

Viren - Malware - Trojaner und Infektoren



Ein Computer-virus (lat. virus: Gift) ist ein sich selbst verbreitendes Computerstörprogramm, das sich unkontrolliert in andere Programme einschleust und sich weiter verbreiten kann.

Angriffsziel Nr. 1:
An den weltweiten Nutzerzahlen gemessen, bleibt Windows das Betriebssystem Nummer 1 als beliebtestes Angriffsziel.

Selbst wenn Sie alle wichtigen Sicherheitsregeln befolgen, und regelmäßig das Betriebssystem sowie alle installierten Programme aktualisieren, Spam-Mails ungelesen löschen, niemals auf verdächtige Links klicken und eine zuverlässige Antiviren-Lösung nutzen, kann es vorkommen, dass Ihr Computer mit einem Schadprogramm infiziert wird.

1. Unerwartete Abstürze: Wenn Sie so etwas schon einmal erlebt haben, wissen Sie, dass Systemabstürze oder das regelmäßige Erscheinen des berühmt-berüchtigten blauen Bildschirms Warnsignale sind, dass etwas mit dem Computer nicht stimmt. In diesem Fall sollten Sie den Rechner sofort auf Schadprogramme scannen.

2. Langsames System: Wenn Sie gerade keine leistungshungrigen Programme geöffnet haben, und der Computer trotzdem sehr langsam arbeitet, könnte das auf eine Infizierung mit einem Virus hindeuten.

3. Übermäßige Aktivität auf der Festplatte: Wenn Sie übermäßige Festplattenaktivität feststellen, obwohl der Computer eigentlich gerade nichts tun muss, ist das ebenfalls ein Zeichen für eine potenzielle Infizierung.



4. Seltsame Fenster: Wenn während des Computerstarts seltsame Fenster auftauchen, vor allem solche, die davor warnen, dass auf einzelne Laufwerke nicht zugegriffen werden kann, ist etwas faul auf Ihrem Computer.

5. Seltsame Benachrichtigungen: Wenn während des normalen Betriebs Benachrichtigungen auftauchen, die besagen, dass bestimmte Programme oder Dateien nicht geöffnet werden können, ist das ebenfalls ein schlechtes Zeichen.

6. Schädliche Programmaktivitäten: Wenn Ihre Programme auf einmal verschwinden, Fehler verursachen, sich automatisch und ohne Ihr Zutun öffnen, und/oder Benachrichtigungen angezeigt werden, dass ein Programm ohne Ihre Aufforderung auf das Internet zugreifen möchte, ist das ein ernstes Warnsignal, dass Sie zum Opfer eines Schadprogramms geworden sein könnten.

7. Zufällige Netzwerkaktivität: Wenn Ihr Router konstant blinkt und damit eine hohe Netzwerkaktivität anzeigt, obwohl Sie keine entsprechenden Programme geöffnet haben und auch keine großen Daten aus dem Internet übertragen, scheint etwas nicht zu stimmen.

8. Unberechenbare E-Mails: Wenn Ihre E-Mails nicht versendet werden, oder Ihnen von Kontakten mitgeteilt wird, dass diese seltsame Mails von Ihnen erhalten haben, die Sie eigentlich gar nicht geschickt haben, ist das ein sicheres Zeichen dafür, dass Ihr Computer kompromittiert wurde (oder dass Ihr E-Mail-Passwort gestohlen wurde).

9. IP-Adresse auf einer Blacklist: Wenn Sie die Benachrichtigung erhalten, dass Ihre IP-Adresse auf eine Blacklist gesetzt wurde, ist dies ein Zeichen, dass Ihr PC vielleicht von einem Hacker kontrolliert wird und nun zu einem Tentakel eines weitreichenden, Spam-versendenden Botnetzes geworden ist.



10. Unerwartetes Ausschalten der Antiviren-Lösung: Viele Schadprogramme versuchen, die installierte Antiviren-Lösung auszuschalten, um nicht davon entdeckt und gelöscht zu werden. Wenn die Sicherheitslösung auf Ihrem Computer plötzlich ausgeschaltet ist, könnte das auf ein größeres Problem hindeuten.

Die 10 Gebote der IT-Sicherheit

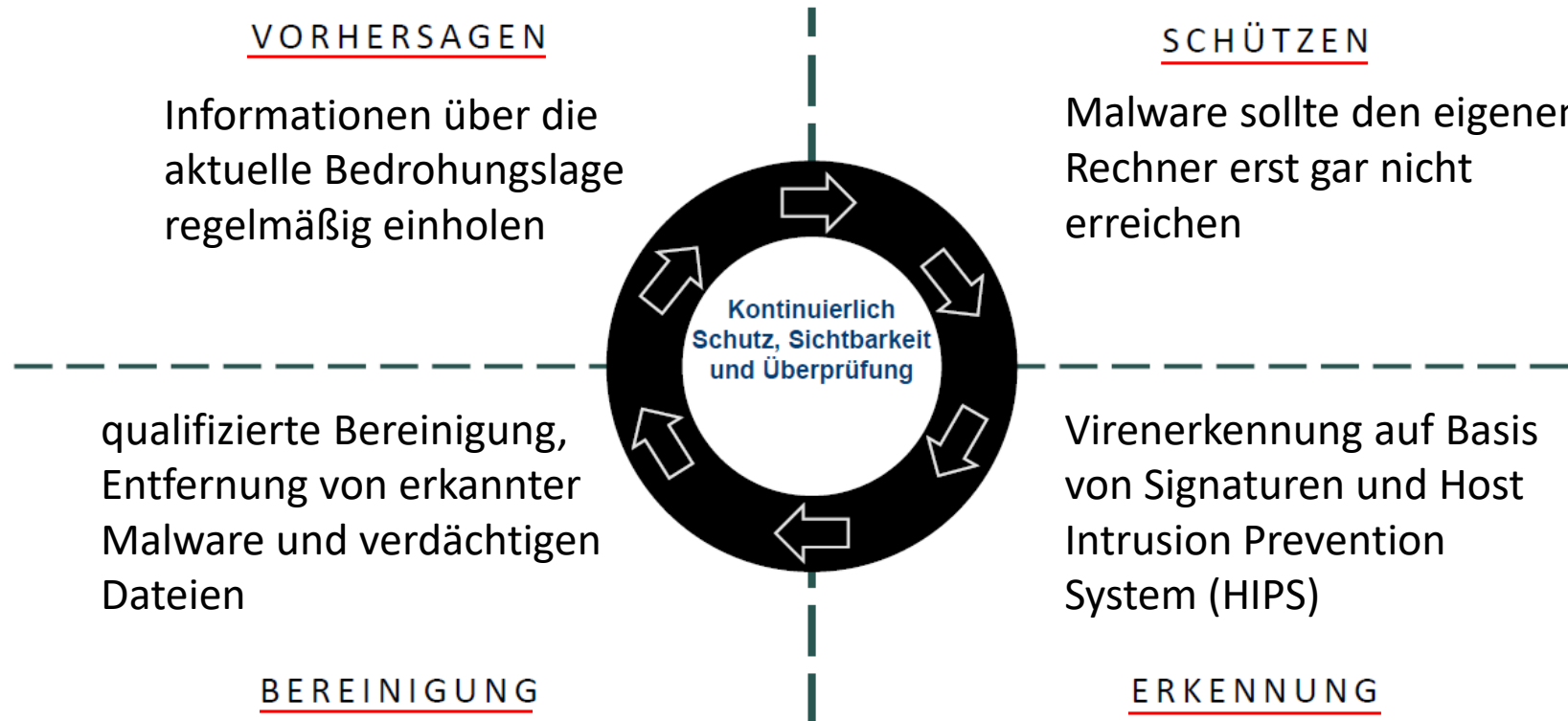
1. **Habe verschiedene Identitäten:** Verschiedene Identitäten - insbesondere E-Mail Adressen - für unterschiedliche Zwecke.
2. **Achte darauf was du wo eingibst:** Nicht jedes Fenster in das man einen PIN eingeben kann, sollte Ihnen gut bekommen.
3. **Klicke nicht auf »OK« ohne zu denken:** Zu schnelle Klicks auf »OK« können zur Bestellung eines Abos oder dem Löschen der Urlaubsfotos führen.
4. **Schreibe nicht in eine E-Mail was du nicht auch auf eine Postkarte schreiben würdest:** Mails können auch von anderen gelesen werden, genauso wie Postkarten vom Briefträger.
5. **Tue den Daten Anderer nur an, was du deinen eigenen Daten antun würdest:** Denn sonst geben andere auch die eigenen Daten bei Diensten ein, wo wir das nicht wollen.
6. **Kenne den Wert deiner Daten:** Auch wenn es scheinbar etwas kostenlos gibt, sobald man seine Daten eingibt, ist dies nicht mehr kostenlos.
7. **Habe gute Passwörter:** Denn auch für Haustüren benutzen wir kein Plastiks Schloss.
8. **Verberge, was du das Internet nicht wissen lassen willst:** Es gibt immer Dinge die nicht jeder andere Wissen soll.
9. **Vergesse nicht was du ins Internet schreibst, denn auch das Internet vergisst nicht:** Denn in irgendeinem Archiv findet man seine Daten wieder.



10. **Verwende das Internet nicht ohne aktuellen Virenschutz:** Man kann innerhalb kürzester Zeit einen Virus bekommen.

Hinweis: Email-Viren sind weitgehend chancenlos, wenn der Nutzer die Verseuchung nicht selbst einleitet, indem er auf etwas klickt, worauf er nicht klicken sollte. Von den aktuellen Viren (Malware, Trojaner, Threat, Infektor, etc.) können nur etwa die Hälfte von der aktuellen Schutzsoftware erkannt werden. Aber, ein schlechter Schutz ist besser als gar keiner.

ADAPTIVE SECURITY LIFECYCLE



Erkennung: In der Vergangenheit stützte sich die Virenerkennung auf Signaturen. Sobald eine neue Bedrohung entdeckt war, wurde eine neue Signatur als Update veröffentlicht, mit der sich der Virus erkennen lässt. Heutige Bedrohungen sind komplex und werden ständig modifiziert. Zur Erkennung moderner Malware ist daher HIPS notwendig. HIPS ist in der Lage, bösartige Verhaltensweisen zu erkennen.

Kann man sich vor Malware schützen?

Die Malware-Datenbank von AV-TEST verzeichnete zum 1. Quartal 2018 insgesamt 771.077.699 Schadprogramme für alle bekannten Betriebssysteme (vorwiegend Windows, ca. 70 %).

Quelle: ujima GmbH



Mussten Virens Scanner im Januar 2017 noch 8.852.322 neue Schadprogramme abwehren, waren es im Januar 2018 bereits 13.695.241 Schadprogramme.

70% der Malware Infektionen werden von Antivirus-Software nicht erkannt

Achtung: Die beste »Schutzsoftware« ist das eigene Verhalten.



Von den aktuellen Viren (Malware, Trojaner, Threat, Infektor, etc.) werden etwa nur 30 bis 60 Prozent von der Schutzsoftware erkannt. *Aber, ein schlechter Schutz ist besser als gar keiner.*

Im Jahr 2017 wurden 121.661.167 neue Schadprogramme (Malware-Samples) entdeckt, dass sind 3,9 neue Schadprogramme pro Sekunde.

Quelle: AV-Test - Institut

Das ewige IT-Mantra der elementaren IT-Sicherheitsregeln:

1. Aktiviere deinen gesunden Menschenverstand bei der Bewegung im Netz!
2. Misstraue allen Geschenken, die Dir per E-Mail zugesandt werden.
3. Öffne keine Dateianhänge in anlasslosen E-Mails, die von Unbekannten kommen.
4. Frage vor dem Öffnen von Dateianhängen/Links auch bei Zusendung durch Bekannte nach, wenn der Anhang Anlass für Fragen gibt.
5. Das fünfte Gebot: Du sollst nicht auf Links klicken, die Dir wilde Versprechungen machen!
6. Das sechste Gebot: Du sollst gar nicht auf Links in E-Mails klicken, wenn der Nutzen nicht klar nachzuvollziehen ist.
7. Du sollst Deinen Rechner mit aktueller Schutzsoftware schützen.
8. Dateianhänge kann und sollte man vor dem Öffnen grundsätzlich auf Viren prüfen.
9. Ach ja: Und Dienst ist Dienst, Schnaps ist Schnaps. Im Büro sollte man bestimmte Sorten von E-Mails so oder so weder versenden, noch öffnen.



Achtung: Die beste »Schutzsoftware« ist das eigene Verhalten.

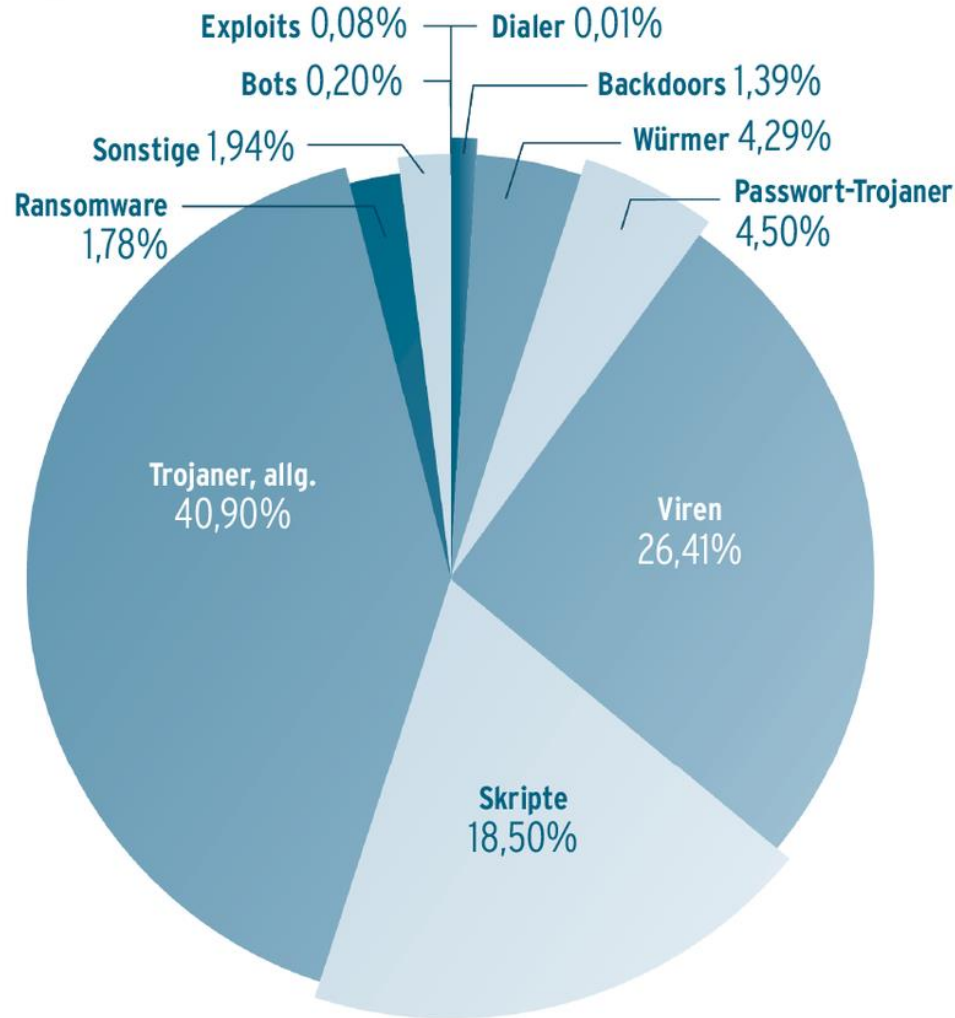
Statistik des Bundeskriminalamt – 2017:

Im Jahr 2017 wurden 251.617 Fälle mit dem »Tatmittel Internet« bekannt, das sind 4,4 % aller erfassten Straftaten (hohes Dunkelfeld).

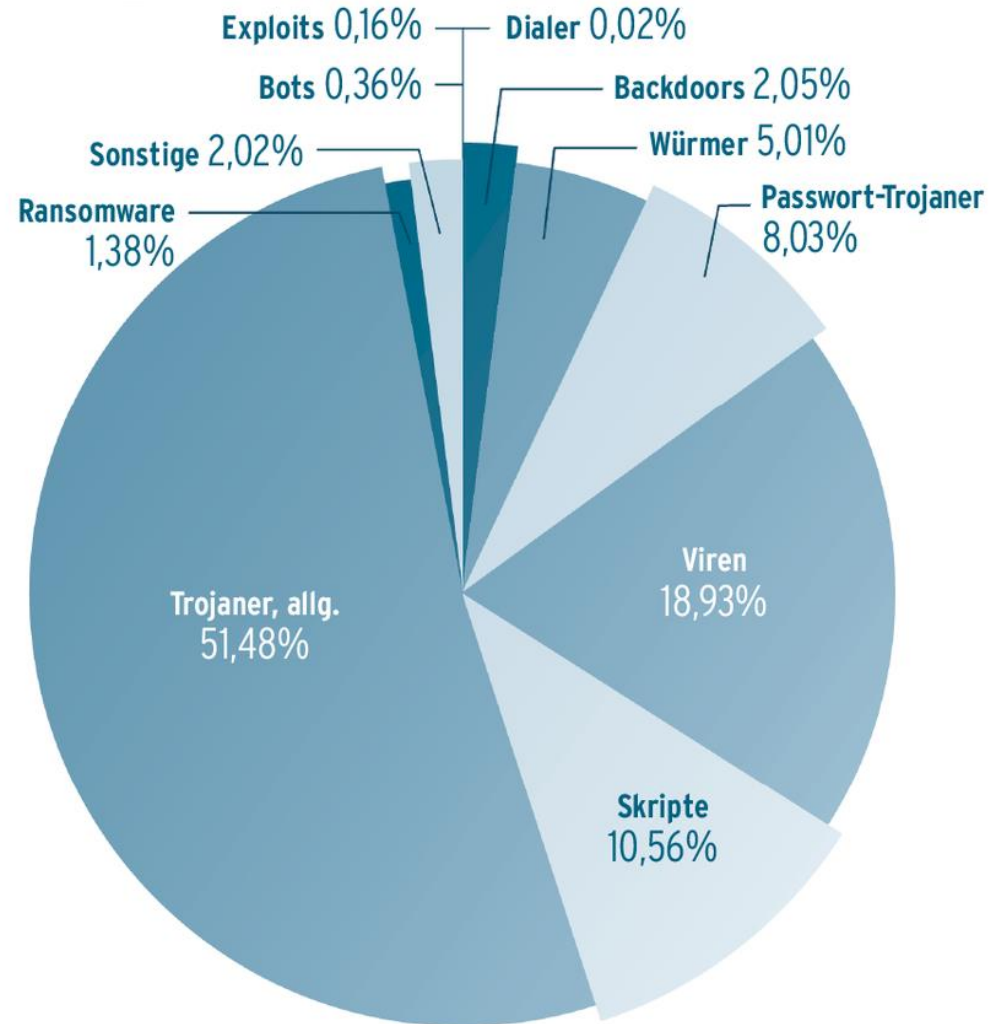


Verbreitung der Malware in Deutschland

Malware-Verteilung unter Windows 2017



Q1 2018



Hinweis: Trojan-Downloader können neue Malware auf den Computer herunterladen und installieren. Diese Programme werden eingesetzt, um Malware, Viren mit erweiterten, spezifischen Funktionen zu installieren oder die Erkennung von Schadprogrammen zu verhindern.

Eigenschaften von Trojaner: tarnen, ausspionieren, täuschen und stehlen



1. Hilfe bei Viren:

- Ruhe bewahren
- Programme beenden
- Computer ausschalten
- Trennung vom Netzwerk
- Benachrichtigung
- Kompletter Virenskan
- Überprüfung der internen und externen Datenspeicher
- Passwörter ändern
- ggf. Neuinstallation

Ein von einem Virus infizierter Arbeitsrechner ist auch nach seiner Bereinigung, nicht mehr als vertrauenswürdig zu betrachten.

IT-Analytiker versuchen den Begriff »Virus« zu vermeiden und bevorzugen **Malware**, Threat, usw. Der Grund dafür ist, dass ein Virus eine bestimmte Art von Malware ist, die ein bestimmtes Verhalten zeigt: Sie infiziert saubere Dateien. Untereinander beziehen sich Analysten auf einen Virus mit dem Begriff **Infektor**.

Bootviren, Bootsekturviren: Bootviren oder Bootsekturviren verbreiten sich nicht über Programme, sondern über externe Datenträger. Sie infizieren den Startbereich eines Datenträgers. Beim Booten (Starten) des Rechners von einem infizierten Datenträger oder Festplatte lädt sich der Bootvirus unbemerkt in den Speicher.

Trojanische Pferde: Der Sage nach belagerte Odysseus mit dem Athener Heer die Stadt Troja. Mit einem Trick schmuggelte er seine griechischen Soldaten im Innern eines als Geschenk getarnten Holzpferdes in die Stadt. Ähnlich die Viren-Trojaner: Die Programme geben

vor, bestimmte Funktionen auszuführen (z.B. Entpacken von Programmen, Systemtuning, ...), in Wahrheit wird eine Schadensfunktion wie z.B. das Ausspähen und Versenden von Passwörtern ausgeführt. Trojaner können auch eingebaute Kameras und Mikrofone heimlich aktivieren, was sie für staatliche Überwachungsorganisationen vieler Länder interessant macht.

Polymorphe Viren: Antivirenprogramme erkennen Viren unter anderem anhand typischer Bytefolgen. Polymorphe Viren verändern ihren eigenen Programmcode bei jeder neuen Infektion, dadurch wird die Erkennung wesentlich erschwert.

Makro-Viren: Makroviren (benötigen einen Interpreter) befallen nicht Programme, sondern Dokumente! Sie verstecken sich in Word- oder Excel-Dokumenten (Endungen DOCX bzw. XLSX) oder in Dokumentvorlagen (Endung DOT). Sie werden durch das Öffnen des befallenen Dokuments aktiv. Da die dazugehörigen Programme Word bzw. Excel sehr weit verbreitet sind und außerdem für verschiedene Betriebssysteme zur Verfügung stehen, kommt dieser Virenart in letzter Zeit eine große Bedeutung zu. Für etwa 80% aller Schadensmeldungen sind Makro-Viren verantwortlich, obwohl sie zahlenmäßig nur etwa 13% aller bekannten Viren umfassen.

Würmer: Als Würmer werden Viren bezeichnet, die sich **selbständig in Rechnernetzen ausbreiten**. Ihre massenhafte Verbreitung hat wesentlich mit der zunehmenden Vernetzung von Rechnern sowohl innerhalb einer Firma als auch über das Internet zu tun. Bevorzugter Ausbreitungsmechanismus sind dabei Email-Anhänge. Werden die Anhänge sorglos geöffnet, kann sich der Virus im System einnisten. Danach verschickt er sich, vom Anwender unbemerkt, selbständig weiter.

In der Vergangenheit mussten mehrere große Firmen (auch Microsoft) ihre Email-Server schon öfter vom Netz trennen, da sie die lawinenartige Zunahme an automatisch verschickten Emails nicht verkrafteten.

Stealth-Viren, Tarnkappenviren: Tarnkappenviren oder auch Stealth-Viren sind Viren mit speziellen Mechanismen, sich vor Virenprogrammen zu verstecken. Sie können z.B. eine infizierte Datei vor der Überprüfung restaurieren und somit die

Verseuchung unkenntlich machen. Oder anders: sie versuchen sich, durch die Ausgabe der ursprünglichen statt der aktuellen Dateigröße, einer Entdeckung durch den Virenschanner zu entziehen. Eine andere Strategie: Greift z.B. ein Antivirenprogramm auf die Datei zu, so entfernt sich der Virus zeitweilig und infiziert die Datei im Anschluss an die Prüfung erneut.

Skriptviren: Ein Skript ist ein Programm, welches nicht durch einen Kompilierer in Maschinensprache übersetzt wird, sondern durch einen Interpreter Schritt für Schritt ausgeführt wird. Ein Skript wird häufig auf Webservern verwendet (z.B. Perl oder PHP) bzw. durch in Webseiten eingebettete Skriptsprachen (z.B. JavaScript).

Banking-Trojaner: Banking-Trojaner verstecken sich und tun alles, damit die Benutzer nichts bemerken. Im Verborgenen warten sie darauf, dass die Benutzer ihren Kontostand abrufen. Erst dann reagieren die Schadprogramme und versuchen, auf unterschiedlichste Art einzugreifen. Beispielsweise ändern einige die Überweisungsdaten im Arbeitsspeicher, nachdem der Nutzer auf »Abschicken« geklickt hat, aber bevor die Daten übermittelt werden.

Ransomware oder Kryptotrojaner

Ransomware sperrt Benutzer aus ihrem eigenen Computer oder von bestimmten Dateien aus und verlangt zur Freigabe ein Lösegeld (**siehe auch:** <https://www.nomoreransom.org/de/>). **Hinweis:** Ransomware reist per E-Mail zum Opfer.

Verschlüsselnde Ransomware: Diese Art bedient sich Verschlüsselungsmethoden, um Dateien bis zur Zahlung des Lösegelds (meist um die 100 \$) unzugänglich zu machen. 2013 tauchte eine neue Variante namens Cryptolocker auf, die alle privaten und beruflichen Dateien verschlüsselt und sie erst nach Begleichen einer Gebühr in Höhe von 300 \$ wieder entschlüsselt. Die Verschlüsselung ist dabei so komplex, dass dem Opfer nichts anderes übrig bleibt, als das Lösegeld zu begleichen – oder eine komplette Neuaufsetzung des Systems vorzunehmen.

Nicht verschlüsselnde Ransomware: Hier gibt es verschiedene Varianten, um von den Benutzern Lösegeld zu erpressen. Eine Variante zeigt eine

gefälschte Windows-Aktivierungsnachricht und eine Zahlungsoption an. Eine andere, noch arglistigere Version sperrt den Benutzer nicht nur aus, sondern zeigt auch eine gefälschte Meldung an, die vorgibt, von einer Strafverfolgungsbehörde zu stammen, und die Zahlung eines Bußgelds wegen des Besitzes illegaler Software oder Kinderpornografie einfordert. Diese neueren Ransomware-Varianten unternehmen große Anstrengungen, um seriös zu erscheinen, und sind in unterschiedlichsten Sprachen erhältlich, um möglichst viele Opfer zu erreichen. **Hinweis:** Ransomware kann sich selbstständig, wurmartig über IT-Schwachstellen (SMB) verbreiten. Smartphones mit dem Android-OS erhalten oft einen Sperrbildschirm.

Payload: Payload bezeichnet die eigentlichen Nutzdaten (Programme, Daten, Malware, ...), die innerhalb eines Paketes oder eine anderen Übertragungseinheit, übertragen werden.

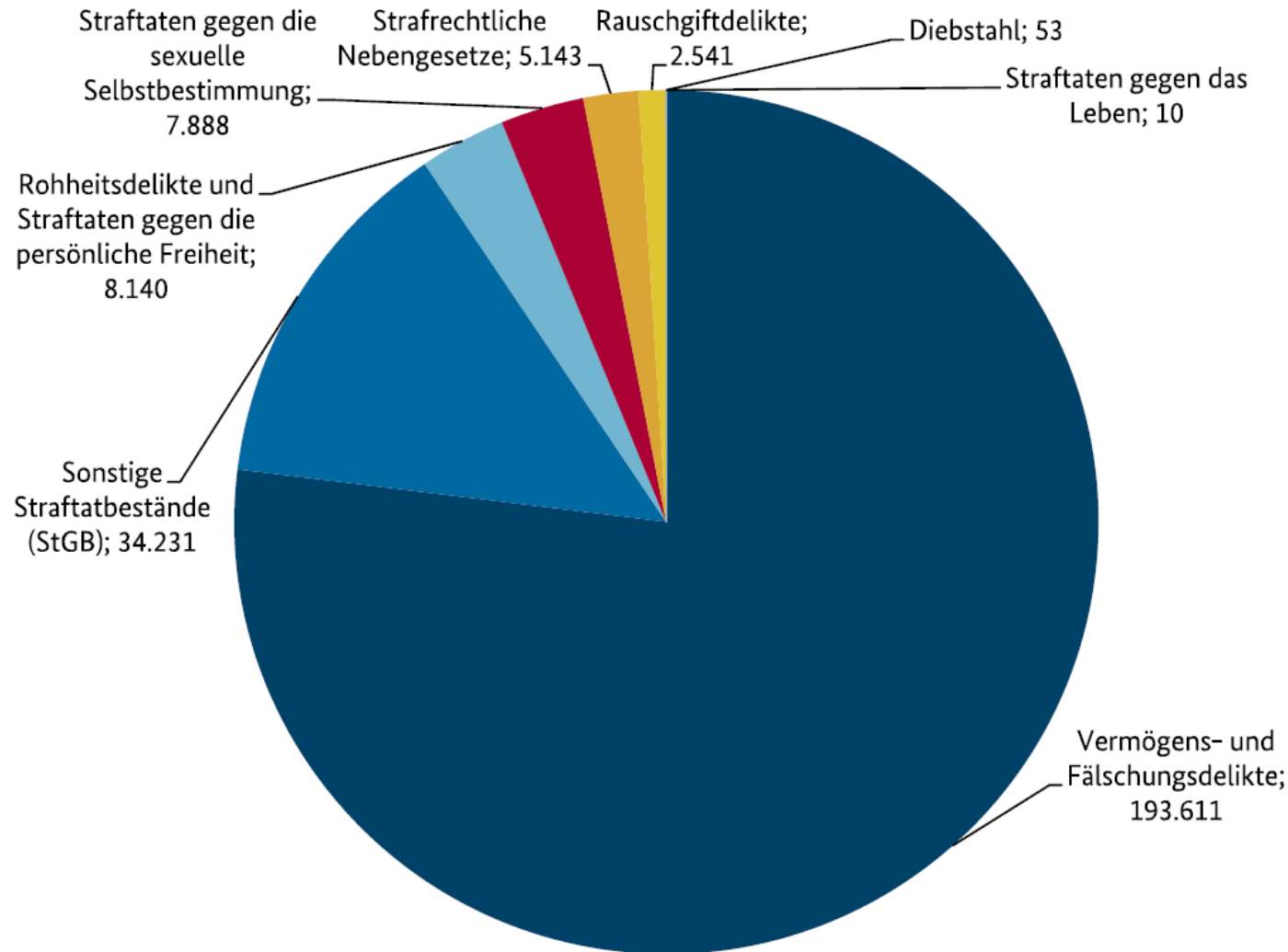
Signaturen: Als Signaturen werden heutzutage alle Einträge in einer Antivirusdatenbank bezeichnet.

Threat: engl.: Drohung, Bedrohung, Gefahr

APT: Ein APT (Advanced Persistent Threat) ist ein zielgerichteter Angriff auf ein Firmen-Netzwerk, bei dem eine unautorisierte Person so lange wie möglich unentdeckt bleibt.

PUA: potentiell unerwünschte Anwendungen (Werbung, Ausspähung, Spionage)

Tatmittel Internet – Verteilung nach Deliktsbereichen (2017)



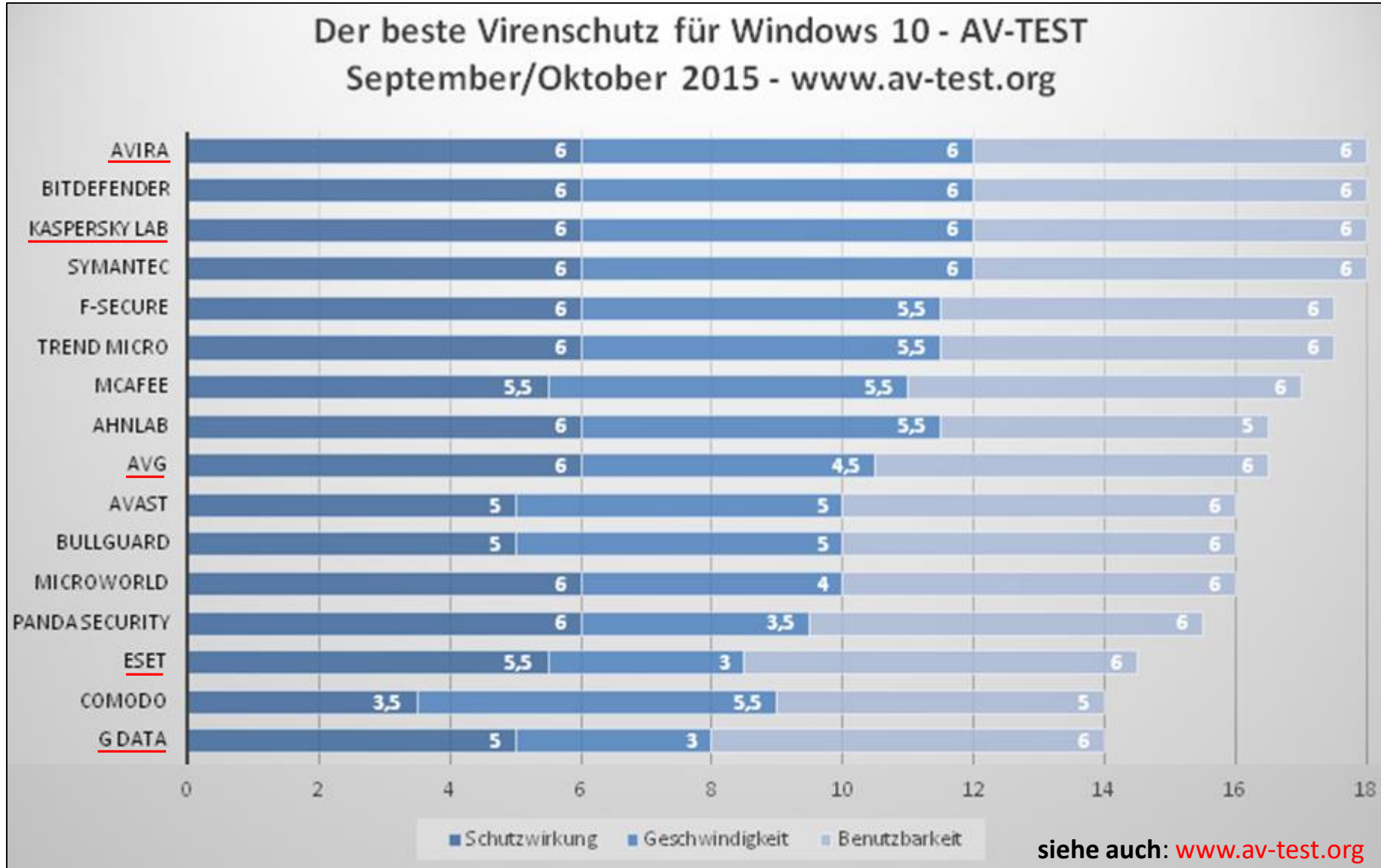
In 74,4 % der in 2017 erfassten Fälle handelte es sich um Betrug. Darunter waren vor allem Fälle von Waren- und Warenkreditbetrug, bei denen Tatverdächtige über das Internet Waren zum Verkauf anboten, diese jedoch entweder nicht oder in minderwertiger Qualität lieferten oder Tatverdächtige die Waren bestellten und nicht bezahlten.

Digitale Erpressung mittels Ransomware ist ein in Deutschland häufig auftretendes Phänomen. Neben Unternehmen sind auch Privatpersonen zunehmend von Erpressungssoftware (Forderungssummen: durchschnittlich 400 €, meist 100 bis 300 €) betroffen.

Die Polizei empfiehlt, keine Zahlung an Erpresser zu leisten. Auf der Webseite www.nomoreransom.org gibt es Empfehlungen was zu tun ist (Informationen, kostenlose Software zur Entschlüsselung der Daten).

Beim Einsatz von Ransomware handelt es sich strafrechtlich betrachtet um eine Kombination der Delikte Computersabotage gemäß § 303b StGB und Erpressung gemäß § 253 StGB.

Virenschutz-Programme



siehe auch: <https://www.besterantivirusprogramm.com/anti-malware-kostenlos>

Auswahl von Schutzsoftware:

Die Preise für Schutzsoftware für den einzelnen Rechner bewegen sich zwischen 20 € bis 50 €. Professionelle Firmenlösungen bekommt man ab 6.000 € aufwärts. Dabei sollten nur die Gesamtkosten pro Jahr betrachtet werden (undurchsichtige Preispolitik).

Schutzsoftware mit einer Erkennungsrate von 100 % gibt es nicht.

Kriterien:

- Bedienbarkeit
- guter Support (Transparenz, schnelle Reaktion)
- unauffällige Arbeit im Hintergrund
- verständliches Handbuch

Phishing



Phishing: Phishing sind ungezielte Angriffe, Betrugsversuche auf Personen, Unternehmen und Organisationen.

Spearfishing: Spearfishing-Angriffe sind gezielte Angriffe, Betrugsversuche auf Personen, Unternehmen und Organisationen.

Um in den Besitz personenbezogener Informationen (digitale Identität) zu gelangen, setzen Täter verschiedene Arten von Malware (Spyware, Trojaner, Keylogger), häufig aber auch Phishing-Mails ein.

Hierzu werden die gestohlenen Identitäten mittels der eingesetzten Malware an spezielle Speicherorte im Internet, auf welche die Täter bzw. deren Auftraggeber zugreifen können, weitergeleitet. Beim Einsatz von Phishing werden die Geschädigten zur Eingabe der relevanten Informationen auf täterseitig kontrollierte Server verleitet.

Seit 2014 lässt sich ein rückläufiger Trend bei den **gemeldeten** Fallzahlen von Phishing im **Online-Banking** feststellen.

Trotz der rückläufigen Entwicklung bleibt Phishing im Hinblick auf die vorhandenen Möglichkeiten und die zu erzielenden Erträge weiterhin ein lukratives und damit attraktives Betätigungsfeld für die Täterseite.

So betrug die durchschnittliche Schadenssumme (Phishing: Online-Banking) im Jahre 2017 rund 4.000 € pro Fall (Gesamt: 5,7 Millionen Euro).

Was ist Phishing?



Nie anklicken

**Nie darauf
antworten**

**Nie Daten
eingeben**



**Kein Email-
Anhang öffnen**

Drive-by-Downloads

Drive-by-Downloads

Ein Drive-by-Download (manipulierte Webseite oder eine E-Mail mit einem Schadlink) beschreibt einen Vorgang, bei dem schädlicher Webcode allein durch den Besuch einer Webseite ungewollt heruntergeladen wird. Der Drive-by-Download läuft automatisch ab, ohne dass der Nutzer es bemerkt.

Am häufigsten treten Drive-By-Downloads in Form unsichtbarer 0x0-Pixel-iFrames auf, die schädlichen JavaScript-Code enthalten. Dieses hochentwickelte JavaScript kann verschleiert werden oder polymorph sein (Code wird bei jedem Aufruf der Webseite geändert). Herkömmliche Antivirus-Lösungen auf Signaturbasis sind gegen solche Code-Tricks machtlos.

Sobald der Drive-By-Download den Browser erreicht hat, wird der ahnungslose Benutzer für ein Download eines Exploit-Kits umgeleitet.

In der nächsten Phase eines modernen Web-Angriffs erfolgt der Download eines Exploit- Kits von der Malware-Webseite. Exploit-Kits führen eine Vielzahl von Exploits (Ausnutzung von Schwachstellen in Webbrowsern) aus.

Sobald der Angreifer eine Anwendungsschwachstelle ausgenutzt und sich Kontrolle über das betreffende System verschafft hat, wird ein schädlicher Payload heruntergeladen und das System infiziert. Der Payload ist die eigentliche Malware oder der Virus, der letztendlich die Daten stiehlt, Dateien verschlüsselt, Benutzer aus ihren Computern auszusperrt oder Geld vom Benutzer erpresst (Ausführung des Angriffs).



Banking-Trojaner zielten in den letzten Jahren immer mehr und ganz direkt auf die Konten der Nutzer von Mobilgeräten. Offensichtlich profitieren die Malware-Entwickler von dem steigenden Trend, Kontobewegungen und Einkäufe immer öfter über Smartphone und Tablet, sowie entsprechende Apps zu erledigen.

Die Infizierung erfolgt gewöhnlich mittels Phishing-Mails mit angehängten Dokumenten, die sich vorgeblich auf geschäftliche Zwecke beziehen. Wenn Cyberkriminelle damit erfolgreich sind, erhalten sie vollen Fernzugriff und nutzen das, um den Datenaustausch zwischen Buchhaltungs- und Banking-Systemen durch ausgetauschte Dateien zu manipulieren – und somit finanzielle Transaktionen zu sich umleiten.

Bei Mac-Anwendern nahmen die Phishing-Aktivitäten im Finanzbereich etwas zu. Die Zahl der Android-Nutzer, die mit Android-Banking-Malware konfrontiert wurden, soll sich im Jahr 2018 sogar verdreifacht haben.

Was ist zu beachten?

Ihre Bank wird Sie niemals per Email zur Aktualisierung Ihrer Online-Daten auffordern, auch nicht per Telefon!

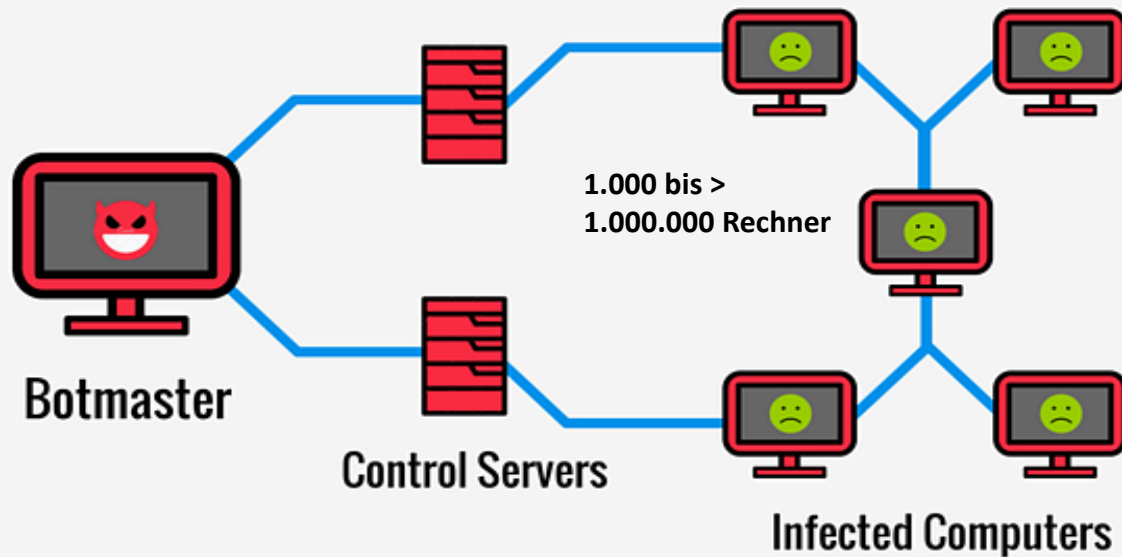
- Reagieren Sie nicht auf Phishing E-Mails und deren Anhänge bzw. SMS oder Anrufe.
- Nutzen Sie die »Zwei Faktor Authentifizierung«, wenn diese angeboten wird.
- Überprüfen Sie regelmäßig die Kontobewegungen bei Ihrer Bank.
- Betreiben Sie nur Online-Banking von eigenen Geräten bzw. von vertrauenswürdigen Geräten.
- Richten Sie sich Limits bei der Bank ein (Tages-, oder Dispo-Limits).
- Achten Sie bei der Eingabe ihres Logins beim Online-Banking darauf, dass Ihnen niemand über die Schulter schaut.
- Wenn Sie sich bei einer Email nicht sicher sind, kontaktieren Sie im Zweifel Ihre Bank.

Fazit: Anwender sollten die Professionalität moderner Cyberkrimineller keinesfalls unterschätzen und ihren Computer ungeschützt lassen.

Botnetze – massenhafte Fernsteuerung von Computern

Bei Botnetzen (Werbebetrug – Zahlung pro Klick, Verteilung von illegalen Materialien, DDoS-Angriffe, Spam-E-mails, Verbreitung von Malware) handelt es sich um zahlreiche, per Schadcode infizierte Systeme von Geschädigten, die ohne Wissen ihrer Besitzer über »Command & Control-Server« ferngesteuert werden. Die Installation der Schadsoftware erfolgt unterschiedlich, sei es durch Öffnung eines infizierten E-Mail-Anhangs oder auch mittels »Drive-by-Download-Infection«.

typische NetBot-Struktur



IoT-Botnetze: IoT-Malware (Internet of Things, Internet der Dinge) zwingt vor allen IP-Kameras und digitale Videorecorder in sein Botnetz, welches dann unter anderem für **DDoS-Attacken** eingesetzt wird.

Die 2016 über die IoT-Malware Mirai geführten Attacken verknüpften zeitweise über 500.000 infizierte IP-Kameras und digitale Videorecorder zu einem der bisher größten Botnetze der Welt.

Über **Distributed-Denial-of-Service-Attacken** wurden dabei weite Teile des Internets lahmgelegt.

Drei amerikanische Studenten hatten die Malware ursprünglich entwickelt, um die Server konkurrierender Minecraft-Spieler aus dem Netz zu schießen. Später wurde das per Mirai erzeugte Botnetz für DDoS-Erpressungen gegen große Provider und Dienstleister genutzt.

Hinweis: Botnetze können gegen Bezahlung für einen vereinbarten Zeitraum gemietet werden (Darknet, 5-400 €).

Kryptominer oder Coinminer 1/2

Zeitalter der Kryptominer bricht an

Und tatsächlich bietet sich Kriminellen dank des Booms von Krypto-Währungen wie Bitcoin, Litecoin und Ethereum seit einigen Jahren ein neues, wirtschaftlich extrem attraktives und zukunftstaugliches Geschäftsmodell.

Und so verwundert es nicht, dass die Anzahl von **Schadprogrammen (mit CPU-Management), die heimlich die Leistung infizierter Geräte zum Errechnen digitaler Währung missbrauchen**, explosionsartig angestiegen ist.

Von den über 4.500 existierenden Krypto-Währungen, werden jedoch etwa nur 1.000 wirklich gehandelt. Als Startwährung mit der mit Abstand größten Marktkapitalisierung stehen große Bitcoin-Summen beim Wechsel in wahre Münze allerdings unter besonderer Beobachtung. Mit 153.225 Mio. US-Dollar macht die bekannteste digitale Währung derzeit über 37 Prozent des Gesamtvolumens aller aktuellen Krypto-Währungen aus.

Kriminelle verwenden darum andere, weniger beobachtete Cyber-Währungen mit weiter Verbreitung wie Litecoin, Ethereum, EOS, Tronix und Monero. Auch diese folgen dem Grundsatz der anonymen Finanzabwicklung.



Digitale Währungen sind virtuelle Geldeinheiten, deren Herstellung und Verwendung auf mathematische Berechnungen und kryptografischen Verfahren beruhen.

Stehlen oder Minen

Prinzipiell gibt es für Kriminelle zwei Wege, an die digitale Währung zu gelangen. Der erste besteht darin, fremde Rechner nach gespeicherten Coins zu durchsuchen und diese zu stehlen. Das Guthaben einer Krypto-Währung besteht ausschließlich aus einem entsprechenden Zahlencode. Der gibt Auskunft über die Anzahl der Coins innerhalb des Systems einer Krypto-Währung. Solche Zahlencodes können als geheimer privater Schlüssel gespeichert, aber beispielsweise auch in Strichcode übersetzt und ausgedruckt werden. Damit sind die Schlüssel für die Verfügung über ein Guthaben allerdings auch leicht aufzuspürende Beute für Computerkriminelle.

Kryptominer oder Coinminer 2/2

Sie lassen sich ähnlich wie Passwörter mit Schadprogrammen ausspähen und abgreifen. Attacken sind wegen der geringen Verbreitung allerdings nur lohnend, wenn das Opfer bekannt ist, gezielt angegriffen werden kann und über eine ausreichende Menge schlecht geschützter Coins verfügt. Denn solch gezielte Angriffe erfordern einiges an Planung und sind entsprechend aufwendig.

Der zweite Weg, auf Kosten anderer an Krypto-Währung zu gelangen, erfordert einen deutlich geringeren Aufwand und ist darum deutlich lukrativer: das Mining von Krypto-Währung durch den **Missbrauch fremder Rechenressourcen**. Die Rechenleistung fremder Hardware wird eingesetzt, um innerhalb der Krypto-Blockchain (Distributed Ledger Technology, dezentral, geführtes digitales Buchführungssystem, Ledger ... Hauptbuch, Kassenbuch) kryptographische Aufgaben zu lösen. Als »Belohnung« für das richtige Ergebnis gibt die entsprechende Blockchain Anteile der in ihr vordefinierten Währung aus.

Jede Krypto-Währung ist ein in sich geschlossenes System mit einer vorher festgelegten Coin-Menge und einem festgelegten Gesamtwert. Mit jedem Coin, der innerhalb eines solchen Währungssystems geschürft wird, steigt jedoch die Komplexität der Rechenaufgaben und somit die notwendige Rechenleistung.



Nutzer können Pools bilden und die Rechenleistung ihrer Hardware koppeln, um gemeinsam zu schürfen. Teils wird aber auch in Grauzonen agiert, indem die Mining-Funktion zum Beispiel in kostenlosen Applikationen für Smartphones und Tablet-PCs versteckt wird. Auch Browser-Addons, mit denen Betreiber von Onlinediensten ihre Nutzer während der Verweilzeit auf der Website für sich schürfen lassen, finden zunehmend Verbreitung.

Und genau hier setzen auch die Cyberkriminellen an: Anstatt die Cyberwährung von ihren Opfern über Ransomware zu erpressen, gingen sie ab dem 4. Quartal 2017 zunehmend dazu über, die **Rechenleistung infizierter Hardware (Rechner, Smartphones, IoT-Geräte, IoT ... Internet of Things) zum Coinmining zu missbrauchen**.

Cyber-Attacke auf das EU-Land Estland



Die Internetangriffe auf Estland begannen am **26. April 2007** und hielten mehrere Wochen an. Sie richteten sich gegen staatliche Organe, darunter das estnische Parlament, den Staatspräsidenten sowie diverse Ministerien, Banken und Medien.

Die Attacken waren vorwiegend **Denial of Service-Angriffe** unter Verwendung eines **Botnetzes** und sorgten für einen zeitweisen Ausfall vieler nationaler Internetdienste. Ziele waren Websites von Regierung und Parlament, sowie diverser Medien und Banken. Dadurch wurde teilweise auch der Geschäftsverkehr beeinträchtigt, insbesondere im Bereich Online-Banking. Die gravierenden Folgen sind der weitgehenden Digitalisierung und dem technologisch modernen Verwaltungssystem geschuldet. Jeder Bürger besitzt eine ID-Nummer. Seit 2007 können Esten über das Internet an Wahlen teilnehmen, ihre Steuern abrechnen und Rezepte vom Arzt empfangen. Im Jahr 2008 wurde ein russischstämmiger estnischer Staatsbürger angeklagt und verurteilt. Im März 2009 bekannte sich Konstantin Goloskokow, ein Funktionär der regierungsnahen russischen Jugendorganisation Naschi, als Drahtzieher zu den Angriffen.

Wegen der Verwundbarkeit durch Cyber-Angriffe wurden Backupserver in Luxemburg eingerichtet. Sie enthalten die digitale Verwaltungssoftware Estlands und die Datensätze der Bürger. Die Internetangriffe des Jahres 2007 waren der Anlass zu diesen Maßnahmen sowie zur der Einrichtung von Cyberkriegsforschungszentren in Estland, an denen auch die NATO beteiligt ist.



Video des Bundesamt
für Bevölkerungsschutz
und Katastrophenhilfe
(BBK)

3 Fragen an...



BBK. Gemeinsam handeln. Sicher leben.

- ✓ Die beste »Schutzsoftware« ist das eigene Verhalten.
- ✓ Einen 100 prozentigen Schutz gegen professionelle Malware gibt es nicht.
- ✓ Ein gezielter Angriff auf einen Rechner durch Profis gelingt immer - früher oder später.





Vielen Dank für ihre Aufmerksamkeit

Fragen?