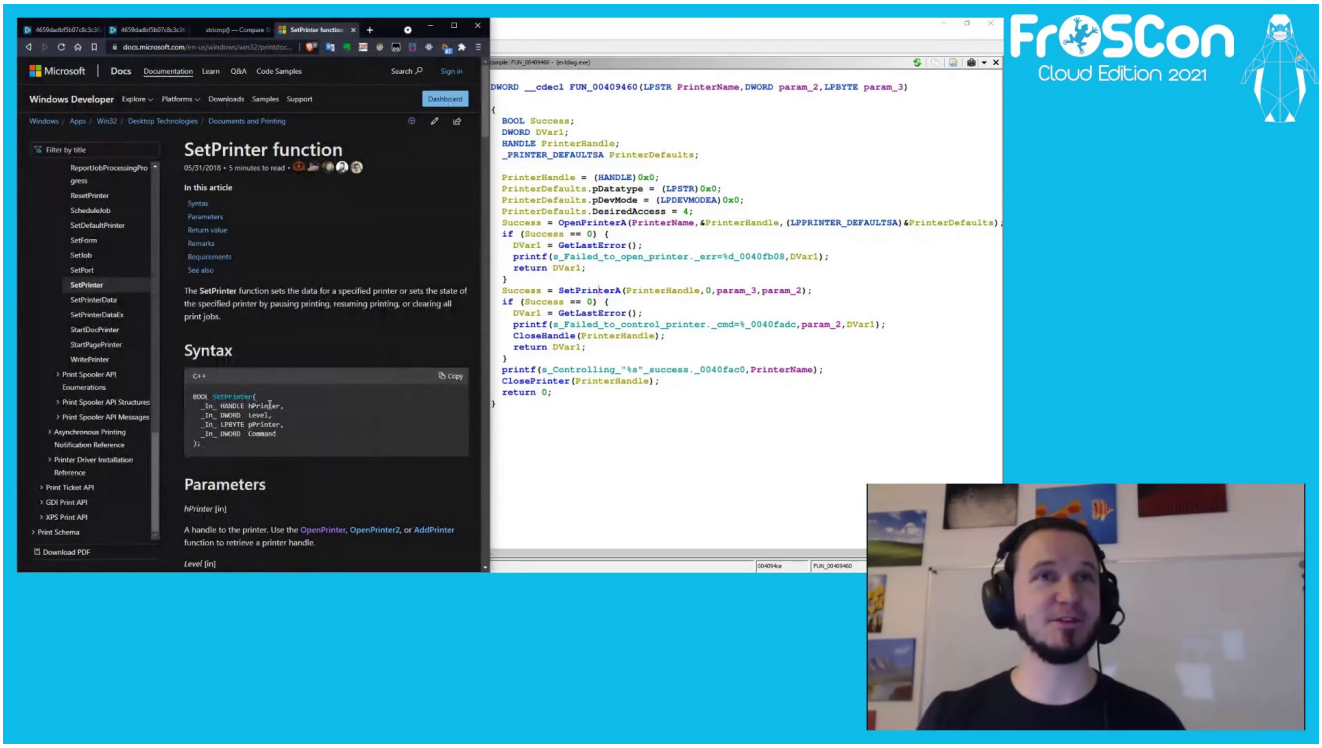
Der Cyber-Bankraub von Bangladesch

media.ccc.de/v/froscon2021-2670-der_cyber-bankraub_von_bangladesch

larsborn



larsborn

Getting to the Source - Vulnerabilities in the mirror are closer than they appear Playlists: 'froscon2021' videos starting here / audio

- 55 min
- 2021-08-22
- 2021-08-31
- 535
- Fahrplan

Vor nunmehr 5 Jahren war die Zentralbank Bangladeshs Ziel eines Cyber-Angriffs. Die Akteure dahinter hatten vor eine Milliarde US-Dollar zu stehlen – einer der spektakulärsten Bankraube überhaupt.

Wir wissen alle, dass wir im Internet Spuren hinterlassen. Ähnlich verhält es sich mit bösartigen Akteuren, die einen Angriff durchführen. Wie beispielsweise den Angriff auf die Zentralbank von Bangladesh in 2016, einer der größten Bankraube in der Geschichte.

Ich möchte anhand dieses Vorfalls beispielhaft einen kleinen Schritt im Vorgehen in der Cyber Threat Intelligence (CTI) skizieren. Dabei geht es nämlich nicht nur um Netzwerk-Indikatoren und Virus-Signaturen sondern darum, Angriff zu verstehen um sie besser abwehren zu können. CTI involviert die Bewertung von Informationen aus sehr vielen verschiedenen sowohl offen als auch verdeckten Quellen; sowohl mit technischen als auch mit nicht-technischen Mitteln. Die Ergebnisse solche Analysen sollen das Erreichen verschiedener Ziele ermöglichen: Eines davon ist, die Personen hinter einem Angriff zu identifizieren, die sogenannte *Attribution*.

In diesem Vortrag werden wir uns nur auf den technischen Analyseschritt konzentrieren: ich werde das Open Source Tool Ghidra verwenden um live einige Komponenten des Angriffs durch Reverse Engineering zu analysieren. Dabei werden wir sogar schon einige Schlussfolgerungen über den Angriff und das Verhalten des Akteurs machen können. Ein wenig wie bei einer polizeilichen Ermittlung, nur das man Sie aus der Geborgenheit der eigenen vier Wände durchführen kann.

Download

Tags