Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Lagebild

31.08.2020

Dauerthemen

- Schadprogramme
- Schwachstellen
- Vorfälle
- DDoS
- Angreifergruppen
- Politische Entwicklungen

- Was davon ist wirklich wichtig?
  - Was macht Schaden?
    (Könnte künftig Schaden machen?)

DDoS Erpressung

DDoS Attack on your network!

We are the Fancy Bear and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your whole network will be subject to a DDoS attack starting at Monday (in 5 days). (This is not a hoax, and to prove it right now we will start a small attack on a few of your IPs that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly ([redacted]) and our attacks are extremely powerful (peak over 2 Tbps)

What does this mean? This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers.

How you can stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: 1N8Ynt5QHjNJ1tBbA6WBMLEW9xNCAM6djg

Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

What if you don't pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Exemplarische Erpressermail von „Fancy Bear“ aus dem August 2020

- Aktuelle Welle seit Mitte August: Erpressungen im Namen von „Fancy Bear“
- „Demo“-Angriff (zwei bis dreistelliger Gbit/s-Bereich
- Erpresserschreiben mit der Androhung eines Angriffs im Tbit/s – Bereich bei Nichtzahlung des angekündigten Lösegelds
- Bisher nur „Demo“-Angriffe beobachtet
- Parallelen zu Kampagen im Oktober 2019 (E-Mails)

Ransomware

- Emotet, Trickbot, Ryuk, Conti, Maze, Ragnar Locker, LockBit
  - Methoden wie bei gezielten Angriffen
    - „Mimikatz“
    - Lateral Movement
    - Befall des ADC

- Alt: „nur“ Verschlüsselung
  - Gegenmaßnahme: Backups!!

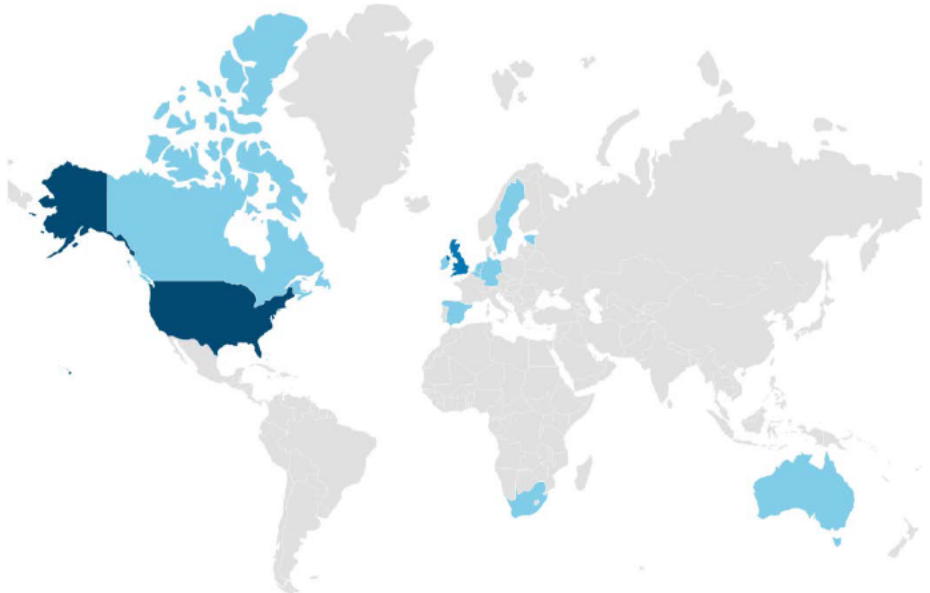
- Neu: zusätzlich Datenausleitung
  - Gegenmaßnahme: ???

- Sensibilisierungskampagne für Monitoring (DLP)

Nicht alles wird schlechter

- Probleme durch Datenschutz
  - Abfrage von Whois-Datenbanken
  - DNS-Einträge
  - Verschlüsselung

- „Neue“ Möglichkeiten
  - DNS-History-Datenbanken
  - Certificate Transparency Logs (Let‘s Encrypt)



- Aufdeckung einer Angriffskampagne (76 Unis, 4 in Deutschland)

Vielen Dank für Ihre Aufmerksamkeit!