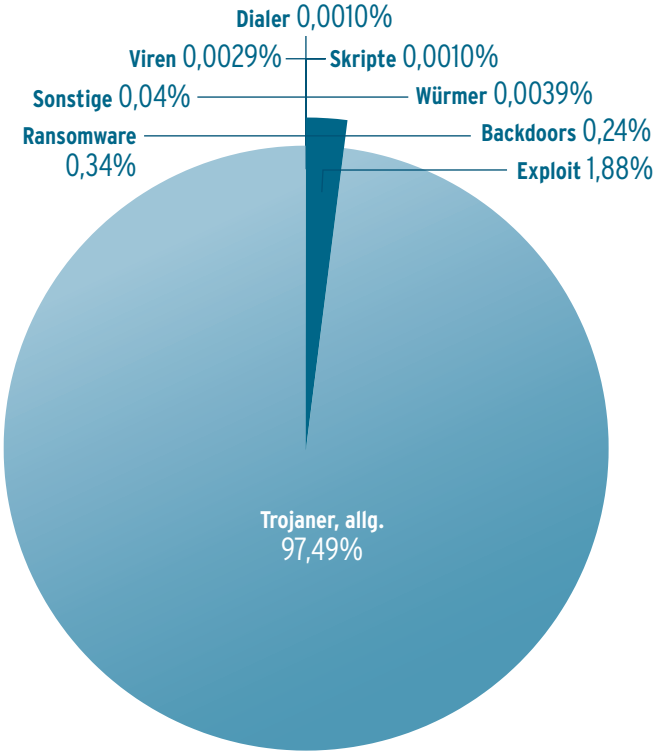
Mobile Q1/Q2 2016
0,13%

Malware-Verteilung Android

2015

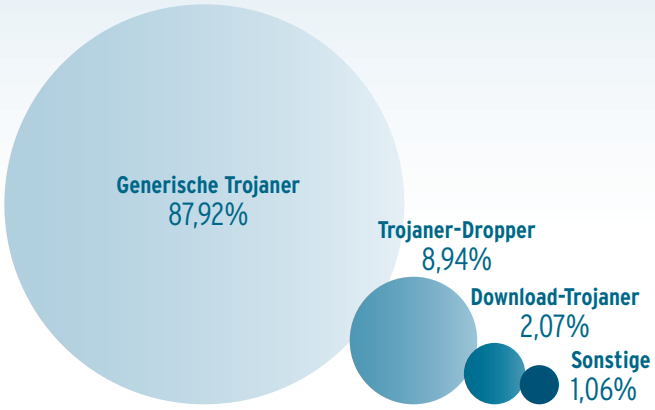


Q1/Q2 2016



Doch mit der wachsenden Verbreitung und dem steigenden Absatz von Smartphones, Tablets und anderen Android-Geräten, rückte die Plattform immer stärker in den Missbrauchsfokus. Und mit zunehmenden Einsatzmöglichkeiten über ein entsprechendes App-Angebot wurden auch die Möglichkeiten von Malware angepasst. Insofern kann die Marktsituation als geklärt betrachtet werden: Aktuell haben über 99 Prozent aller Schadprogramme, die auf Mobilsysteme zielen, Android-Geräte im Visier. Andere Plattformen sind derzeit für Cyberkriminelle entweder wegen zu geringer Marktbedeutung uninteressant oder aufgrund einer geschlossenen App-Infrastruktur nur mit übermäßigen Aufwand auszubeuten. Darum spielt die Malware-Situation dieser Systeme hier keine Rolle.

Trojaner-Verteilung Android 2015



Trend 2016

Die AV-TEST-Messungen des ersten Halbjahres 2016 untermauern die 2015er-Messungen: Auch 2016 sind Mobilsystemen wie iOS und Windows Mobile für Cyberkriminelle weniger interessant, da Android für sie effizienter auszunutzen ist.

Trojaner-Attacken auf Android

Versuchten Kriminelle in der Anfangsphase von Android noch mit Dialern ihr Glück, ist deren Stern längst gesunken. Von den über 2 Millionen Android-Schädlingen, die die AV-TEST-Systeme 2015 enttarnten, war der Anteil von Dialern mit gerade mal 58 Schädlingen nur noch verschwindend gering. Doch das gibt wenig Grund zur Freude, denn betrachtet man die Aufteilung von Android-Malware genauer, zeigt sich neben der schieren Masse vor allem die „Innovationsgeschwindigkeit" der Cyberkriminellen: Obwohl die ersten, simpel gestrickten Malware-Samples für Android erst seit 2013 nachweisbar sind, erfassten die AV-TEST-Systeme gerade mal vier Jahre später das volle Spektrum derzeit möglicher Schadcodes. Zu den Dialern haben sich in kürzester Zeit Viren, Würmer, schädliche Skripte, Backdoors und Trojaner gesellt. Somit entwickelt sich die Malware-Situation für Android-Geräte zunehmend in die Richtung von Windows-PCs. Das verwundert nicht, denn quasi jede Anwendung, von E-Mail bis zum Online-Banking, die noch vor einigen Jahren mit dem PC erledigt werden musste, funktioniert jetzt bequem von unterwegs über entsprechende Apps. Und während sich bei Windows-Nutzern längst die Erkenntnis durchgesetzt hat, dass ein PC einen Virenschutz braucht, ist der Einsatz entsprechender Schutz-Apps auf Android-Mobilgeräten längst nicht so verbreitet. In Kombination mit der oft unzureichenden und langwierigen Patch-Reaktion der Hersteller auf bekannte Sicherheitslecks wird Android für Kriminelle so zum optimalen Ziel.

Der Einsatz spezialisierter Trojaner scheint für Kriminelle aktuell besonders lukrativ zu sein. Denn mit fast 1,9 Millionen erfassten Exemplaren stellt diese Schädlingsgattung (91,2 Prozent) die Hauptbedrohung für Android-Nutzer dar. Selbst wenn generische Trojaner mit 87,9 Prozent 2015 den größten Anteil in dieser Schädlingsgruppe stellen, lohnt sich auch hier ein Blick auf das bereits vorhandene Spektrum der Code-Entwicklung: Denn auch hier sind – zumindest grundlegend – innerhalb kürzester Zeit alle Schadfunktionen verfügbar, die es auch für Windows gibt. So war etwa die Anzahl von Verschlüsselungstrojanern in 2015 mit 144.008 Exemplaren noch verhältnismäßig gering. Dennoch gilt es festzuhalten, dass Kriminelle in kürzester Zeit einen Weg gefunden haben, das auf Windows offenbar gut funktionierende Erpressungsmodell in kürzester Zeit auf die Android-Plattform zu übertragen. Gleiches gilt für kriminelle Eingriffe per Trojaner in mobiles Online-Banking: Obwohl längst nicht alle Banken über eine App verfügen, die Android-Nutzern Kontoverfügung erlaubt, werden die vorhandenen Apps bereits von 20.051 auf Online-Banking spezialisierten Android-Trojanern attackiert. Auch diese stellen mit einem Prozentanteil knapp über ein Prozent noch einen verschwindend geringen Teil der Gesamtbedrohung. Mit zunehmender Nutzerakzeptanz des Mobile Bankings wird sich deren Anzahl aber mit großer Sicherheit schnell erhöhen.

Top 5 Android-Malware

Auf dem ersten Platz der meistverbreiteten Schadprogramme stand 2015 „Agent". Der Android-Trojaner ist nicht nur wegen seiner weiten Verbreitung bemerkenswert. Denn im Unterschied zu vielen anderen Schadprogrammen, die über infizierte Apps auf Android-Geräte kommen und damit von deren Nutzern selbst irrtümlich installiert werden müssen, beherrscht diese Malware eine zusätzliche Verbreitungstaktik: Ähnlich einem Windows-Schädling kann Agent ungeschützte Geräte seiner Opfer beim Besuch infizierter Webseiten kapern. Allerdings verbreitet er sich ebenfalls hauptsächlich über infizierte Apps. Einmal auf dem Gerät, kann der Trojaner andere Malware nachladen oder bietet Angreifern die Möglichkeit, die Sicherheitseinstellungen des infizierten Geräts aus der Ferne herabzusetzen, und ermöglicht so den Diebstahl privater Informationen.

Mit „TrojanSMS" befand sich 2015 dagegen ein echter Klassiker mobiler Schädlingsprogrammierung auf Platz 2 der Top 5 für Android-Malware. Wer sich einen Schädling dieser Trojaner-Familie über die Installation einer Fake-App einfing, drohte vornehmlich auf zwei unterschiedliche Arten von Angreifern abgezockt zu werden: Zum einen verursachten Exemplare dieser Gattung erhebliche Kosten durch die heimliche Nutzung kostenpflichtiger SMS-Dienste. Zum anderen konnte der Zugriff auf die SMS-Funktion durch den Schädling aber noch weitreichendere Folgen nach sich ziehen. Denn der Trojaner hatte es ebenfalls auf per SMS eingehende M-TANs für Online-Banking-Sitzungen abgesehen.

Wie schon TrojanSMS sind die folgenden Android-Schädlinge der Top 5 darauf angewiesen, dass Nutzern in der quasi unüberschaubaren Masse an Apps ein Verwechslungsfehler unterläuft. So tarnte sich der Trojaner „FakeInst" als vermeintliche Virenschutzlösung und der Trojaner „Opfake" gab sich den Anstrich einer Mini-Version des beliebten Opera-Browsers. All diesen Schädlingen ist gemein, dass sie die SMS-Funktionen gekaperter Geräte missbrauchen und darüber hinaus weiteren Schadcode nachladen können.

TOP 5 Android-Malware 2015

1	AGENT	679.480
2	TROJANSMS	225.847
3	FAKEINST	188.211
4	OPFAKE	182.247
5	INOCO	114.264

TOP 5 Android-Malware Q1/Q2 2016

1	AGENT	971.442
2	FAKEINST	104.437
3	SHEDUN	98.870
4	OPFAKE	92.030
5	SMSSPY	70.686

Trend 2016

Mit „Shedun" (Platz 3) betritt ein neuer, mächtiger Schädling die Bühne der Android-Top 5. Seinen hohen Verbreitungsgrad verdankt er der schieren Masse an Fake-Apps, über die er auf Android-Geräte kommt. In knapp 20.000 gefälschten Apps – darunter Facebook, Twitter, Snapchat oder WhatsApp – versteckt sich die Malware, die aus Dritt-App-Stores geladen wird. Infizierte Geräte werden im Hintergrund gerootet und unter anderem mit Werbung geflutet.

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

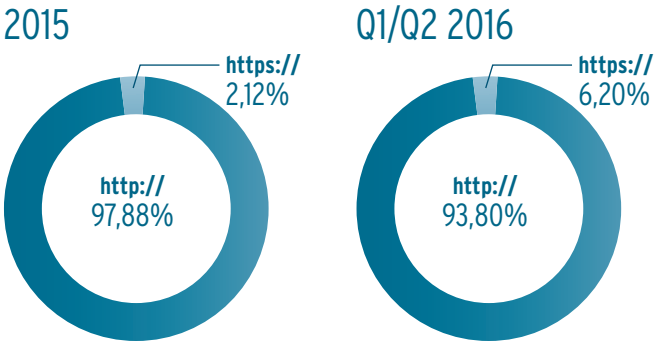
Um Malware zu verbreiten, ist das Internet für Kriminelle der effektivste Weg. Warum erklären die Zahlen aus den AV-TEST-Labors.

HTTP als Einfallstor

Als „Web Threats" erfassen und listen die AV-TEST-Analysesysteme mit „Blackhat SEO" und „Webdust PE URL" Gefahren, die aktuell auf Internetnutzer lauern. Dazu gehören insbesondere mit Malware infizierte Websites. Schon beim bloßen Aufruf solch verseuchter Online-Angebote versuchen Schadprogramme, Besucher-PCs über Software-Schwachstellen zu kapern. Für solche Drive-by-Downloads erstellen Kriminelle eigene Websites, die sie über groß angelegte Spam-Kampagnen bewerben. Doch auch bekannte und viel genutzte Online-Angebote werden zur Malware-Verbreitung gehackt und infiziert. Wie die Erkennungssysteme von AV-TEST zeigen, nutzten Angreifer 2015 fast ausschließlich Websites mit dem ungeschützten Übertragungsprotokoll HTTP zur Verteilung von Malware (97,88 Prozent). Angriffe über HTTPS-Seiten kamen dagegen so gut wie gar nicht vor (2,12 Prozent).

Die Rangliste der meistgenutzten Domains zur Verteilung von Schadprogrammen wurde im letzten Jahr klar von der Top Level Domain „COM" angeführt, was wenig verwundert. Sie ist mit Abstand die verbreitetste Domain und für jedermann leicht und schnell zu registrieren. Auf Platz 2 der Top 10 gefährlicher Websites rangierte die russische Domain „RU" und auch die Sowjetunion (SU) lebte im Bereich Cybercrime mit Platz 4 wieder auf. Auch für die Domain „ORG" interessierten sich Angreifer 2015, weil sie von den meisten freien Software-Projekten und Open-Source-Anbietern genutzt wird. Auffällig ist, dass sofort danach europäische Länderkennungen folgen. Länder mit gut ausgebautem Datennetz und vielen Online-Nutzern wie Russland, Italien, Deutschland und Polen standen bei Angreifern 2015 darum hoch im Kurs.

Malware-Verteilung über verschlüsselte und unverschlüsselte Internetseiten



Trend 2016

In der ersten Hälfte von 2016 verdreifachte sich die Zahl der Angriffe auf HTTPS-Seiten auf 6,2 Prozent. Für die Domain-Rangliste zeigen die aktuellen Messwerte der AV-TEST-Systeme eine geografische Verschiebung in Richtung Nordamerika beziehungsweise in den englischen Sprachraum. So erobern US-Seiten Platz 7 der Malware-URLs. Dafür verschwinden bis auf Deutschland alle europäischen Seiten aus den Top 10. Deutschland fällt von Platz 6 auf Platz 8.

TOP 10 Malware-Domains 2015

1	COM	47,68%
2	RU	13,15%
3	SU	10,06%
4	NET	5,89%
5	ORG	3,97%
6	TR	1,90%
7	IT	1,16%
8	DE	1,15%
9	PL	0,89%
10	INFO	0,71%

TOP 10 File Extensions Malware 2015

1	EXE	37,90%
2	HTML	35,12%
3	ZIP	11,08%
4	RAR	5,80%
5	PHP	4,03%
6	SWF	2,32%
7	ASP	1,67%
8	HTM	1,28%
9	PDF	0,22%
10	ASPX	0,15%

Gefährliche „EXE“

Die Rangliste der Dateiformate, die am häufigsten zur Verbreitung von Schadprogrammen genutzt werden, führten 2015 klar die ausführbaren Dateien „EXE“ an. Der Anteil der über dieses Format verbreiteten Schadprogramme lag deutlich über dem der folgenden HTML- und ZIP-Formate. Ein weiteres Datenkompressionsformat taucht auf Platz 5 der Top 10 der gefährlichsten Dateiformate auf: RAR. Weiterhin standen zur Malware-Verbreitung 2015 klassische Online-Formate hoch im Kurs: PHP, HTM und Co. wurden von Angreifern häufig genutzt, um Schädlinge in Websites einzubetten. Angriffe über infizierte ASP-Dateien zielten oft auf Opfer, denen vorgegaukelt wurde, sie müssten Flash Player-Updates einspielen. Auf das PDF-Format griffen Kriminelle im letzten Jahr ebenfalls gern zurück, da es sich, wie auch die Kompressionsformate, sowohl für den Mail-Versand von Schädlingen als auch für Infektionen per Download eignet.

Trend 2016

Für die erste Hälfte dieses Jahres zeigen die Analysesysteme von AV-TEST vor allem an der Spitze der Top 10 Veränderungen: Kriminelle setzen zur Malware-Verbreitung zwar weiterhin oft das EXE-Format ein, doch deutlich häufiger nutzen sie HTML-Formate. Diese überholen in der erste Hälfte des Jahres die ausführbaren Dateien und verdrängen sie auf Platz 2 der Top 10.

AV-TEST av-test.org

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 PUA

Die Anzahl der von den AV-TEST-Systemen erfassten Potenziell Unerwünschten Anwendungen (PUA) nimmt nicht nur stetig zu, sie bedroht mittlerweile auch die Privatsphäre der Nutzer aller gängigen Plattformen.

Windows-Nutzer größtes PUA-Ziel

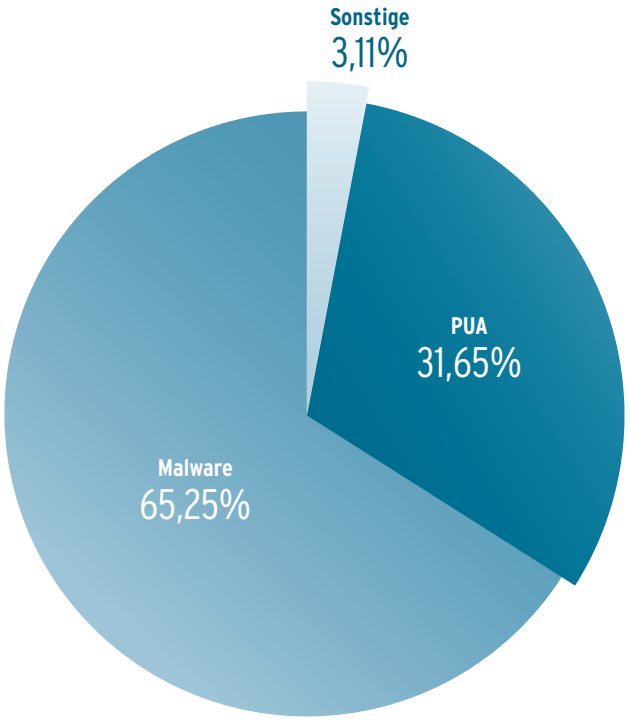
Mit mehr als 37 von über 40 Millionen PUA-Erkennungen im Jahr 2015 gerieten vor allem Windows-Nutzer unter die Kontrolle der Werbeindustrie (94 Prozent aller Erkennungen). Doch auch auf allen anderen Software- und Mobil-Plattformen zielten Spionageprogramme auf Surfdaten und andere Privatinformationen von Online-Nutzern. Selbst für Linux wurden 412 Samples erfasst. Und während die Malware-Zahlen für Mac-Rechner mit 819 Samples im Jahr 2015 recht übersichtlich waren, sah es im Bereich PUA schon ganz anders aus: Über 76.000 Samples machten Jagd auf die Online- und Nutzungsgewohnheiten von Internetnutzern mit Mac.

Windows bleibt Hauptangriffsziel

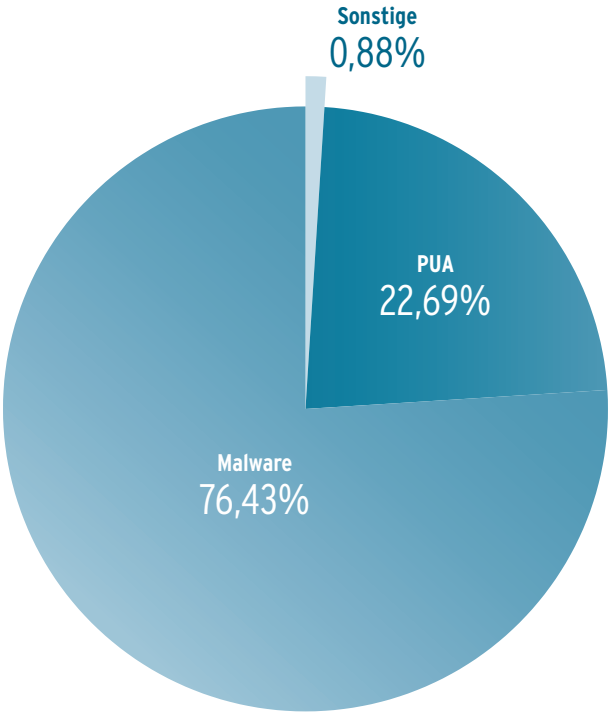
Das lag allerdings mit Sicherheit nicht an der 2015 meist eingesetzten Spionage-Software „Multiplug", wie die PUA-Top 10 beweisen. Platz 1 der Top 10 protokolliert das Surfverhalten von infizierten PCs und verschickt entsprechende Profile heimlich per Internet an Werbefirmen. Im Anschluss ist es denen dann möglich, Webseiten im Browser gezielt zu modifizieren sowie zusätzliche Webseiten mit entsprechend angepasster Werbung einzublenden (Pop-ups). Multiplug kommt meist im Bundle mit Gratis-Tools über Freeware-Plattformen auf die Rechner.

PUA-Erkennung gesamt

2015



Q1/Q2 2016



TOP 10 Windows-PUA 2015

1	MULTIPLUG	7.655.388
2	BROWSEFOX	4.269.061
3	SOFTPULSE	3.845.293
4	OUTBROWSE	2.463.053
5	INSTALLCORE	1.466.608
6	MORSTAR	1.460.919
7	LINKURY	1.337.107
8	LOADMONEY	1.246.415
9	SOLIMBA	738.053
10	AMONETIZE	601.900

TOP 10 Windows-PUA Q1/Q2 2016

1	BROWSEFOX	2.149.379
2	OUTBROWSE	1.117.703
3	INSTALLCORE	761.292
4	ICLOADER	455.582
5	DOWNLOADGUIDE	303.663
6	LOADMONEY	284.867
7	LINKURY	226.756
8	TOOLBAR	222.771
9	ADLOAD	205.302
10	SOFTPULSE	201.883

Auch der zweitplatzierte „Browsefox" kommt heimlich im Verbund mit Gratis-Download-Freeware auf den PC. Die Adware installiert Add-Ons in Microsofts Internet Explorer, Mozilla Firefox sowie Google Chrome und verändert die Startseite der Browser und deren Suchmaschinenanbindung. Zusätzlich zeigt der Schädling personalisierte Werbung auf besuchten Webseiten an und öffnet Reklame-Pop-Ups.

Alle anderen Vertreter der PUA-Top 10 arbeiten beim Ausspionieren des Nutzerverhaltens und der Surfgewohnheiten nach ähnlichen Mustern und werden durch die AV-TEST-Systeme entsprechend erfasst.

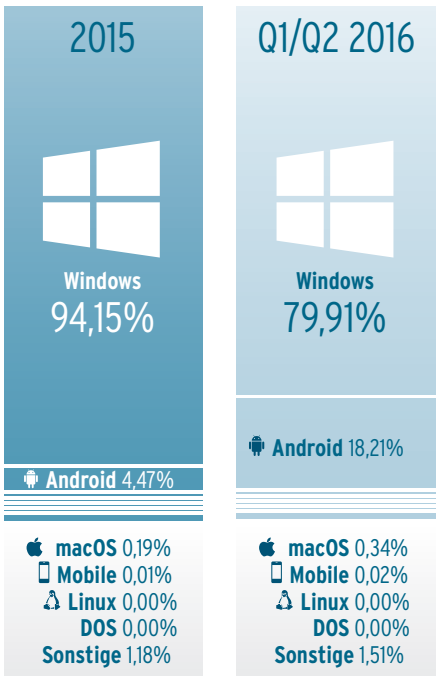
Spionageziel Android verstärkt im Visier

Wie bereits festgestellt, steigt die Anzahl der von AV-TEST gemessenen PUA-Samples für Android von 2015 auf 2016 dramatisch an. Allerdings ist die Frage, was eigentlich genau unter den Begriff „potenziell unerwünscht" fällt, auch hier noch nicht abschließend geklärt. Zum einen, weil es sich um eine rechtliche Grauzone handelt und sich Anbieter von Schutz-Apps mit der PUA-Erkennung nicht unnötig in die Schusslinie eines Heeres von Anwälten der Werbeindustrie stellen wollen. Zum anderen, weil sich die zum Teil sehr aggressiven PUA-Versionen oft kaum von klassischer Malware unterscheiden. So zeigt die Analyse einiger PUA-Samples etwa in puncto Ausspähen von Nutzerdaten fast ähnliche Mechanismen wie die klar der Malware zugeordneten Trojaner. Auch bezüglich der Verbreitung von PUA sind die Übergänge zur Malware fließend. So wird Mobile Malware ebenso über infizierte Apps verbreitet, wie PUA als Bundle mit eigentlich nützlichen Apps auf die Geräte bespitzelter Smartphone- und Tablet-Nutzer kommt. Die Erkennung von PUA wird natürlich zusätzlich dadurch erschwert, dass sich auch quasi jede gutartige Gratis-App über das Ausspielen von Werbung finanziert.

Selbstverständlich weist PUA für Android und Mobilgeräte weiterer Mobilplattformen andere Spezifikationen auf als für Windows-PCs. PUA für Mobilgeräte bringt personalisierte Werbung innerhalb vordefinierter Werbefenster einer App oder zeigt kurzeitig displayfüllende Werbung bei Start oder Beenden einer App (Interstitial Ads). Doch auch die Push-Benachrichtigungen von Geräten oder der Home-Screen können als Werbefläche missbraucht werden (Icon Ads).

Hinzu kommt, dass PUA für Mobilgeräte skrupellosen Werbern auch Informationen über Bewegungsmuster von Gerätenutzern liefert und entsprechende Profile für ortsgebundene Werbung erstellen kann. Dass solche Bewegungsdaten ein von Werbern extrem begehrter Rohstoff sind, verdeutlichen folgende Vergleichszahlen für alle mobilen Plattformen außer Android: Zwar sind iOS, Windows Mobile und Symbian mit gerade mal 0,01 Prozent des PUA-Gesamtaufkommens quasi nicht existent, allerdings verdoppelt sich die Anzahl der Samples im ersten Halbjahr 2016 im Vergleich zu 2015. Deutlich interessanter ist jedoch, dass die Menge von PUA-Samples für Android im Jahresvergleich sprunghaft ansteigt – und zwar um über 13 Prozent. Sicherheits-Software für Android ist aktuell noch wenig verbreitet. Somit sind Android-Nutzer leichte Beute für die Werbeindustrie.

PUA-Erkennung nach Betriebssystem



Mac: statt Malware Spionage

Dass Malware für Apple-Systeme nicht massenhaft gestreut wird, wurde in diesem Report bereits dargelegt. Anders sieht es dagegen bei Verletzungen der Privatsphäre von Mac-Nutzern durch PUA aus. Während die AV-TEST-Systeme 2015 gerade mal 819 unterschiedliche Malware-Samples registrierten, lag die Anzahl von PUA-Samples mit 76.464 deutlich höher und machte über 96 Prozent der Gesamterkennungsrate von Mac-Angriffen aus.

Die PUA-Top 10 des letzten Jahres dominierte die Adware „VSearch". Sie kommt im Bundle mit beliebten Freeware-Downloads auf ungeschützte Mac-Rechner nichtsahnender Nutzer. Im Stile eines Trojaners nistet sich die Adware über ein Shell-Skript im Speicher ein und schickt heimlich System- und Nutzerdaten über das Internet. Zudem kapert sie die Browser-Einstellungen, verändert etwa die Startseite und blendet Pop-up-Werbung ein.

Mit hoher Verbreitung belegt „Macnist" Platz 2. Dabei handelt es sich um eine trojaner-ähnliche Adware die Mitte letzten Jahres als Browser-Erweiterung für Safari, Chrome und Firefox auftauchte. Auf besuchten Websites blendete die auch als „Yontoo" bezeichnete Spionage-Software eigene Werbeanzeigen ein und schickte Protokolle des Surfverhaltens an unbekannte Server im Internet. Mac-Rechner enterte der Schädling als vermeintliches Plug-in zur Wiedergabe von Online-Spielfilmen getarnt, war aber auch als Medienabspiel-Software oder Download-Beschleuniger zu finden.

Es bleibt festzuhalten, dass sich der Einsatz eines Schutzprogramms auch für Mac-Nutzer lohnt. Wer seine Privatsphäre geschützt sehen will, sollte darum zu einem AV-Produkt greifen, das auch PUA erkennt und blockt. Welche Programme entsprechenden PUA-Schutz leisten, überprüft AV-TEST in regelmäßigen Abständen in umfangreichen Tests zu Sicherheitsprogrammen für Mac.

TOP 10 Mac-PUA 2015

1	VSEARCH	31.796
2	MACNIST	31.504
3	OSX	5.422
4	BUNDLORE	2.023
5	GENIEO	1.872
6	XAMLOADER	1.856
7	INSTALLCORE	393
8	SPIGOT	294
9	KEYGEN	235
10	CROSSRIDER	190

TOP 10 Mac-PUA Q1/Q2 2016

1	VSEARCH	20.819
2	OSX	8.475
3	BUNDLORE	4.905
4	EXTINSTALL	3.686
5	XAMLOADER	2.303
6	GENIEO	1.368
7	CROSSRIDER	543
8	INSTALLCORE	521
9	SPIGOT	254
10	TOOLBAR	238

Trend 2016

Im ersten Halbjahr dieses Jahres ist ein deutlicher Trend erkennbar; und zwar ein Angriff auf die Privatsphäre von Android-Nutzern durch die Werbeindustrie.

Die AV-TEST-Systeme registrierten im ersten Quartal 2016 einen massiven Anstieg von Potentiell Unerwünschten Anwendungen für Android mit einer Steigerungsrate von mehr als 13 Prozent im Vergleich zum Vorjahr. Gleichzeitig sinkt die Anzahl im Gesamtverhältnis gemessener PUA-Angriffe auf Windows-PCs quasi um genau diesen Prozentanteil (14,24 Prozent). Der Trend ist also deutlich: Die Werbeindustrie nimmt 2016 verstärkt Googles Mobilplattform Android ins Visier. Diesen Trend stützt auch der Vergleich der Messungen für die PUA-Entwicklung bei Windows.

PUA-Entwicklung unter Beobachtung

Aktuell bewegen sich Werbefirmen mit PUA noch in einem nahezu rechtsfreien Raum. Die meisten Hersteller von AV-Produkten wären zwar technisch in der Lage, solche Angriffe auf die Privatsphäre von Online-Nutzern auf allen gängigen Plattformen zu erkennen, allerdings ist die Erkennung von PUA nach wie vor ein Politikum. Das zeigen auch Verhandlungen der Clean Software Alliance (CSA), eine Diskussionsplattform von PUA-einsetzender Werbeindustrie und Anbieter von Schutz-Software. Das AV-TEST Institut, als aktiver Teilnehmer der bisherigen CSA-Konferenzen, wird die Entwicklung von PUA auf allen wesentlichen Plattformen weiterhin messen und analysieren sowie regelmäßig über die aktuelle Lage informieren.

AV TEST av-test.org

Die AV-TEST GmbH überprüft regelmäßig alle auf dem Markt relevanten Schutz-Lösungen auch auf die Abwehr von PUA. Die aktuellen Testergebnisse können kostenlos auf der Website unter https://www.av-test.org/de/antivirus/ abgerufen werden.

Teststatistiken

Als eines der führenden Institute im Bereich Sicherheitsforschung nutzt AV-TEST ausgeklügelte und selbstentwickelte Analysesysteme und Testverfahren.

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 Reaktionszeiten jeweiliger Hersteller auf neue Bedrohungen erfasst das System ebenfalls automatisiert. So erweitert VTEST ständig eine der größten Datenbanken für Schadprogramme weltweit. Deren Datenbestand wächst seit mehr als 15 Jahren kontinuierlich auf über 250 Servern mit einer Speicherkapazität von über 2200 Terabyte. Zum Veröffentlichungsstand dieses Jahresreports beinhaltete die AV-TEST Datenbank 578.702.687 Schadprogramme für Windows und 16.514.928 Schadprogramme für Android!

Zur gezielten Malware-Analyse bringt AV-TEST die Eigenentwicklung „Sunshine“ zum Einsatz. Das Analyse-System 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 potentiell 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. 2015 wurden so über 200 Produkttests allein für Privatanwender- und Unternehmensprodukte gefahren. Dabei wurden pro Produkt 171.433 Malware-Attacken durchgeführt sowie 3.227.191 einzelne Datensätze für Fehlalarmtests eingesetzt und ausgewertet. Im gesamten Jahr 2015 waren das 683.123.424 von den Testexperten zu überprüfende Datensätze. In den monatlichen Android-Tests nahmen sich die Tester 2015 über 160 einzelne Produkte vor. Dabei musste sich jede überprüfte Sicherheits-App gegen über 29.030 spezielle Android-Schädlinge zur Wehr setzen. Zur Gegenprobe erfassten die Experten zudem über 469.128 Scans von sicheren Apps, um die Anfälligkeit für Fehlalarme zu überprüfen. Im Labor wurden in Tests von Sicherheitsprodukten darum insgesamt 1.352.234 Scan-Vorgänge gemonitort 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 selbstentwickelte Analysesysteme und garantiert so von Dritten unbeeinflusste und jederzeit reproduzierbare Testergebnisse für alle gängigen Betriebssysteme und Plattformen.

Dank langjähriger Expertise, intensiver Forschung und ständig aktualisierten Laborumgebungen gewährleistet AV-TEST höchste Qualitätsstandards getesteter und zertifizierter IT-Sicherheitsprodukte. Neben der klassischen Viren-Forschung arbeitet AV-TEST 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