

Informationssicherheit

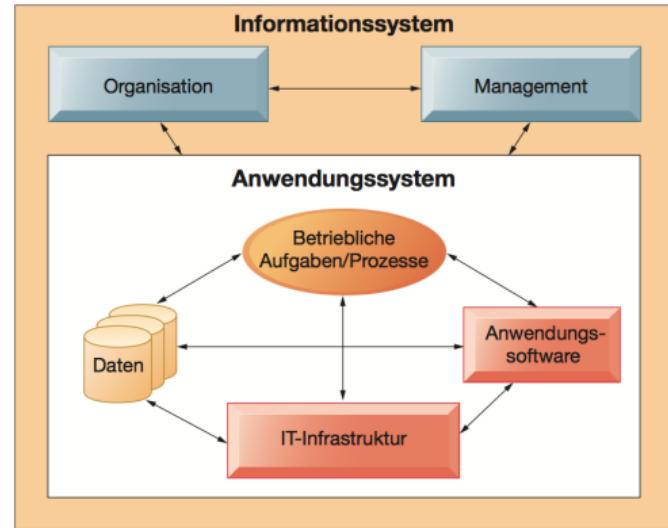
5. Systemsicherheit

Prof. Dr. Christoph Skornia

christoph.skornia@oth-regensburg.de

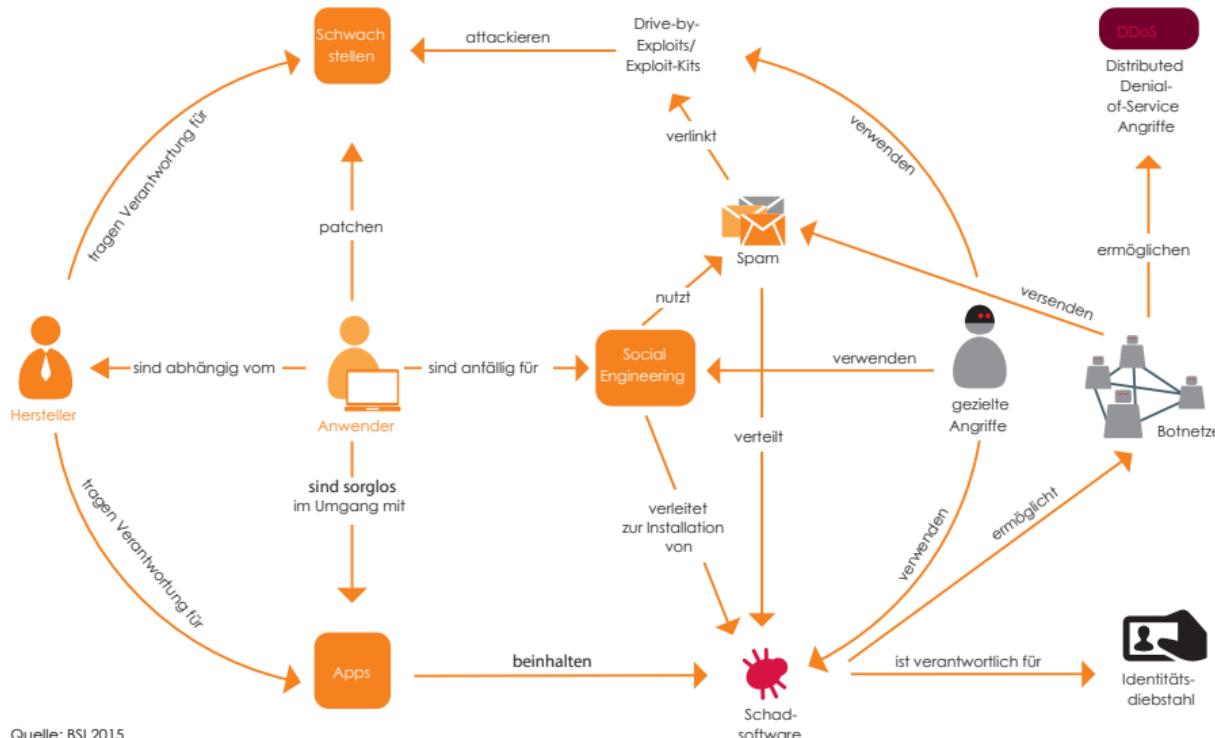
Aspekte der IT-Systemsicherheit:

- Analyse von möglichen Angriffsvektoren
 - Ausnutzung von Schwachstellen
 - Kombination verschiedener Bereiche von Schwachstellen
- Analyse der Ausbreitung von Angriffen
 - Infektionswege
 - Epidemiologie
- Analyse von Schadenszenarien
 - Einschätzung der Schadenshöhe
 - Identifikation von verborgenen Schäden und aktuell laufenden Angriffen



- Entwicklung von Abwehrmaßnahmen
 - Proaktive Mechanismen
 - Reaktive Mechanismen
 - Prophylaxe

Systemsicherheit Überblick



Quelle: BSI 2015

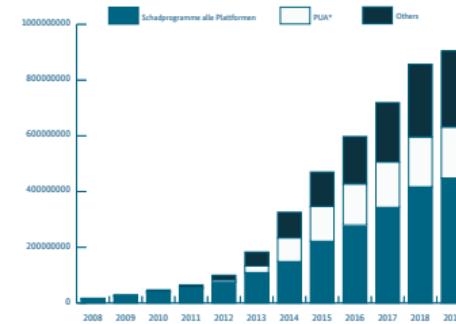
Systemsicherheit Überblick

Cyber-Sicherheitslage 2019

Aktion und Reaktion

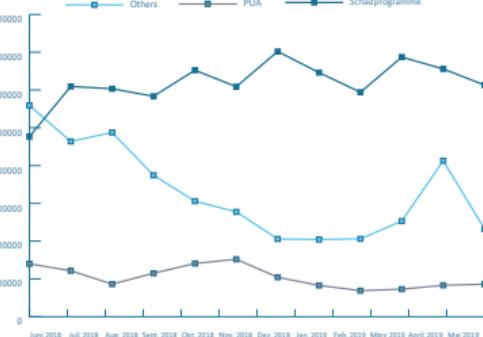


Systemsicherheit Überblick



Known Malware-Variants in total, Source: AV-Test

Quelle: BSI 2019



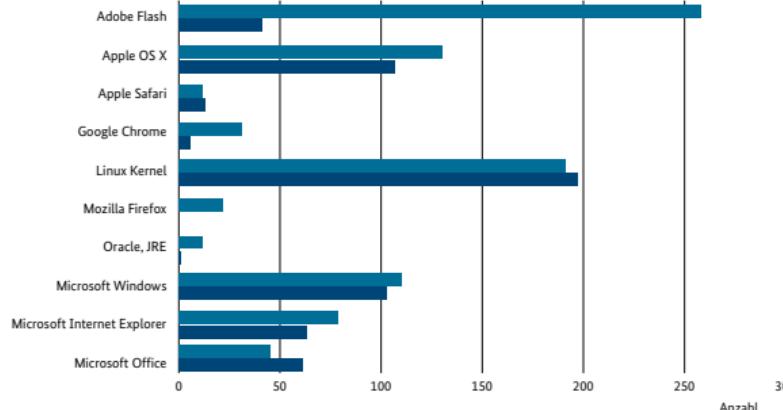
Development of new malware variants per month

*PUA: Potentially unwanted application. Bezeichnet Anwendungssoftware (oft als „Bundled“-Software vertrieben), die nicht eindeutig als Malware klassifiziert werden kann und daher unter dem Begriff „grayware“ subsumiert wird. PUA zeichnet sich insbesondere dadurch aus, dass sie z. B. vom Anwender zwar installiert wurde, jedoch ggf. nicht das erwartete Verhalten zeigt oder verdeckt Funktionen ausführt, die als „un erwünscht“ angesehen werden, z. B. Informationsammlung und ggf. Weiterleitung des Anwenderverhaltens, Einblendung von Werbung etc.

**Andere: u. a. betriebssystem-unabhängige Skripte, maliziöse Dokumente, Java-Malware usw.

***Schadprogramme: Betriebssystemabhängige Malware

Quelle: BSI 2019



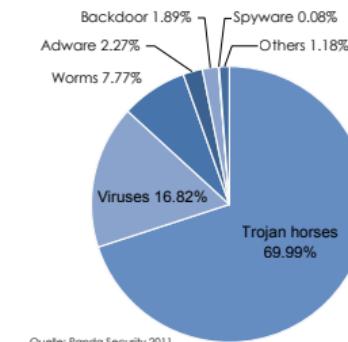
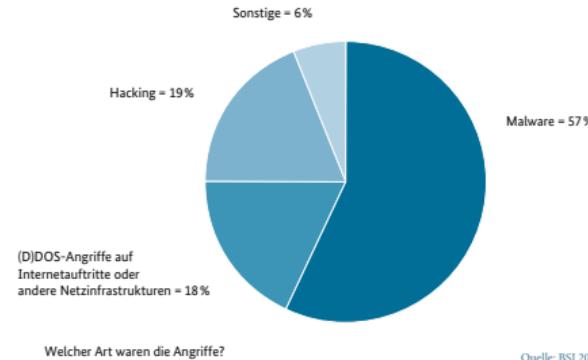
Critical CVE Entries, Stand: 31.03.2018

Quelle: BSI 2018

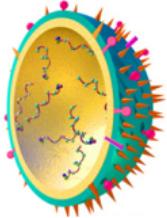
Zentrale Komponente: Malware

Malware (*Malicious Software*):

- Software, die Systemschwachstellen ausnutzt
- zentrale Komponente der überwiegenden Mehrzahl von Angriffen
- hochentwickelte Technologie
- verschiedenste Verbreitungswege
- de facto für jedes System vorhanden



Malware: Die wichtigsten Typen



Merkmale eines **Virus**:

- Ausführbarer Code, der sich in anderes Programme einnistet
- Beinhaltet Infektions- und Schadteil
- Nur aktiv, wenn der Wirt aktiv
- Ausbreitung in Netzwerken „nur“ durch Austausch infizierter Dateien.



Allgemeine Struktur

```
PROCEDURE Virus;  
BEGIN  
  4711  
  
  suche eine nicht infizierte erste Zeile  
  Programdatei; ≠ 4711  
  IF (gesundes Programm gefunden)  
  THEN kopiere Virus in das Programm;  
  
  Auslöser  
  IF (Datum = Freitag der 13.)  
  THEN formatiere Festplatte;  
  
  springe an den Anfang des Wirtsprogramms;  
END.
```

Beispiel

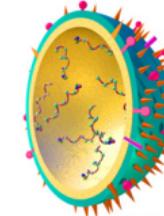
Malware: Die wichtigsten Typen

Infektion:

Allgemeines Format Bsp Programm

| | |
|--------------------------------|--------------------------|
| Name der Datei | Spiel_X |
| Länge der Datei | 13200 |
| Einsprungadresse des Programms | 4500 |
| Programmcode | Load JSB 1 |

vor der Infektion



Malware: Die wichtigsten Typen

Infektion:

Allgemeines Format Bsp Programm

| | |
|--------------------------------|--------------------------|
| Name der Datei | Spiel_X |
| Länge der Datei | 13200 |
| Einsprungadresse des Programms | 4500 |
| Programmcode | Load JSB 1 |

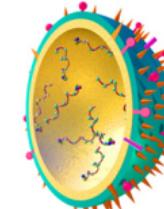
vor der Infektion

Allgemeines Format Bsp Programm

| | |
|------------------------------------|----------------------|
| Name der Datei | Spiel_X |
| neue Gesamtlänge der Datei | 13840 |
| neue Einsprungadresse in den Virus | 18000 |
| Programmcode | Load ... JSB 1 |

Viruscode:
Kennung
...
Sprung

nach der Infektion



Malware: Die wichtigsten Typen

Infektion:

Allgemeines Format Bsp Programm

| | |
|--------------------------------|--------------------------|
| Name der Datei | Spiel_X |
| Länge der Datei | 13200 |
| Einsprungadresse des Programms | 4500 |
| Programmcode | Load JSB 1 |

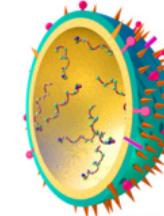
vor der Infektion

Allgemeines Format Bsp Programm

| | |
|------------------------------------|----------------------|
| Name der Datei | Spiel_X |
| neue Gesamtlänge der Datei | 13840 |
| neue Einsprungadresse in den Virus | 18000 |
| Programmcode | Load ... JSB 1 |

Viruscode:
Kennung
...
Sprung

nach der Infektion

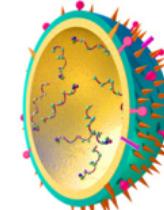


Vorsicht:
Infizierter Bootsektor

| | |
|--------------|--|
| Virus Code | Lade Virus (resident) Virus-Kennung ... |
| Bootprogramm | Lade Betriebssystem Lade Treiber Lade Konfigurationsdaten ... |

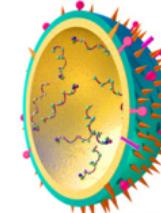
2. Generation von Viren:

- Gezielter Befall von Addons, Plugins und Interpretern
- Virenbefall als Vorbereitung des eigentlichen Angriffs
z.B. befallener PDF-Interpreter wartet auf Dokument,
welches dann die spezifischen Befehle zum Angriff
enthält



2. Generation von Viren:

- Gezielter Befall von Addons, Plugins und Interpretern
- Virenbefall als Vorbereitung des eigentlichen Angriffs
z.B. befallener PDF-Interpreter wartet auf Dokument,
welches dann die spezifischen Befehle zum Angriff
enthält

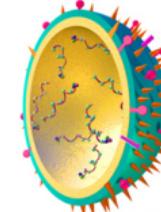


Makro- oder Datenviren:

- Makros sind in Dokumente eingebettet
Code-Bestandteile (z.B. in Word oder Excel)
- Makros werden in einer Makrosprache (z.B. VBA)
formuliert und dann interpretiert
- Lesender Zugriff auf nur ein verseuchtes Dokument
kann eine Infektion auslösen

2. Generation von Viren:

- Gezielter Befall von Addons, Plugins und Interpretern
- Virenbefall als Vorbereitung des eigentlichen Angriffs z.B. befallener PDF-Interpreter wartet auf Dokument, welches dann die spezifischen Befehle zum Angriff enthält



Makro- oder Datenviren:

- Makros sind in Dokumente eingebettet Code-Bestandteile (z.B. in Word oder Excel)
- Makros werden in einer Makrosprache (z.B. VBA) formuliert und dann interpretiert
- Lesender Zugriff auf nur ein verseuchtes Dokument kann eine Infektion auslösen

ani-Viren (Variante von Datenviren):

- verseuchte Dokumente, welche eine Schwachstelle in einem Interpreter ausnutzen
- Auch in Dateien, die selbst keinen ausführbaren Code beeinhalten
- Android Stagefright nutzt z.B. eine Buffer-Overflow Schwachstelle im Preprocessing von MMS-Nachrichten

Würmer

- selbstständig lauffähiges Programm**
- Fähigkeit zur Reproduktion.**
- Infektions- und Schadteil (wie bei Viren)**
- verbreitet sich aktiv selbst z.B. über:**
 - Versand von e-mail mit sich selbst als Anhang
 - Ausnutzen von Schwachstellen in Serverdiensten
- Mischformen zwischen Viren und Würmern**



Malware: Die wichtigsten Typen

Würmer

- selbsständig lauffähiges Programm
- Fähigkeit zur Reproduktion.
- Infektions- und Schadteil (wie bei Viren)
- verbreitet sich aktiv selbst z.B. über:
 - Versand von e-mail mit sich selbst als Anhang
 - Ausnutzen von Schwachstellen in Serverdiensten
- Mischformen zwischen Viren und Würmern



Trojanische Pferde

- Schadprogramm oder Code, welches sich als ordnungsgemäßes Programm tarnt
- Installiert häufig wirklichen Schadcode nach z.B.:
 - Backdoors
 - Spionagesoftware
 - etc.
- Trend: „Brückenkopftrojaner“ d.h. minimaler Footprint, jegliche relevante Funktion wird nachgeladen



Malware: Die wichtigsten Typen

Würmer

- selbsständig lauffähiges Programm
- Fähigkeit zur Reproduktion.
- Infektions- und Schadteil (wie bei Viren)
- verbreitet sich aktiv selbst z.B. über:
 - Versand von e-mail mit sich selbst als Anhang
 - Ausnutzen von Schwachstellen in Serverdiensten
- Mischformen zwischen Viren und Würmern



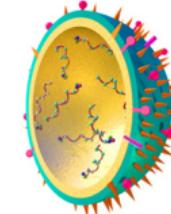
Trojanische Pferde

- Schadprogramm oder Code, welches sich als ordnungsgemäßes Programm tarnt
- Installiert häufig wirklichen Schadcode nach z.B.:
 - Backdoors
 - Spionagesoftware
 - etc.
- Trend: „Brückenkopftrojaner“ d.h. minimaler Footprint, jegliche relevante Funktion wird nachgeladen
- Trojaner sind eigentlich die Opfer des Pferdes... ☺**



Typische Malware-Infektionswege sind:

- Downloads von infizierten oder bösartigen Webseiten
- EMail
 - Spam
 - „Lustige Mails“, die aktiv selbst weitergeleitet werden.
- Eigene Verbreitungsmechanismen
- Soziale Netwerke (z.B. WhatsApp etc.)
- sonstige Schwachstellen (z.B. im Update Mechanismus)
- etc.



Rootkits

- Sammelbegriff für einen Satz an Werkzeugen (ursprünglich Unix-Welt)
- Ziele:**
 - Erlangung von Root- bzw. Administrationsrechten
 - Verbergen der eigenen Aktivität und eingeschleuster Malware
- Typen:**
 - App-Rootkit: Modifikation von Systemprogrammen
 - Kernel-Rootkit: Modifikation von Kernel-Mode Code (z.B. Treiber)
 - Userland-Rootkit: Modifikation von Usermode-Shared-Libs (z.B. Kapselung von Prozesskommunikation)
 - Speicher-Rootkits: Modifiziert „nur“ RAM von laufenden Prozessen
- Rootkit selbst muss keinen Schadteil enthalten, erstmal nur Werkzeug



Rootkits

- Sammelbegriff für einen Satz an Werkzeugen (ursprünglich Unix-Welt)
- Ziele:**
 - Erlangung von Root- bzw. Administrationsrechten
 - Verbergen der eigenen Aktivität und eingeschleuster Malware
- Typen:**
 - App-Rootkit: Modifikation von Systemprogrammen
 - Kernel-Rootkit: Modifikation von Kernel-Mode Code (z.B. Treiber)
 - Userland-Rootkit: Modifikation von Usermode-Shared-Libs (z.B. Kapselung von Prozesskommunikation)
 - Speicher-Rootkits: Modifiziert „nur“ RAM von laufenden Prozessen
- Rootkit selbst muss keinen Schadteil enthalten, erstmal nur Werkzeug
- Einmal erfolgreich eingeschleustes Rootkit → R.I.P**



Botnet:

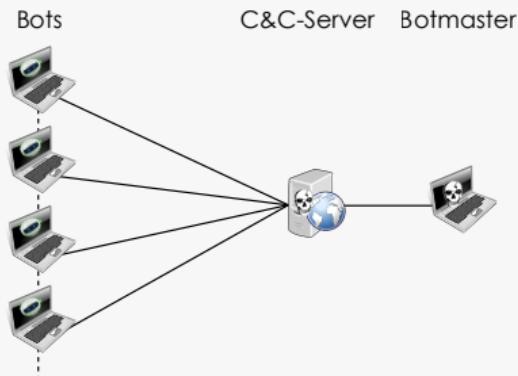
- Gruppe von Programmen welche auf Anweisung Befehle einer zentralen Instanz ausführen und auf einer vernetzten Gruppe von Rechnern laufen
- Illegales Botnet:** Bots werden ohne Wissen und Zustimmung der Eigentümer der Rechner installiert und für illegale Zwecke eingesetzt z.B.:
 - Versenden von Spam
 - *Distributed-Denial-Of-Service (DDOS)*-Angriffe
 - Proxy für illegale Inhalte
 - verteilter Datenspeicher für illegale Inhalte



Typen von Botnetzen

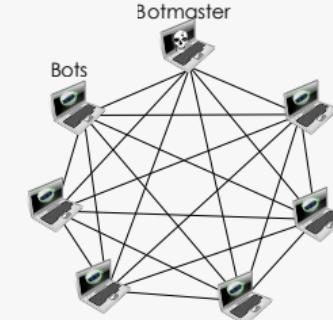
Klassisches Botnetz

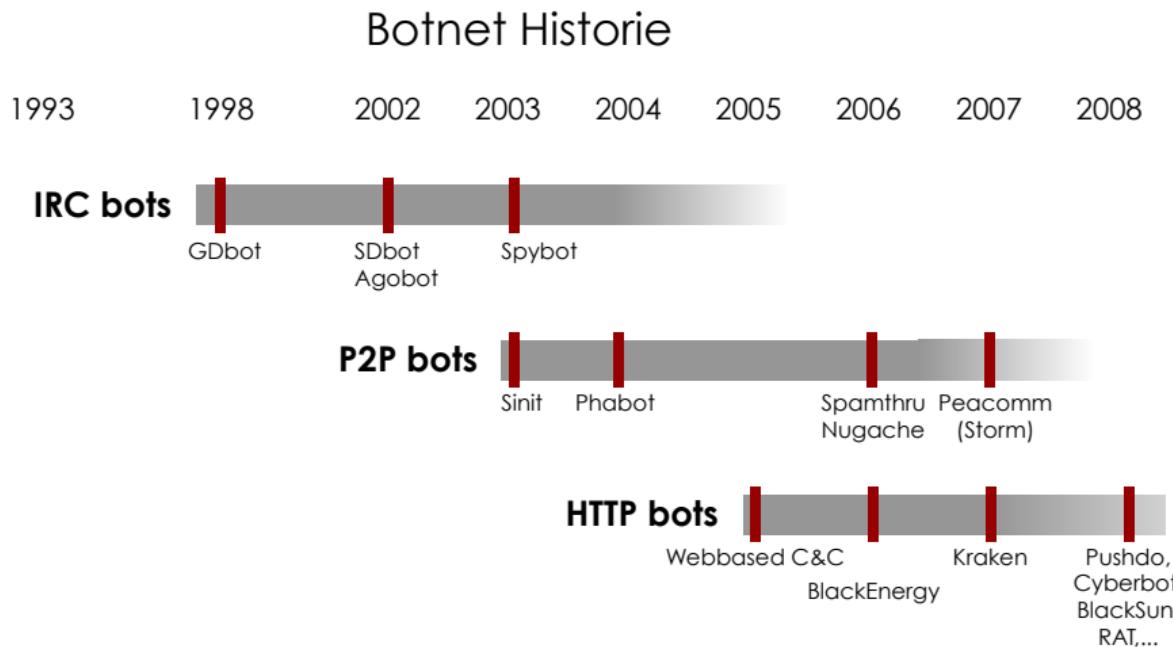
(mit Command & Control Server)



P2P Botnetz

(mit oder ohne C&C Server)





Zusammenfassung:

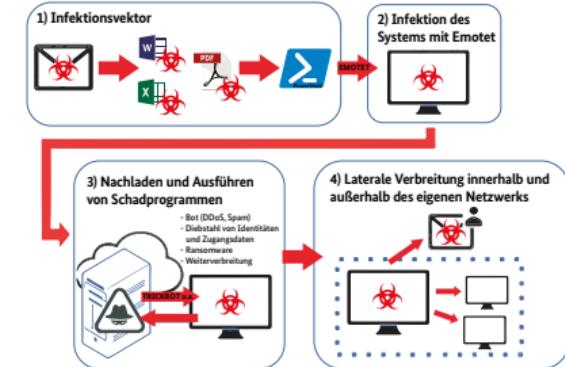
- Üblicher Einsatz in einem servicebasiertem Modell, d.h. der Angreifer mietet ein Botnetz für seine Zwecke, der Betreiber des Botnetzes ist „nur“ Serviceanbieter
- geschätzt jeder zehnte PC weltweit ist Teil eines Botnetzes
- Größte bekannte(!) Botnetze:
 - BredoLab, ca. 30 Mio. Mitglieder, seit Oktober 2010 abgeschaltet
 - Mariposa, ca. 10 Mio. Mitglieder, seit Dezember 2009 abgeschaltet
 - Conficker, ca. 9 Mio. Mitglieder
- Botnetze gelten als aktuell eines der drängendsten Probleme in der Informationssicherheit



Gezielte Angriffe und Industriespionage gewinnen an Bedeutung

- Beispiele: Stuxnet, RSA-Secure-ID Northdrop, Duqu, Flame, Mini-Duke
- Schema:

- 1 Erstelle einen Brückenkopftrojaner (z.B. Mini-Duke 20kB)
- 2 Nutze eine unbekannte Zero-Day-Lücke zur Verteilung
- 3 Lade spezialisierte Angriffe nach
- 4 Infiziere so viele Rechner der angegriffenen Instanz wie möglich
- 5 Spioniere die Infrastruktur aus



Grafiken: <https://www.fortinet.com/resources/icon-library.html>, Microsoft, Adobe

Quelle: BSI 2019

- Staaten und Geheimdienste operieren nach dem selben Muster
- Erfolgreiche Angriffe, welche über längere Zeit Daten extrahieren und nicht entdeckt werden nennt man **Advanced Persistant Threats APT**



Weitere Malwaretypen

Zoo der Schädlinge:

Zu den bislang besprochenen Typen gibt es noch eine ganze Reihe weiterer Schädlinge

- Spyware
- Adware
- Scareware
- Exploitkits
- Ransomware
- Keylogger
- etc. etc. etc.



In vielen Fällen ist ein Stück Malware auch verschiedenen Kategorien zuzuordnen.

Reaktive Mechanismen:

- ❑ Client
 - klassische VirensScanner
 - Prüfung von Systemdateien (z.B. Registry, MBR, etc.) auf Modifikation
- ❑ Server
 - Anti-Malware & Anti-Spam auf dem email-Server
 - Anti-Malware auf FileServern
 - Klassifizierung und Verbot von Downloads (z.B. über Proxy und Firewalls)

Proaktive Mechanismen:

- ❑ Windows
 - Application Whitelisting:
<http://technet.microsoft.com/en-us/library/bb457006.aspx>
 - Automatic Updates und Patching
 - Client-Firewall
- ❑ Unix
 - Partition mit ausführbarer Software read-only mounten
 - User-Partitionen nonexec mounten
- ❑ Problem:
 - Kein absoluter Schutz möglich

Weiterführende Mechanismen:

- Kontrolle von OS und HW außerhalb des eigentlichen Systems
- Definition von sicheren Zuständen und erlaubten Veränderungen
- OS-Hersteller behält die Kontrolle über das System
 - z.B. Trusted Computing, iOS, UEFI Boot etc.
 - Frage des Vertrauens in den Hersteller
 - Problem für die Privatheit des Benutzers
- Kryptographische Überprüfung ausführbarer Komponenten und Hardware-Schlüsselspeicher
- Komplett neue Betriebssysteme

Weiterführende Mechanismen:

- Kontrolle von OS und HW außerhalb des eigentlichen Systems
- Definition von sicheren Zuständen und erlaubten Veränderungen
- OS-Hersteller behält die Kontrolle über das System
 - z.B. Trusted Computing, iOS, UEFI Boot etc.
 - Frage des Vertrauens in den Hersteller
 - Problem für die Privatheit des Benutzers
- Kryptographische Überprüfung ausführbarer Komponenten und Hardware-Schlüsselspeicher
- Komplett neue Betriebssysteme

Problem: Kein absoluter Schutz möglich!!!

Verhalten bleibt ein wesentlicher Aspekt

Danke für Ihr Interesse

Fortsetzung folgt

