

Cyber-Angriffe - Ein Blick hinter die Schlagzeilen

03.05.2023





Ein Blick zurück

1989 - Eine erste Schlagzeile

Die Polizei stürmt eine Wohnung im Norden Deutschlands. Es ist der Moment, in dem die Öffentlichkeit das erste Mal von den Ereignissen erfährt, welche bekannt werden sollten als — *der KGB Hack*.

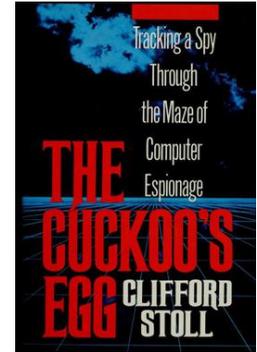
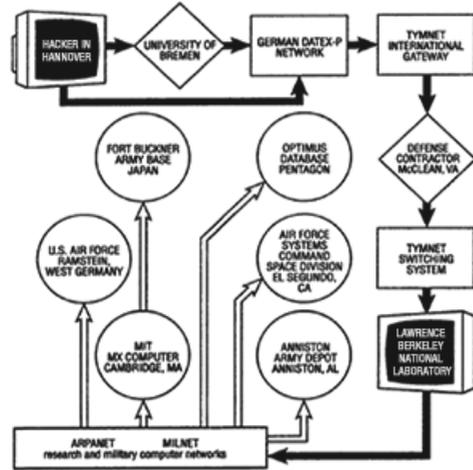


In der ARD Tagesschau vom 02.03.1989



<https://www.youtube.com/embed/gRr2zVVFkQw>

Der KGB Hack



Die Merkmale des Hacks

Die Angreifer

- Keine einmalige Aktion, sondern eine langandauernde Operation.
- Das eigentliche Ziel wurde nicht direkt angegriffen.
- Ein staatlich geförderter Angriff mit zivilen und staatlichen Zielen.
- Die Angreifer waren keine Staatsangestellten, sondern Söldner.

Die Verteidiger

- Zufall und Neugier brachten die Verteidiger auf die Spur.
- Logs, Alerts und Attrappen waren wichtige Mittel.
- Die Täter agieren international und die Behörden aber national.



Zurück in die Gegenwart



Ransomware - Die andere Pandemie

- Dominante Form der Cyberkriminalität
- Erpressung durch Verschlüsselung
- Ransomware kann ein Unternehmen runinieren
- IT-Abhängigkeit wird sichtbar
- Jeder kann zum Opfer werden

Wie wurde Ransomware zur Pandemie?



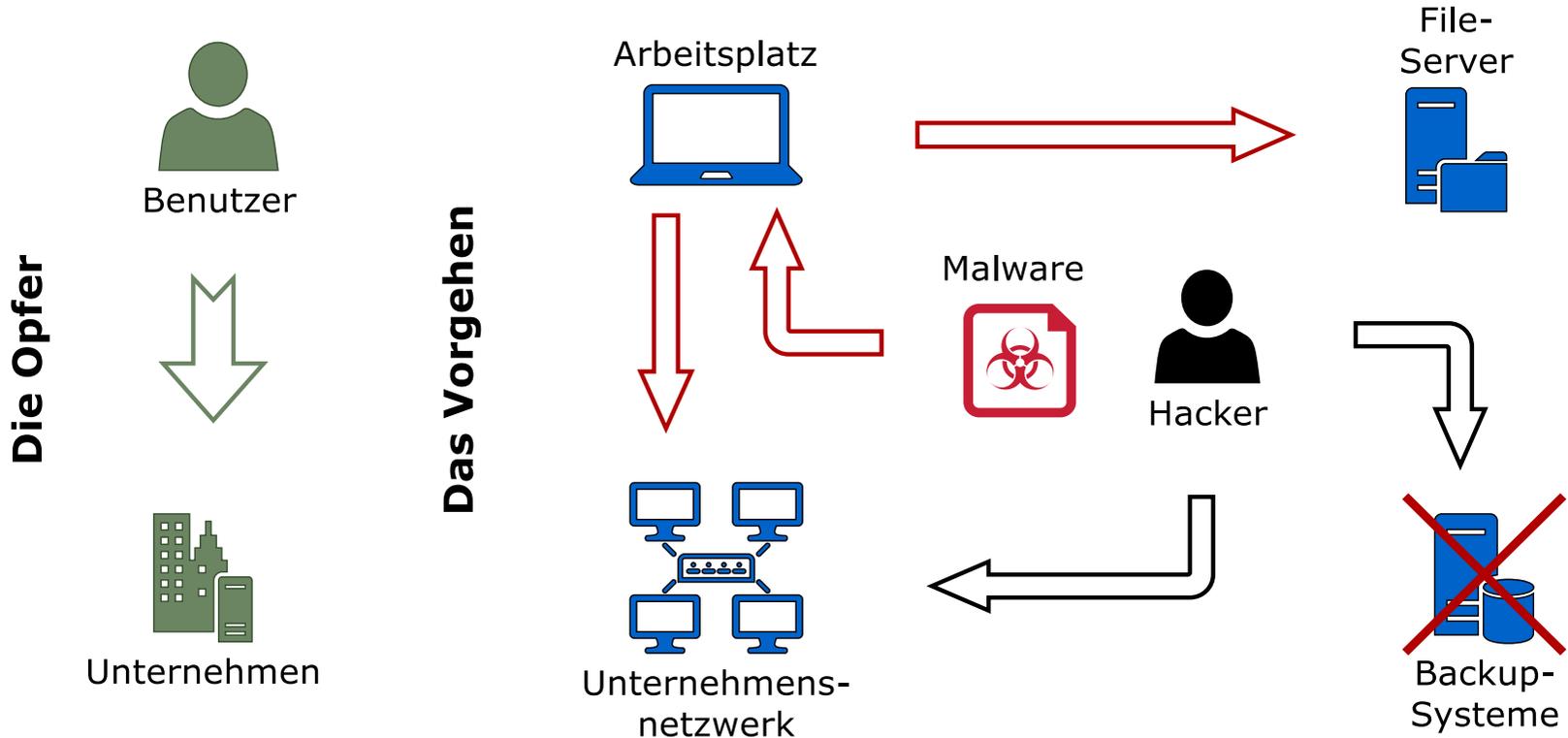
resserschriften, in Form

ware lease from PC Cyborg Corporation.
payment for the lease option of your choice.
PRICE, then be sure to refer to the important
correspondence. In return you will receive:
easy-to-follow, complete instructions;
diskette that anyone can apply in minutes.
9796-2695577-
is US\$189. The price of a lease for the
\$378. You must enclose a bankers draft,
money order payable to PC CYBORG CORPORATION
\$378 with your order. Include your name,
country, zip or postal code. Mail your order
P.O. Box 87-17-44, Panama 7, Panama.

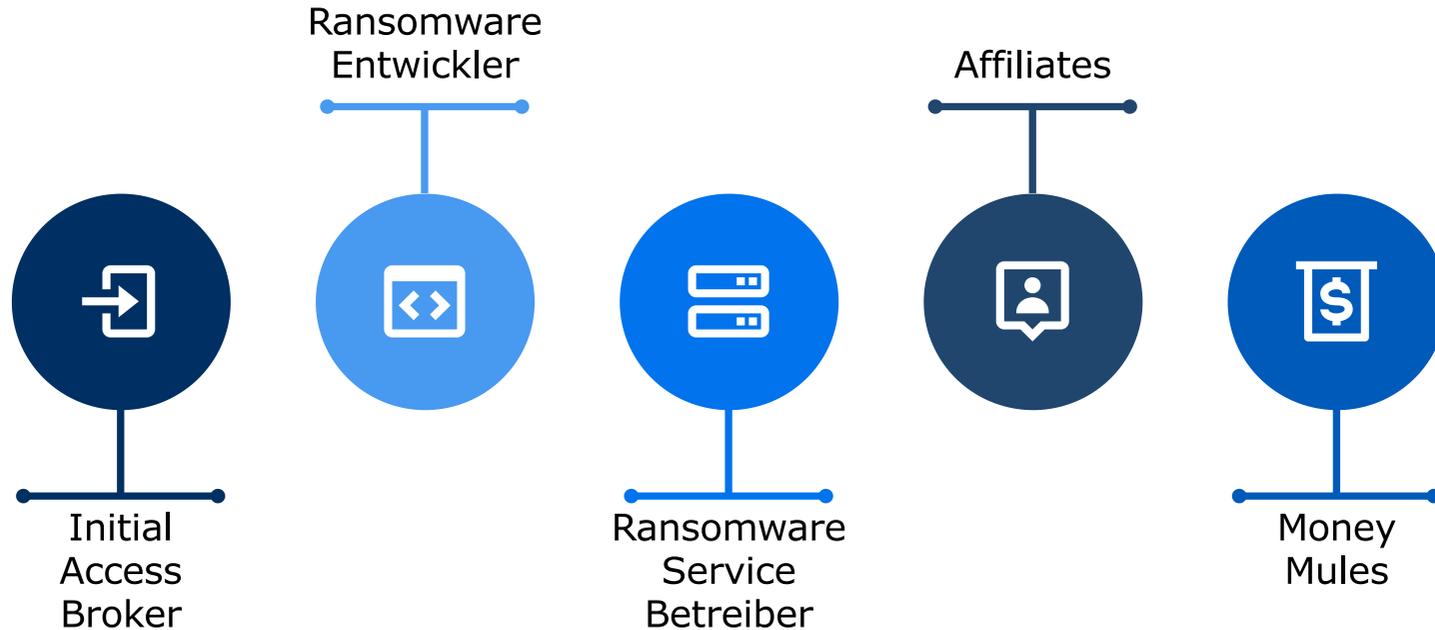
Press ENTER to continue

AIDS oder PC Cyborg
Trojan, die erste
Ransomware von 1989.

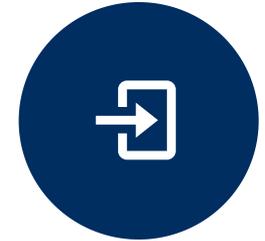
Die Evolution der Ransomware-Angriffe



Das Ransomware-Ökosystem



Initial Access Broker



Stehlen von Zugangsdaten z.B. mittels Phishing

Verkauf der Zugangsdaten im Darkweb

Access UK
By [redacted], March 20 in Auctions

Posted March 20

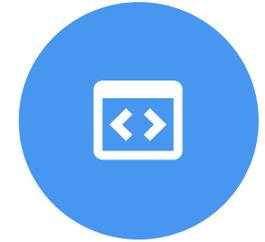
byte

- IT Infrastructure Solutions and Services Provider
- Country: United Kingdom
- Access type: Citrix + work computer
- Employees: 15,000
- Zoom revenue: 6 billion
- The rights of the user, he did not give anyone work, he did not pick.
- Computer in domain, cmd opens
- I don't send users without a deposit, messages, zoom and other information
- Start: \$4000
- Step: 200\$
- Flash: \$6000

Activity
other / other

+ Quote

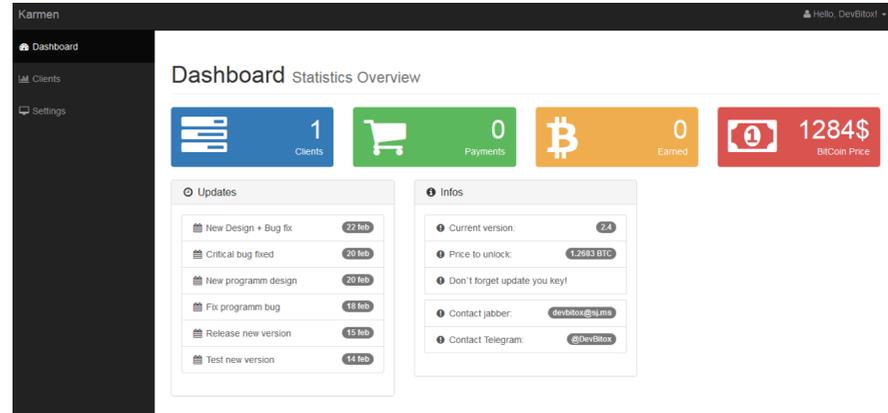
Ransomware Entwickler



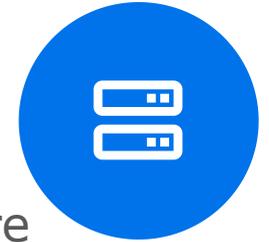
```
17 string sinput;
18 int iLength;
19 double dblTemp;
20 bool again = true;
21
22 while (again) {
23     iN = -1;
24     again = false;
25     getline(cin, sinput);
26     stringstream(sinput) >> dblTemp;
27     iLength = sinput.length();
28     if (iLength < 4) {
29         again = true;
30         continue;
31     } else if (sinput[iLength - 3] != '.') {
32         again = true;
33         continue;
34     } while (++iN < iLength) {
35         if (isdigit(sinput[iN])) {
36             continue;
37         } else if (iN == (iLength - 3)) {
38             continue;
39         }
```

Entwicklung der Ransomware-Software

Inklusive der notwendigen Serverkomponenten



Ransomware Service Betreiber



Betrieb der Server-
Infrastruktur

Bereitstellen der Software
als Service



Affiliates



Verteilen und Ausführen
der Ransomware

Bezahlung via Service
Provider mittels Cryptocurrency



Money Mules



Umtauschen der
Cryptowährung in
traditionelle Währungen

Überweisen der Geldes
mittels Geldtransfer-Service





**Vielen Dank für ihre
Aufmerksamkeit.**