



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Neue Malware- und PUA-Varianten

Dezember 2021

Statistik-Bericht Nr. 2 zur Lage der Cyber-Sicherheit



Inhalt

| | | |
|----------|--|----|
| 1 | Methodische Erläuterungen..... | 3 |
| 2 | Tabellen und Grafiken..... | 4 |
| 2.1 | Kennzahlen: Neue Malware- und PUA-Varianten..... | 4 |
| 2.2 | Neue Malware- und PUA-Varianten im Dezember 2021 nach Art der Malware..... | 6 |
| 2.3 | Lange Reihe: Neue Malware-Varianten 2015 bis Dezember 2021..... | 8 |
| noch 2.3 | Lange Reihe: Neue Windows-Malware-Varianten 2015 bis Dezember 2021..... | 11 |
| noch 2.3 | Lange Reihe: Neue Android-Malware-Varianten 2015 bis Dezember 2021..... | 14 |
| 3 | Statistische Konzepte und Definitionen..... | 18 |

Zeichenerklärung

| | |
|---|---|
| f | Wert wurde fortgeschrieben. |
| . | Wert ist unbekannt. |
| - | Wert ist empirisch Null (d.h. nichts vorhanden). |
| 0 | Wert ist rechnerisch Null (d.h. empirisch größer als nichts). |
| X | Aussage ist nicht sinnvoll. |
| r | Wert wurde gegenüber früheren Publikationen berichtigt. |
| / | Wert ist statistisch unsicher und wird daher nicht ausgewiesen. |

In der Reihe „**Statistik**-Berichte zur Lage der Cyber-**Sicherheit**“ erscheinen:

Zur Bedrohungslage:

Bericht 1: E-Mails und Spam-E-Mails in der Wirtschaft in Deutschland

Bericht 2: Neue Malware- und PUA-Varianten

Bericht 3: Schwachstellen (Bericht im Aufbau)

Zur Prävention in der Bundesverwaltung:

Bericht 4: E-Mails und Spam-E-Mails an die Bundesverwaltung

Bericht 5: Malware Protection der Bundesverwaltung (Bericht im Aufbau)

Impressum

Bundesamt für Sicherheit in der Informationstechnik

Referat OC 33 – Nationales IT-Lagezentrum, Analysen und Prognosen

Postfach 20 03 63

53175 Bonn

Tel.: +49 228 99 9582-6227

E-Mail: statistik@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2022

1 Methodische Erläuterungen

1. Ziel der Statistik:

Die Malware-Statistik stellt den Stand und die Entwicklung des neu bekannt gewordenen Malware-Aufkommens im Internet dar. Darüber hinaus werden neue Varianten potenziell unerwünschter Anwendungssoftware (PUA) erhoben. Berichtet wird nicht über Angriffe mit Malware, sondern über das bekannt gewordene Malware-Aufkommen insgesamt. Berichtszeiträume sind Monate und Quartale.

2. Grundgesamtheit:

Grundgesamtheit der Malware-Statistik sind alle im Internet verfügbaren Programme, die schädliche Operationen durchführen können, einschl. solcher Programme, die andere Programme befähigen, schädliche Operationen durchzuführen (z.B. Nachlade-Software). Nicht enthalten sind URLs, über die solche Programme heruntergeladen werden, enthalten sind aber die heruntergeladenen Programme. Als Variante einer Malware gilt jede auch nur geringfügig veränderte Kopie dieser Malware. Im Gegensatz zu neuer Malware besitzen neue Varianten von bereits bekannter Malware keine neuen Funktionalitäten. Neue Varianten sind aber im Hinblick auf den resultierenden Hashwert einzigartig.

3. Stichprobe:

In die Stichprobe fließen alle neuen Malware-Varianten ein, die dem BSI aus den Erhebungen des Instituts AV-Test GmbH bekannt geworden sind.

4. Reichweite und Aussagekraft:

Die Malware-Statistik umfasst Programme, die schädliche Operationen ausführen können oder andere Programme dazu befähigen, dies zu tun. Erhoben werden u.a. die Art der Malware sowie die Plattform und das Format. Darüber hinaus werden neue Varianten potenziell unerwünschter Anwendungssoftware (PUA) erhoben. Da jede neue Malware-Variante eine Bedrohung in dem Sinne darstellt, dass sie für Angriffe verwendet werden kann, quantifiziert die Statistik die Bedrohungslage durch neue Malware. Die errechneten Indikatoren sind Frühwarn-Indikatoren für Cyber-Angriffe, da mehr neue Malware-Varianten auch mehr Angriffe mit diesen neuen Varianten nach sich ziehen werden. Die Wahrscheinlichkeit von Malware-Angriffen steigt also mit der Menge neuer Malware-Varianten, wobei aber zwischen dem Auftreten neuer Varianten und Angriffen kein zeitlicher Zusammenhang bestehen muss. Umgekehrt bedeutet ein Rückgang der Indikatoren nicht immer eine Entspannung der Bedrohungslage, da die Produktion neuer Varianten auch deshalb zurückgegangen sein kann, weil die Angreifer mit den bestehenden Varianten ihre Ziele erfolgreich erreichen und die Produktion neuer Varianten insofern nicht erforderlich ist.

Eine qualitative Einschätzung der Bedrohung im Sinne einer Gewichtung nach Verbreitungsgrad oder Schadenspotenzial einer Malware wird durch die Malware-Statistik nicht ermöglicht. Aussagen über Angriffe mit Malware sind ebenfalls nicht möglich.

5. Qualitätsbewertung:

Die Ergebnisse der Malware-Statistik können aufgrund des Umfangs und des Aktualisierungs-Konzepts der zugrundeliegenden Datenbanken als vergleichsweise genau betrachtet werden. Da keine Erkenntnisse über das Dunkelfeld der unbekannt Malware vorliegen, gilt dies allerdings nur für das tatsächlich in der Statistik erfasste Hellfeld der neu bekannt gewordenen Malware.

Inkonsistenzen können durch die sich kontinuierlich verbessernden Methoden der Malware-Detektion, insbesondere der Viren-Scanner, entstehen. Diese werden durch standardisierte Revisionen zwar größten Teils aufgefangen. Da die Revisionszyklen jedoch maximal eineinhalb Quartale umfassen, ist davon auszugehen, dass ältere Berichtszeiträume das tatsächliche Malware-Aufkommen tendenziell etwas unterschätzen.

2 Tabellen und Grafiken

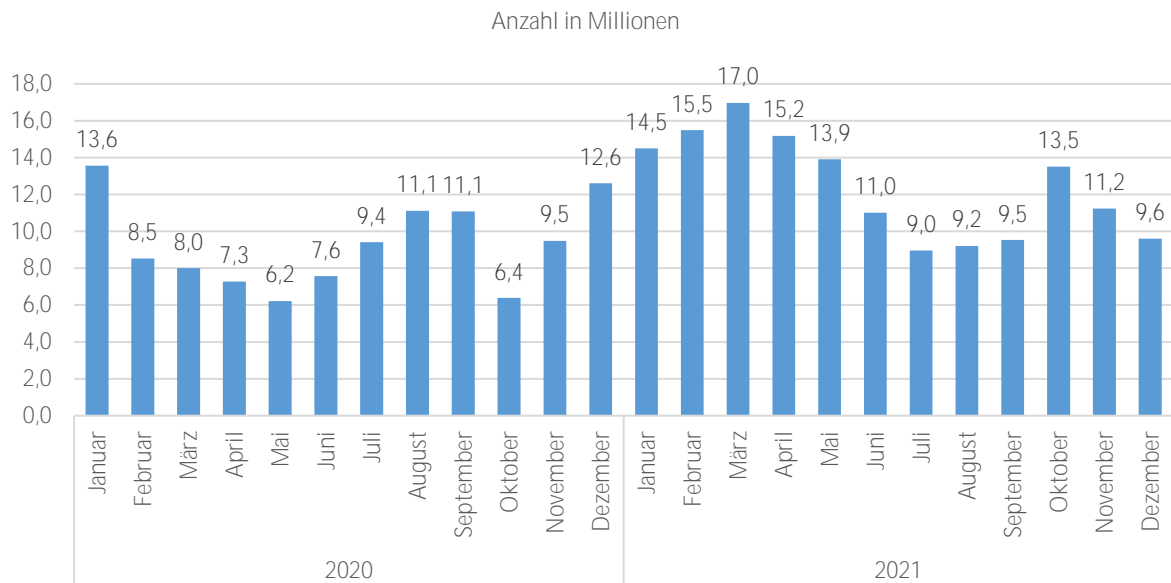
2.1 Kennzahlen: Neue Malware- und PUA-Varianten

| Kennzahlen | Einheit | Dezember 2021 | November 2021 | Dezember 2020 |
|--------------------------------------|-----------------|---------------|---------------|---------------|
| Neue Malware-Varianten | Anzahl in 1.000 | 9.607 | 11.227 | 12.611 |
| Messzahl | 2018=100 | 117 | 137 | 151 |
| Durchschnittlicher täglicher Zuwachs | Anzahl in 1.000 | 310 | 374 | 407 |
| Veränderung zum Vormonat | % | -17 | -14 | 33 |
| Abweichung vom 12-Monatsdurchschnitt | % | -24 | -10 | 34 |
| Neue PUA-Varianten | Anzahl in 1.000 | 380 | 711 | 1.418 |
| Messzahl | 2018=100 | 26 | 48 | 88 |
| Durchschnittlicher täglicher Zuwachs | Anzahl in 1.000 | 12 | 24 | 46 |
| Veränderung zum Vormonat | % | -48 | 34 | -18 |
| Abweichung vom 12-Monatsdurchschnitt | % | -51 | -14 | 46 |

© Bundesamt für Sicherheit in der Informationstechnik

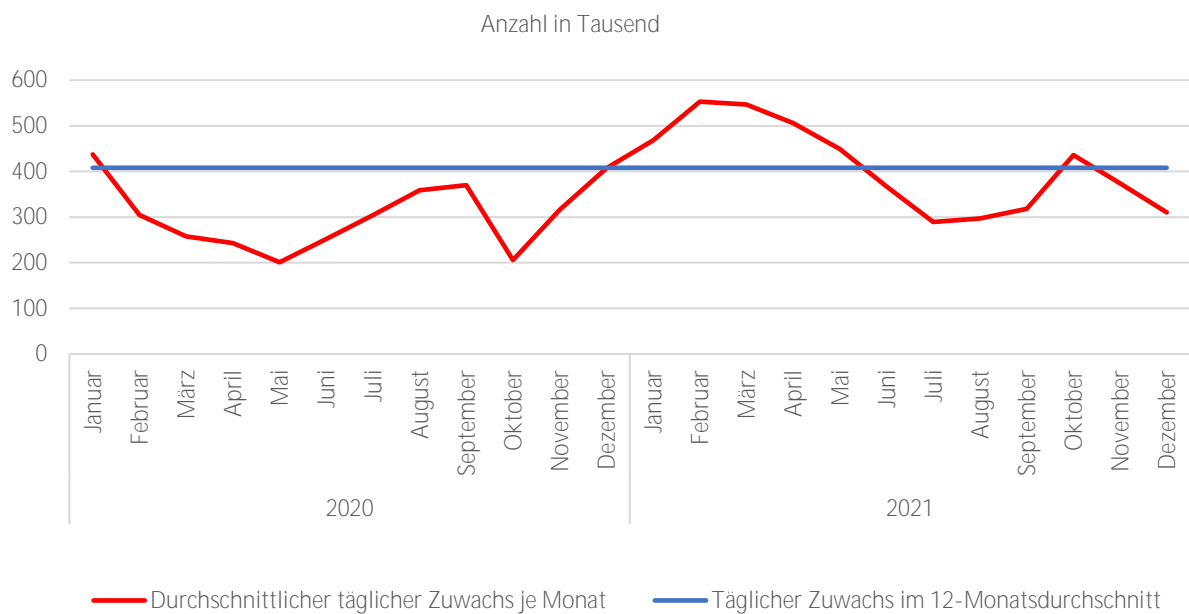
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Neue Malware-Varianten von Januar 2020 bis Dezember 2021



© Bundesamt für Sicherheit in der Informationstechnik 2022

Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten von Januar 2020 bis Dezember 2021



© Bundesamt für Sicherheit in der Informationstechnik 2022

| 2.2 Neue Malware- und PUA-Varianten im Dezember 2021 nach Art der Malware | | | | |
|---|-----------------|---------------------------|-----------------|---------------------------|
| Art der Malware | Malware | | PUA | |
| | Anzahl in 1.000 | Anteil in % der Kategorie | Anzahl in 1.000 | Anteil in % der Kategorie |
| Plattformbezogene Malware | | | | |
| Plattformen für Desktop-Rechner und Server | 7.860 | 96,7 | 264 | 73,0 |
| Windows | 7.571 | 96,3 | 263 | 99,5 |
| Linux | 289 | 3,7 | / | / |
| MacOS | / | / | 1 | 0,4 |
| Plattformen für mobile Geräte | 266 | 3,3 | 98 | 27,0 |
| iOS | / | / | / | / |
| Android | 266 | 99,9 | 98 | 99,9 |
| andere | / | / | / | / |
| Zusammen | 8.126 | 84,6 | 362 | 95,3 |
| Plattformunabhängige Malware | | | | |
| Skript | 936 | 63,2 | 18 | 99,2 |
| Office | 19 | 1,3 | 0 | 0,6 |
| Java | 1 | 0,0 | / | / |
| Dos | / | / | / | / |
| Dokumententypen | 525 | 35,5 | / | / |
| Zusammen | 1.481 | 15,4 | 18 | 4,7 |
| Insgesamt | | | | |
| Insgesamt | 9.607 | X | 380 | X |

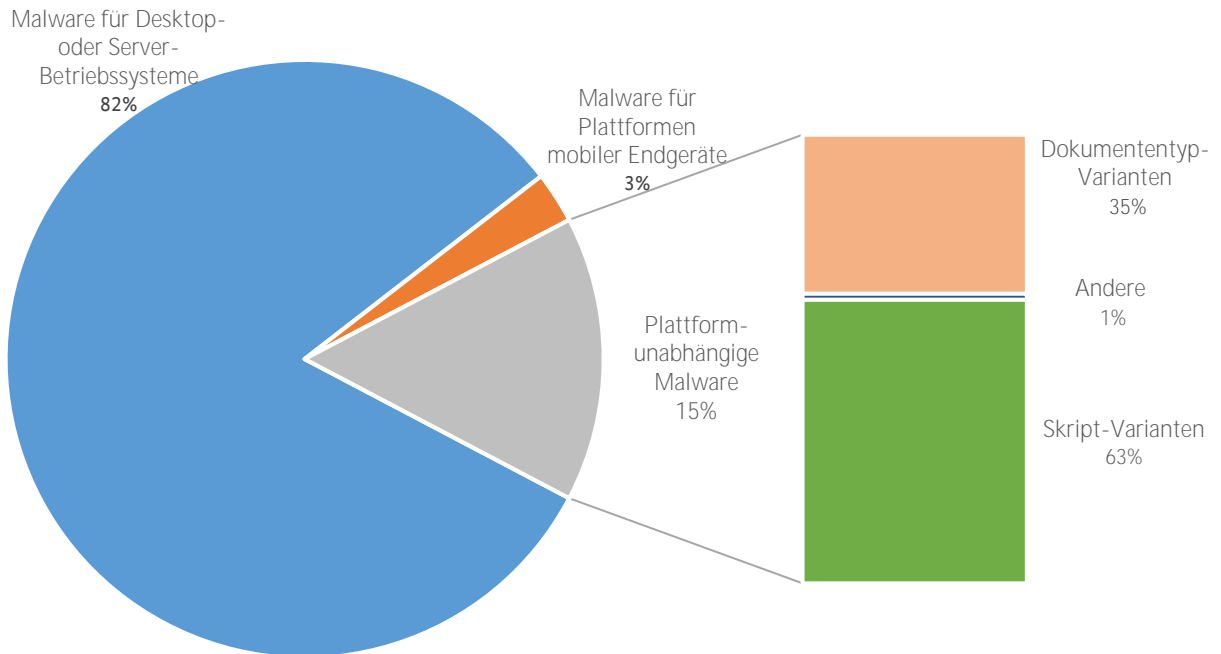
© Bundesamt für Sicherheit in der Informationstechnik

Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Neue Malware-Varianten im Dezember 2021 nach Art der Plattform

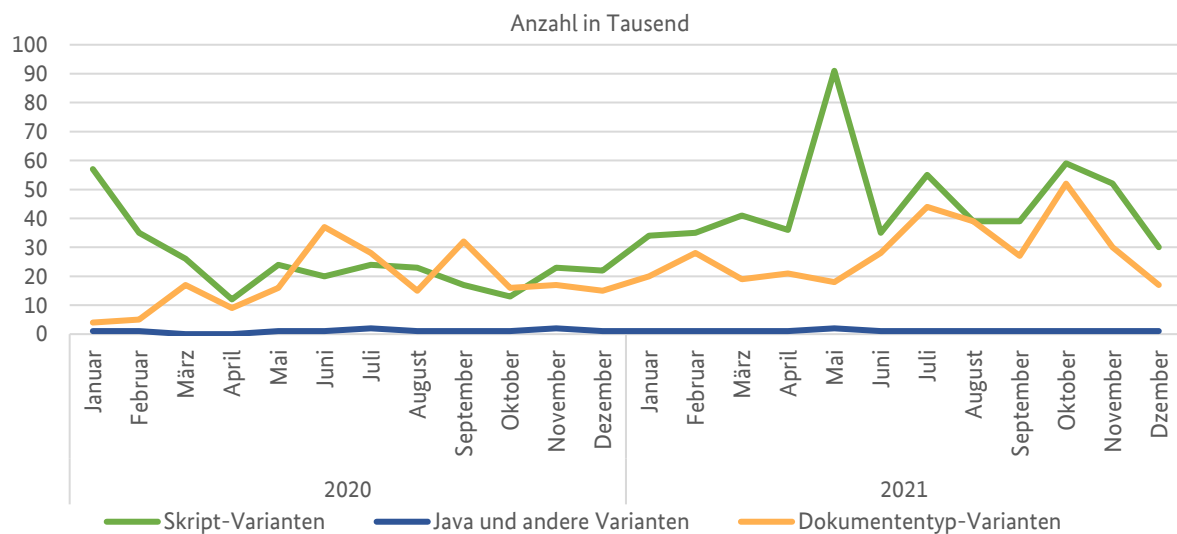
Anteil in % an allen neuen Malware-Varianten

Anteil in % an allen plattformunabhängigen neuen Malware-Varianten



© Bundesamt für Sicherheit in der Informationstechnik 2022

Durchschnittlicher täglicher Zuwachs neuer plattformunabhängiger Varianten von Januar 2020 bis Dezember 2021 nach Art der Malware



© Bundesamt für Sicherheit in der Informationstechnik 2022

| 2.3 Lange Reihe: Neue Malware-Varianten 2015 bis Dezember 2021 | | | | |
|--|-----------|-----------|--------------------------------------|-----|
| Jahr | Monat | Insgesamt | | |
| | | Anzahl | Durchschnittlicher täglicher Zuwachs | |
| | | 1.000 | Veränderung zum Vormonat in % | |
| 2021 | | 149.087 | 409 | X |
| | Dezember | 9.607 | 310 | -17 |
| | November | 11.227 | 374 | -14 |
| | Oktober | 13.517 | 436 | 37 |
| | September | 9.525 | 318 | 7 |
| | August | 9.211 | 297 | 3 |
| | Juli | 8.959 | 289 | -21 |
| | Juni | 11.003 | 367 | -18 |
| | Mai | 13.909 | 449 | -11 |
| | April | 15.172 | 506 | -8 |
| | März | 16.966 | 547 | -1 |
| | Februar | 15.488 | 553 | 18r |
| | Januar | 14.503 | 468 | 15 |
| 2020 | | 111.243 | 305 | X |
| | Dezember | 12.611 | 407 | 33 |
| | November | 9.474 | 316 | 48 |
| | Oktober | 6.382 | 213 | -42 |
| | September | 11.087 | 358 | 0 |
| | August | 11.115 | 371 | 18 |
| | Juli | 9.414 | 304 | 24 |
| | Juni | 7.573 | 252 | 22 |
| | Mai | 6.223 | 201 | -15 |
| | April | 7.281 | 243 | -9 |
| | März | 8.000 | 258 | -6 |
| | Februar | 8.528 | 305 | -37 |
| | Januar | 13.555 | 437 | 2 |
| 2019 | | 111.787 | 306 | X |
| | Dezember | 13.323 | 430 | 10 |
| | November | 12.143 | 392 | 21 |
| | Oktober | 10.033 | 334 | -29 |
| | September | 14.091 | 455 | 43 |
| | August | 9.886 | 330 | 41 |
| | Juli | 7.023 | 227 | 7 |
| | Juni | 6.594 | 220 | -8 |
| | Mai | 7.163 | 231 | -21 |
| | April | 9.121 | 304 | 12 |

| | | | | |
|------|-----------|--------|-----|-----|
| | März | 8.133 | 262 | 20 |
| | Februar | 6.791 | 243 | -9 |
| | Januar | 7.489 | 242 | -6 |
| 2018 | | 99.991 | 274 | X |
| | Dezember | 8.007 | 258 | 6 |
| | November | 7.524 | 243 | 64 |
| | Oktober | 4.584 | 153 | -45 |
| | September | 8.288 | 267 | -8 |
| | August | 9.015 | 301 | 0 |
| | Juli | 9.028 | 291 | 5 |
| | Juni | 8.639 | 288 | 0 |
| | Mai | 8.680 | 280 | -18 |
| | April | 10.538 | 351 | 10 |
| | März | 9.601 | 310 | 33 |
| | Februar | 7.228 | 258 | -18 |
| | Januar | 8.858 | 286 | -18 |
| 2017 | | 86.179 | 236 | X |
| | Dezember | 10.829 | 349 | 17 |
| | November | 9.259 | 299 | -31 |
| | Oktober | 13.367 | 446 | 128 |
| | September | 5.866 | 189 | -15 |
| | August | 6.935 | 231 | 210 |
| | Juli | 2.236 | 72 | -65 |
| | Juni | 6.324 | 211 | -10 |
| | Mai | 7.061 | 228 | 12 |
| | April | 6.298 | 210 | -11 |
| | März | 7.050 | 227 | 39 |
| | Februar | 5.067 | 181 | -14 |
| | Januar | 5.888 | 190 | 24 |
| 2016 | | 78.235 | 215 | X |
| | Dezember | 4.753 | 153 | 10 |
| | November | 4.329 | 140 | -7 |
| | Oktober | 4.655 | 155 | -13 |
| | September | 5.331 | 172 | -5 |
| | August | 5.608 | 187 | 9 |
| | Juli | 5.161 | 166 | -46 |
| | Juni | 9.473 | 316 | 33 |
| | Mai | 7.115 | 230 | -9 |
| | April | 7.776 | 259 | -1 |
| | März | 7.837 | 253 | -2 |
| | Februar | 7.979 | 285 | -3 |
| | Januar | 8.217 | 265 | 36 |
| 2015 | | 86.628 | 238 | X |
| | Dezember | 6.049 | 195 | 7 |

| | | | |
|-----------|--------|-----|-----|
| November | 5.643 | 182 | -27 |
| Oktober | 7.731 | 258 | 53 |
| September | 5.065 | 163 | 8 |
| August | 4.689 | 156 | -25 |
| Juli | 6.257 | 202 | -46 |
| Juni | 11.640 | 388 | 29 |
| Mai | 9.039 | 292 | -10 |
| April | 10.034 | 334 | 17 |
| März | 8.566 | 276 | 32 |
| Februar | 6.497 | 232 | 20 |
| Januar | 5.417 | 175 | . |

© Bundesamt für Sicherheit in der Informationstechnik

Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

noch 2.3 Lange Reihe: Neue Windows-Malware-Varianten 2015 bis Dezember 2021

| Jahr | Monat | Windows-Malware | | |
|------|-----------|-----------------|--------------------------------------|-----|
| | | Anzahl | Durchschnittlicher täglicher Zuwachs | |
| | | 1.000 | Veränderung zum Vormonat in % | |
| 2021 | | 117.077 | 323 | X |
| | Dezember | 7.571 | 244 | -11 |
| | November | 8.216 | 274 | -13 |
| | Oktober | 9.493 | 316 | 32 |
| | September | 7.203 | 240 | 15 |
| | August | 6.464 | 209 | -29 |
| | Juli | 5.513 | 178 | -46 |
| | Juni | 8.777 | 293 | -11 |
| | Mai | 10.220 | 330 | -25 |
| | April | 13.158 | 439 | -8 |
| | März | 14.811 | 478 | 0 |
| | Februar | 13.353 | 477 | 20 |
| | Januar | 12.297 | 397 | 11 |
| 2020 | | 91.274 | 250 | X |
| | Dezember | 11.056 | 357 | 34 |
| | November | 7.985 | 266 | 60 |
| | Oktober | 5.159 | 166 | -44 |
| | September | 8.861 | 295 | -4 |
| | August | 9.586 | 309 | 28 |
| | Juli | 7.480 | 241 | 30 |
| | Juni | 5.557 | 185 | 23 |
| | Mai | 4.650 | 150 | -29 |
| | April | 6.381 | 213 | 3 |
| | März | 6.380 | 206 | -18 |
| | Februar | 7.051 | 252 | -30 |
| | Januar | 11.129 | 359 | -1 |
| 2019 | | 89.999 | 246 | X |
| | Dezember | 11.206 | 361 | 7 |
| | November | 10.144 | 338 | 26 |
| | Oktober | 8.305 | 268 | -23 |
| | September | 10.486 | 350 | 31 |
| | August | 8.265 | 267 | 49 |
| | Juli | 5.545 | 179 | -1 |
| | Juni | 5.431 | 181 | -3 |
| | Mai | 5.813 | 188 | -11 |
| | April | 6.305 | 210 | -2 |

| | | | | |
|------|-----------|--------|-----|-----|
| | März | 6.671 | 215 | 6 |
| | Februar | 5.702 | 204 | 3 |
| | Januar | 6.127 | 198 | -9 |
| 2018 | | 63.997 | 175 | X |
| | Dezember | 6.719 | 217 | 14 |
| | November | 5.682 | 189 | 132 |
| | Oktober | 2.533 | 82 | -55 |
| | September | 5.494 | 183 | 5 |
| | August | 5.385 | 174 | -3 |
| | Juli | 5.565 | 180 | 29 |
| | Juni | 4.179 | 139 | 2 |
| | Mai | 4.221 | 136 | -29 |
| | April | 5.734 | 191 | -6 |
| | März | 6.334 | 204 | 7 |
| | Februar | 5.352 | 191 | -13 |
| | Januar | 6.799 | 219 | -11 |
| 2017 | | 53.482 | 147 | X |
| | Dezember | 7.636 | 246 | 48 |
| | November | 5.008 | 167 | -2 |
| | Oktober | 5.271 | 170 | 13 |
| | September | 4.514 | 150 | -7 |
| | August | 5.038 | 163 | 618 |
| | Juli | 701 | 23 | -84 |
| | Juni | 4.326 | 144 | 24 |
| | Mai | 3.591 | 116 | -5 |
| | April | 3.644 | 121 | -29 |
| | März | 5.269 | 170 | 14 |
| | Februar | 4.188 | 150 | 8 |
| | Januar | 4.296 | 139 | 17 |
| 2016 | | 52.332 | 143 | X |
| | Dezember | 3.667 | 118 | 12 |
| | November | 3.174 | 106 | 4 |
| | Oktober | 3.147 | 102 | -24 |
| | September | 3.989 | 133 | 4 |
| | August | 3.960 | 128 | 1 |
| | Juli | 3.911 | 126 | -28 |
| | Juni | 5.277 | 176 | -18 |
| | Mai | 6.613 | 213 | 27 |
| | April | 5.052 | 168 | 6 |
| | März | 4.921 | 159 | 17 |
| | Februar | 3.796 | 136 | -13 |
| | Januar | 4.826 | 156 | 10 |
| 2015 | | 69.078 | 190 | X |
| | Dezember | 4.374 | 141 | 1 |

| | | | |
|-----------|--------|-----|-----|
| November | 4.179 | 139 | -12 |
| Oktober | 4.916 | 159 | 69 |
| September | 2.815 | 94 | -12 |
| August | 3.316 | 107 | -23 |
| Juli | 4.285 | 138 | -59 |
| Juni | 10.215 | 341 | 32 |
| Mai | 7.991 | 258 | -16 |
| April | 9.189 | 306 | 25 |
| März | 7.630 | 246 | 25 |
| Februar | 5.528 | 197 | 32 |
| Januar | 4.639 | 150 | . |

© Bundesamt für Sicherheit in der Informationstechnik

Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

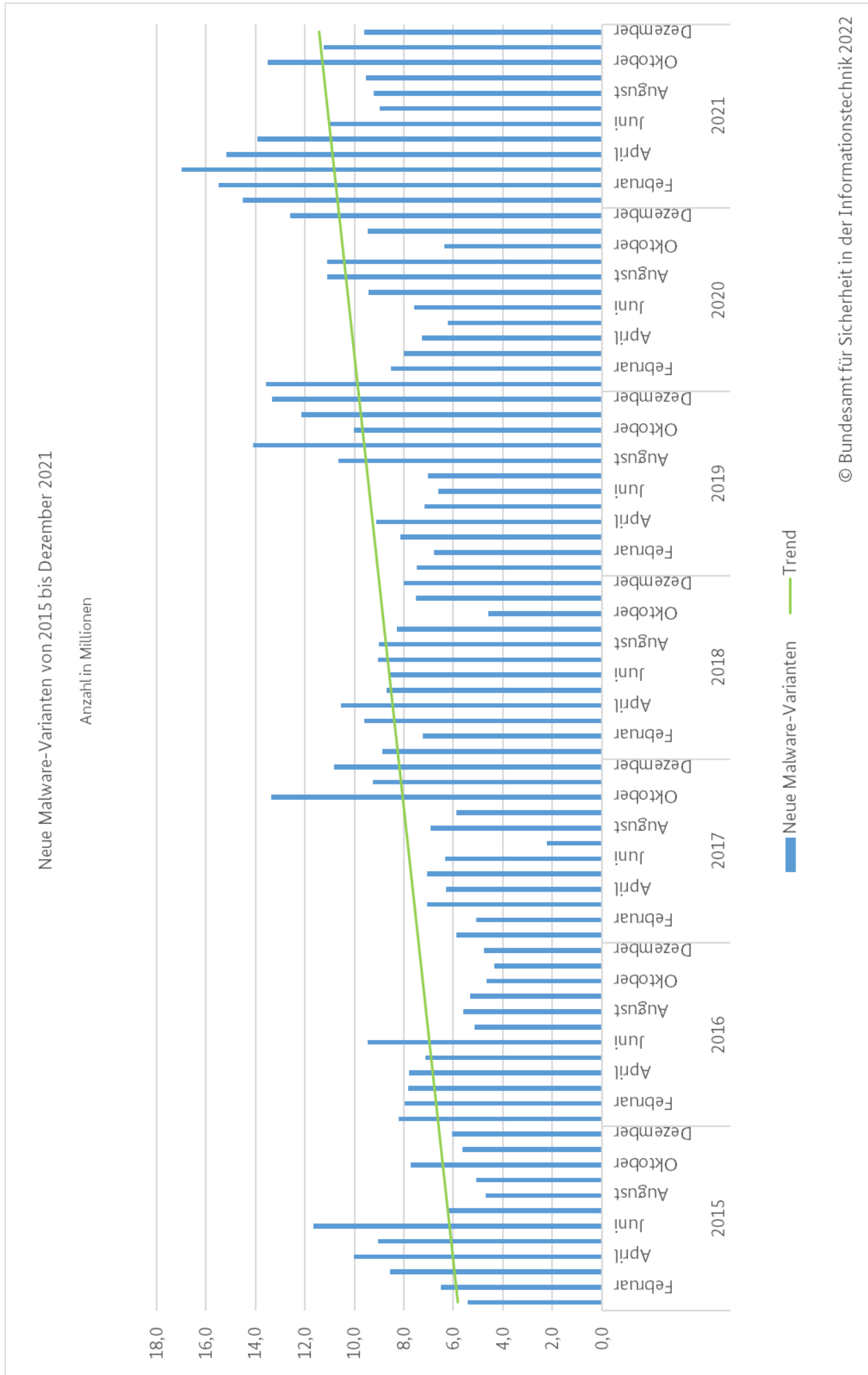
| noch 2.3 Lange Reihe: Neue Android-Malware-Varianten 2015 bis Dezember 2021 | | | | |
|---|-----------|-----------------|--------------------------------------|-----|
| Jahr | Monat | Android-Malware | | |
| | | Anzahl | Durchschnittlicher täglicher Zuwachs | |
| | | 1.000 | Veränderung zum Vormonat in % | |
| 2021 | | 3.269 | 9 | X |
| | Dezember | 266 | 9 | 8r |
| | November | 239 | 8 | -9r |
| | Oktober | 271 | 9 | 8r |
| | September | 242 | 8 | -4r |
| | August | 260 | 8 | -15 |
| | Juli | 287 | 9 | -6 |
| | Juni | 296 | 10 | 24 |
| | Mai | 246 | 8 | 16 |
| | April | 206 | 7 | 11 |
| | März | 192 | 6 | -43 |
| | Februar | 305 | 11 | 18r |
| | Januar | 458 | 15 | 69 |
| 2020 | | 3.182 | 9 | X |
| | Dezember | 271 | 9 | 15 |
| | November | 229 | 8 | 7 |
| | Oktober | 220 | 7 | 70 |
| | September | 126 | 4 | -52 |
| | August | 272 | 9 | 5 |
| | Juli | 259 | 8 | 3 |
| | Juni | 243 | 8 | -16 |
| | Mai | 297 | 10 | 20 |
| | April | 240 | 8 | -3 |
| | März | 256 | 8 | -20 |
| | Februar | 290 | 10 | -33 |
| | Januar | 480 | 15 | 11 |
| 2019 | | 3.131 | 9 | X |
| | Dezember | 433 | 14 | 28 |
| | November | 327 | 11 | 37 |
| | Oktober | 246 | 8 | -11 |
| | September | 267 | 9 | -1 |
| | August | 278 | 9 | 7 |
| | Juli | 261 | 8 | 32 |
| | Juni | 191 | 6 | -15 |
| | Mai | 231 | 7 | 6 |
| | April | 211 | 7 | 10 |

| | | | | |
|------|-----------|-------|----|-----|
| | März | 198 | 6 | -7 |
| | Februar | 193 | 7 | -28 |
| | Januar | 294 | 9 | 12 |
| 2018 | | 5.527 | 15 | X |
| | Dezember | 263 | 8 | -34 |
| | November | 383 | 13 | 8 |
| | Oktober | 366 | 12 | 11 |
| | September | 320 | 11 | -46 |
| | August | 617 | 20 | 29 |
| | Juli | 479 | 15 | -18 |
| | Juni | 568 | 19 | 20 |
| | Mai | 488 | 16 | -8 |
| | April | 512 | 17 | 3 |
| | März | 516 | 17 | 9 |
| | Februar | 427 | 15 | -20 |
| | Januar | 589 | 19 | 44 |
| 2017 | | 6.201 | 17 | X |
| | Dezember | 410 | 13 | -36 |
| | November | 624 | 21 | 17 |
| | Oktober | 551 | 18 | -11 |
| | September | 602 | 20 | -1 |
| | August | 631 | 20 | 10 |
| | Juli | 576 | 19 | 24 |
| | Juni | 451 | 15 | -37 |
| | Mai | 740 | 24 | 106 |
| | April | 348 | 12 | -34 |
| | März | 547 | 18 | 64 |
| | Februar | 302 | 11 | -20 |
| | Januar | 419 | 14 | 2 |
| 2016 | | 6.734 | 18 | X |
| | Dezember | 410 | 13 | 17 |
| | November | 339 | 11 | -39 |
| | Oktober | 578 | 19 | 13 |
| | September | 496 | 17 | -18 |
| | August | 628 | 20 | 28 |
| | Juli | 489 | 16 | -72 |
| | Juni | 1.692 | 56 | 308 |
| | Mai | 429 | 14 | 12 |
| | April | 370 | 12 | 19 |
| | März | 320 | 10 | -33 |
| | Februar | 429 | 15 | -14 |
| | Januar | 554 | 18 | 46 |
| 2015 | | 2.572 | 7 | X |
| | Dezember | 381 | 12 | 4 |

| | | | |
|-----------|-----|----|-----|
| November | 353 | 12 | 31 |
| Oktober | 279 | 9 | -5 |
| September | 284 | 9 | 11 |
| August | 264 | 9 | 50 |
| Juli | 175 | 6 | -11 |
| Juni | 191 | 6 | 81 |
| Mai | 109 | 4 | -26 |
| April | 143 | 5 | 9 |
| März | 136 | 4 | -17 |
| Februar | 147 | 5 | 46 |
| Januar | 111 | 4 | . |

© Bundesamt für Sicherheit in der Informationstechnik

Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH



3 Statistische Konzepte und Definitionen

Bedrohung:

Eine Bedrohung ist ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen wie zum Beispiel Cyber-Angriffe. Neue Malware-Varianten stellen eine Bedrohung dar, weil sie in der Regel produziert werden, um bestehende Schutzmaßnahmen gegen bekannte Malware zu unterwandern.

Malware:

Als Malware im Sinne der Malware-Statistik gilt jede Datei, die ganz oder teilweise aus Quell- oder Binärcode besteht, der auf dem befallenen System schädliche Operationen ausführen kann oder solchen Code in anderen Dateien dazu befähigen kann, schädliche Operationen durchzuführen (z.B. Nachlade-Malware).

Messzahl, Index:

Messzahlen stellen Veränderungen und Entwicklungen unabhängig von den absoluten Zahlen dar, indem die absoluten Zahlen ins Verhältnis zu einem früher gemessenen Durchschnittswert gesetzt werden. So bedeutet eine Malware-Messzahl von 120 Punkten (2018=100) beispielsweise, dass das Aufkommen an neuen Malware-Varianten 1,2 mal so hoch lag, wie im Durchschnitt des Jahres 2018. Durch die Verwendung von Messzahlen werden Trends und Entwicklungen unabhängig von den absoluten Größen direkt miteinander vergleichbar.

Neue Malware-Varianten:

Als Variante einer Malware gilt jede im Hinblick auf ihren Hashwert einzigartige Kopie einer Malware, auch wenn diese nur geringfügig verändert wurde. Im Gegensatz zu ganz neuer Malware besitzen neue Varianten von bereits bekannter Malware keine neuen Funktionalitäten. Sie stellen aber gleichwohl eine Bedrohung dar, weil jede neue Malware-Varianten in der Regel produziert werden, um bestehende Schutzmaßnahmen gegen bekannte Malware zu unterwandern.

Plattformbezogene Malware:

Als plattformbezogene Malware gilt jede Malware, die eine Schwachstelle in einem Betriebssystem ausnutzt. Plattformbezogene Malware unterscheidet sich nach der Art der Plattform in Malware für Desktop- oder Serverbetriebssysteme (Windows, Linux, MacOS) und Malware für Plattformen mobiler Endgeräte (Android, iOS, andere).

Plattformunabhängige Malware für Anwendungen:

Als plattformunabhängig gilt Malware, die Schwachstellen in Anwendungen wie zum Beispiel Office-Programmen, Browsern u.Ä. ausnutzt, sowie Malware, die als Anwendungsdatei getarnt ist. Dies trifft beispielsweise auf Excel-Makro-Viren (xlsx) zu, aber auch auf Bilddateien (jpeg u.Ä.) und Dokumententypen wie pdf, rtf, txt und andere.

PUA (Potentiell unerwünschte Anwendung):

Anwendungssoftware (oft als „Bundled“-Software vertrieben), die nicht eindeutig als Schadsoftware klassifiziert werden kann. Eine PUA zeichnet sich insbesondere dadurch aus, dass sie in der Regel vom Anwender zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als „unerwünscht“ angesehen werden, z. B. Informationssammlung und ggf. Weiterleitung des Anwenderverhaltens, Einblendung von Werbung, oder Ähnliches.

Täglicher Zuwachs:

Der durchschnittliche tägliche Zuwachs ist eine Kennzahl für die Menge neuer Malware-Varianten, die Angreifer in einem Berichtszeitraum produziert haben. Je höher der durchschnittliche tägliche Zuwachs, desto mehr Varianten wurden täglich produziert und desto größer die Bedrohung durch diese neuen Varianten.

