CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Motivation Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

02 Lage der IT-Sicherheit

Malware

Neue Malware-Varianten von Juni 2021 bis Mai 2022
Anzahl in Millionen

Abbildung 1:
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Malware

Durchschnittlicher täglicher Zuwachs neuer Malware-Varianten von Juni 2021 bis Mai 2022
Anzahl in Tausend

Abbildung 2:
Quelle: Malware-Statistik des BSI auf Basis von Rohdaten des Instituts AV-Test GmbH

Malware

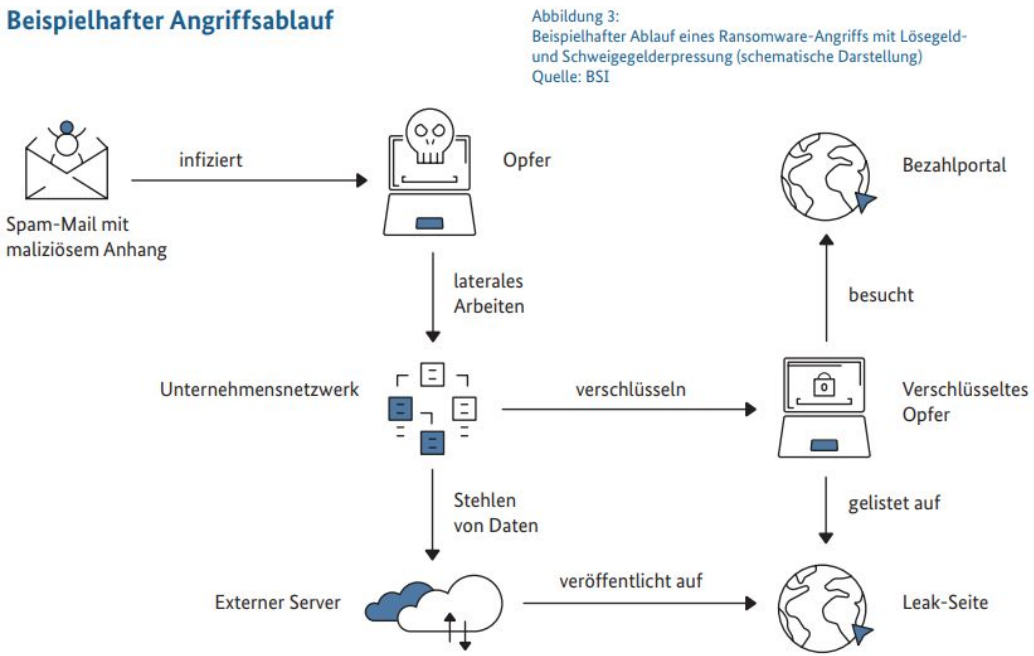
Ab wann gilt eine Malware-Variante als neu?

- Als neue Malware-Variante wird ein Schadprogramm bezeichnet, an dessen Programmcode Änderungen vorgenommen wurde. Also sprich, sobald der Hash-Wert sich ändert!

Warum stellt eine neue Variante ein höheres Risiko dar?

- Da durch die Abänderung des Codes etablierte Sicherheitsrichtlinien und Sicherheitsmechanismen umgangen werden können.

Malware


Beispielhafter Angriffsablauf
Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld- und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI
infiziert
Opfer
Bezahlportal
Spam-Mail mit maliziösem Anhang
laterales Arbeiten
besucht
Unternehmensnetzwerk
verschlüsseln
Verschlüsseltes Opfer
Stehlen von Daten
gelistet auf
Externer Server
veröffentlicht auf
Leak-Seite

Malware

Schweigegelderpressung

- Nachdem der Angreifer Zugriff auf relevante Daten erlangt hat, fordert er das Opfer auf, Betrag X zu zahlen, damit die Veröffentlichung der betriebsinternen, privaten oder kompromittierenden Inhalte, nicht erfolgt.

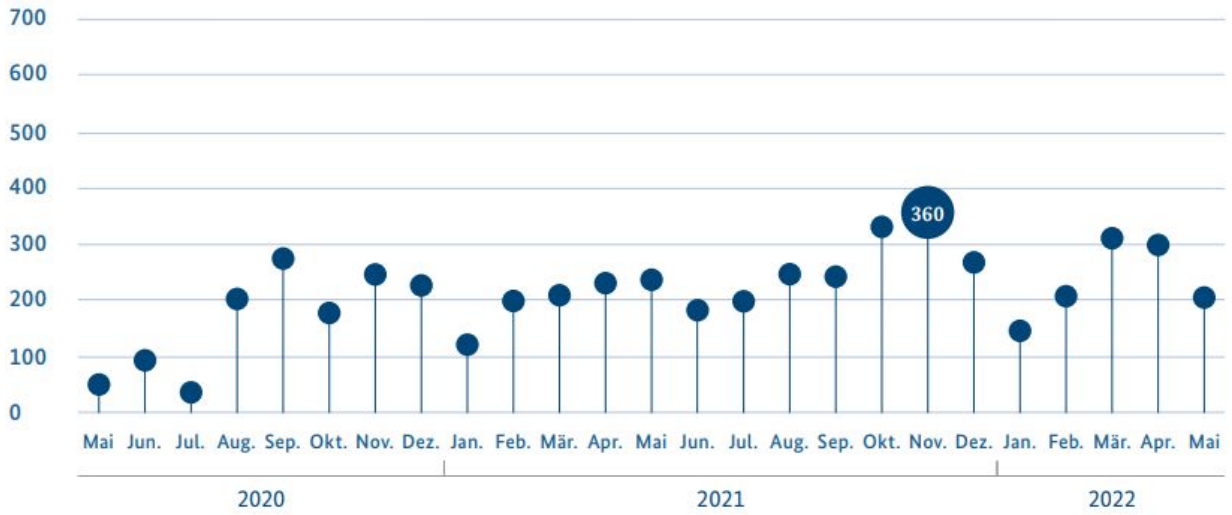
Lösegeld-Erpressung (Ransomware)

- Nach Verschlüsselung der relevanten Daten, fordert der Angreifer das Opfer auf, Betrag X zu zahlen. Nach Zahlung des Betrages soll das Opfer den benötigten kryptographischen Schlüssel zur Entschlüsselung der Dateien erhalten.

Malware

Entwicklung der Bedrohungslage
Victim Data Released on
Ransomware Extortion Site

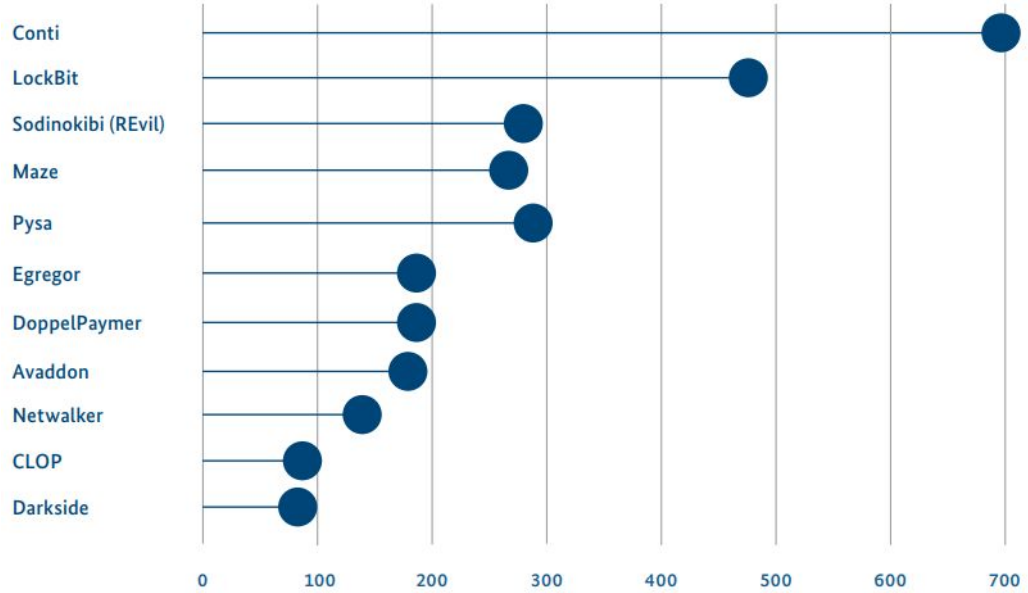
Abbildung 5:
Opfer von Daten-Leaks von Jan. 2020 bis Mai 2022
Quelle: The Record



Malware

Opfer von Daten-Leaks nach Angreifer-Gruppe
Victims Posted to Extortion Sites

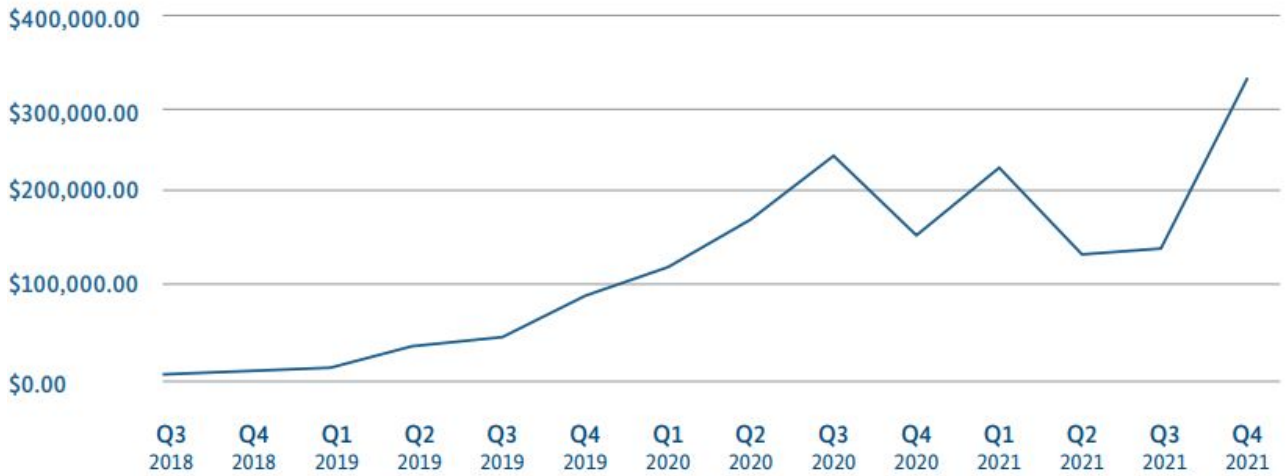
Abbildung 6: Opfer von Daten-Leaks nach Angreifer-Gruppe
Quelle: the Record



Malware

Durchschnittliche Lösegeldzahlungen pro Quartal

Abbildung 7:
Lösegeld-Zahlungen 2018 bis 2021
Quelle: Coveware



Botnetze

Das BSI erklärt Botnetze wie folgt:

- Als Botnetz bezeichnet man den Zusammenschluss mehrerer mit einem Schadprogramm infizierter Systeme (Bots), welche über ein zentrales Steuerungssystem, dem sogenannten Command-and-Control-Server, von einem Bot-Master kontrolliert werden können.
- Bot-Software existiert heutzutage für nahezu alle internetfähigen Geräte. Somit können neben klassischen Computersystemen auch mobile Geräte wie Smartphones oder Tablets, aber auch IoT-Geräte wie Router, Webcams oder Smart-TVs kompromittiert und von Angreifern übernommen werden.

Botnetze

Unique-IP-Index[1] für Deutschland im Berichtszeitraum
2019 = 100

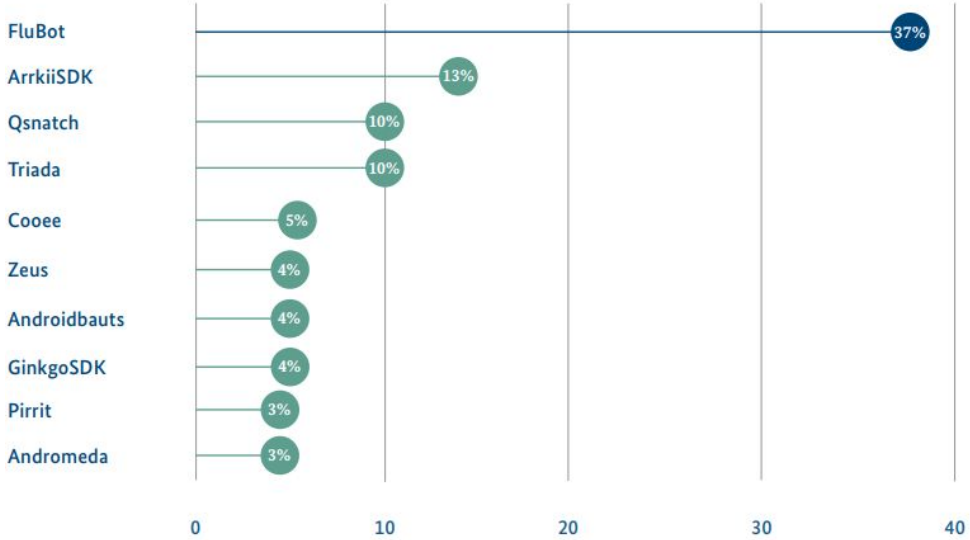
Abbildung 8:
Unique-IP-Index für Deutschland im Berichtszeitraum
Quelle: BSI

[1] Ohne infizierte IP-Adressen, die nicht im Sinkholding erfasst wurden

Botnetze

Bots (Unique IPs) je beobachtetes Botnetz in Deutschland im Durchschnitt des Berichtzeitraums
Anteil in % in allen Unique IPs

Abbildung 9:
Bots (Unique IPs) je beobachtetes Botnetz in Deutschland im Durchschnitt des Berichtszeitraums
Quelle: BSI



Spam und Phishing

Was ist Spam?

- Unerwünschte E-Mails, die oft kommerzielle Inhalte oder Links enthalten.

Was ist Phishing?

- Beim Phishing handelt es sich um den Versuch, über einen Trick persönliche Informationen zu erhalten.

Arten von Phishing:

- Täuschendes Phishing
- Spear Phishing
- Whaling
- Vishing
- Love-Scamming

Spam und Phishing

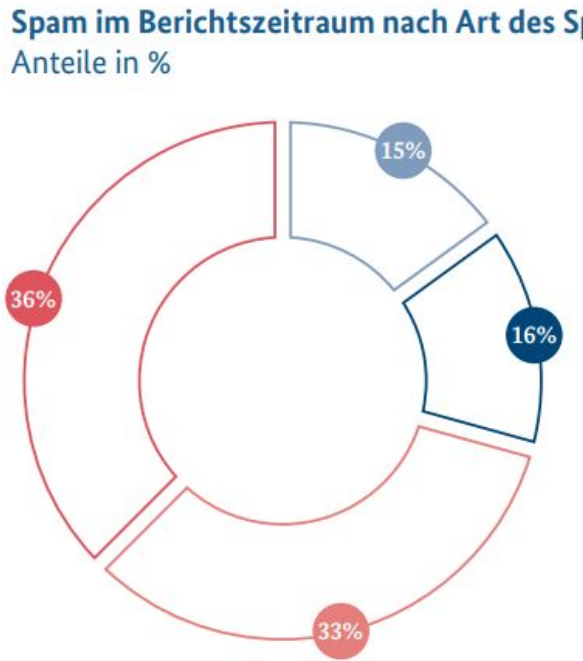


Abbildung 10:
Spam im Berichtszeitraum nach Art des Spam
Quelle: E-Mail-Verkehrsstatistik

- Sonstiges
- Werbung
- Betrug
- Erpressung

Spam und Phishing

Spam-Ratio in der Wirtschaft in Deutschland
Anzahl Spam-Mail je legitime, erwünschte E-Mail

Abbildung 11:
Spam-Ratio in der Wirtschaft in Deutschland
Quelle: E-Mail-Verkehrsstatistik

Social Bots

Der BSI erklärt Social Bots wie folgt:

- Bei Social Bots handelt es sich um Computerprogramme, mit deren Hilfe die Kommunikation in sozialen Netzwerken simuliert und automatisiert werden kann. Diese Automatisierung wird als Mittel zur Verbreitung von Inhalten benutzt. Dadurch können Social Bots als schädliches Werkzeug eingesetzt werden, um Falschmeldungen und Propaganda, sowie Schadinhalte (zum Beispiel Phishing-Postings in sozialen Netzwerken) systematisch zu verbreiten.

Schwachstellen

Coordinated-Vulnerability-Disclosure-Fälle von 2017 bis 2021
Anzahl

Abbildung 14: Coordinated-Vulnerability-Disclosure-Fälle von 2017-2021
Quelle: BSI

Schwachstellen

Bekannt gewordene Schwachstellen 2021 nach dem CVSS-Score[1] für Kritikalität
Anzahl

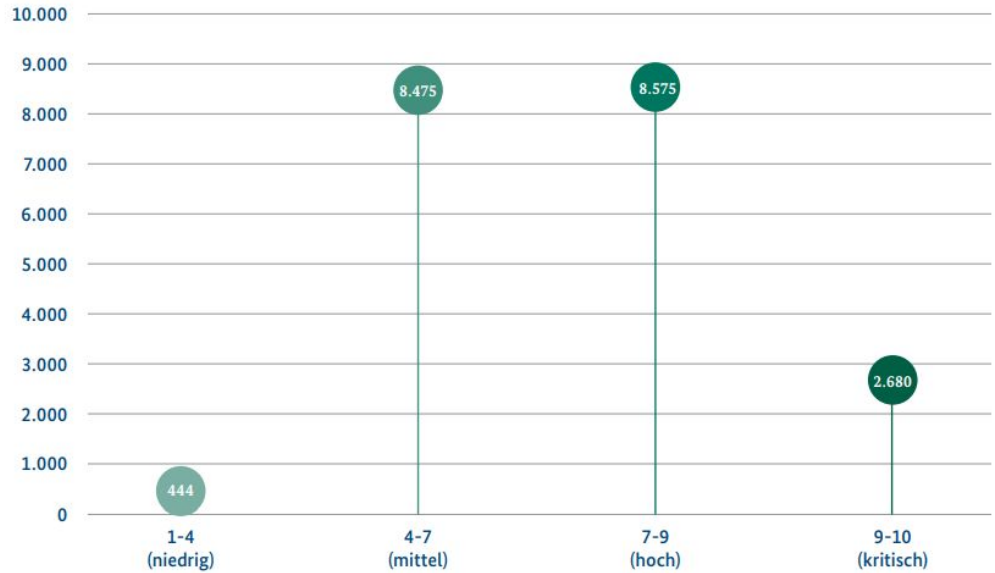


Abbildung 15:
Bekannt gewordene Schwachstellen 2021
nach dem CVSS-Score für Kritikalität
Quelle: Schwachstellen-Statistik

[1] Risikobewertung nach CVSS-Version 3.1

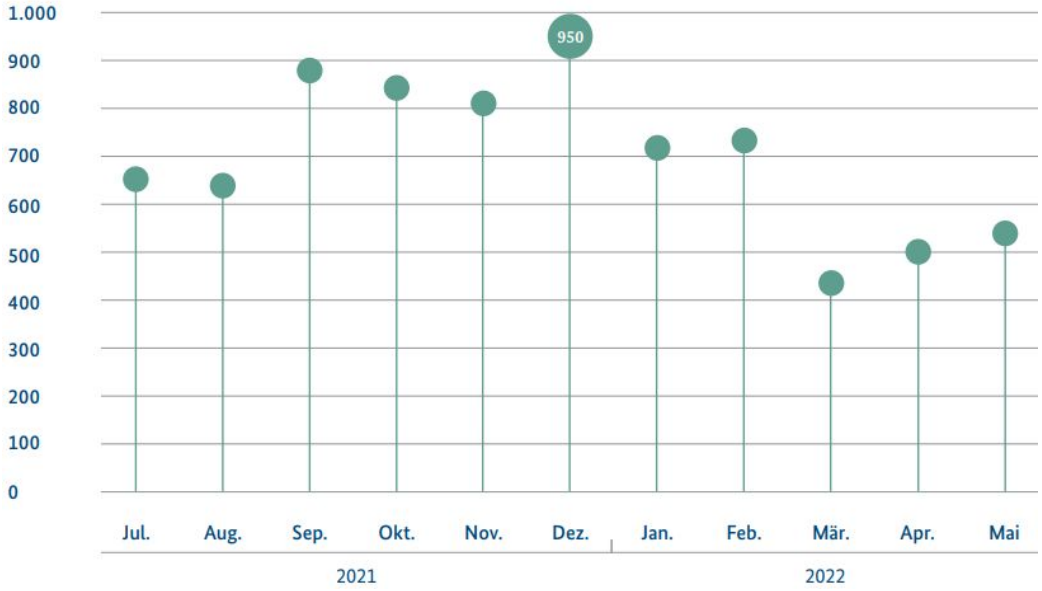
Distributed Denial of Service

Eine DDoS-Attacke (engl. Distributed Denial of Service, dt. verteilte Dienstblockade) ist ein Angriff auf ein Ziel, der dessen Überlastung/Ausfall zum Ziel hat. Während eine DoS-Attacke meist nur von einem Rechner ausgeführt wird, besteht die große Schlagkraft eines DDoS darin, dass viele Rechner zu einem Botnetz zusammengeschlossen werden, um den Serverausfall zu provozieren. Hierfür werden meist massenhaft manipulierte IP-Pakete auf einmal an das Ziel gesendet. DDoS-Attacken werden sowohl von Internetkriminellen als auch von Protestbewegungen wie Anonymous verwendet.

Distributed Denial of Service

Durchschnittliche Brandbreite aller bekannt gewordenen DDoS-Angriffe je Monat
Megabits pro Sekunde

Abbildung 17:
Durchschnittliche Bandbreite bekannt gewordener DDoS-Angriffe je Monat
Quelle: BSI



IT-Sicherheit in Deutschland 2022

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

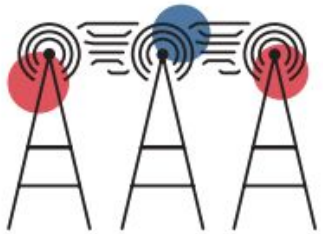
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

IT-Sicherheit in Deutschland 2022

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



34.000

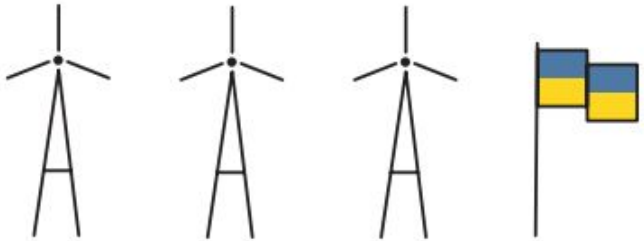
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

IT-Sicherheit in Deutschland 2022

Kollateralschaden
nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.

IT-Sicherheit in Deutschland 2022

69%

aller Spam-Mails im Berichts-zeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm