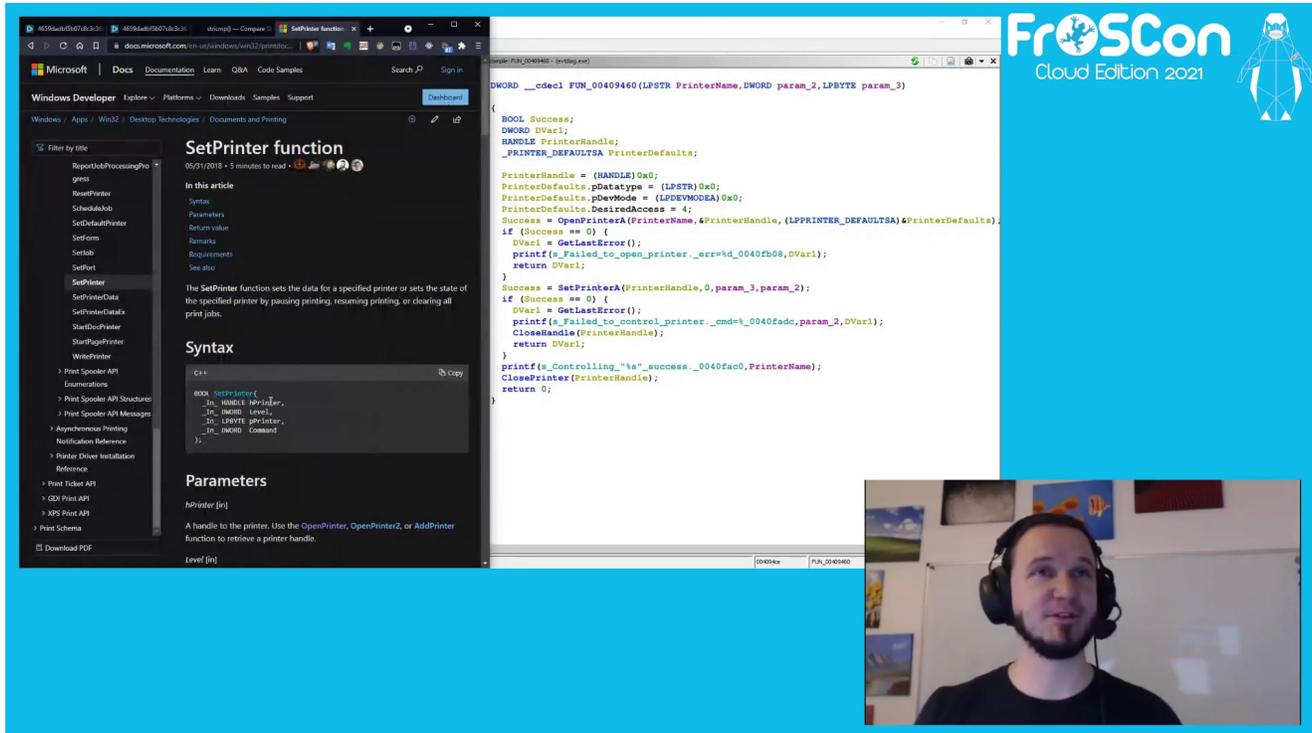


Der Cyber-Bankraub von Bangladesch

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

larsborn



The image shows a Windows Developer environment with the Microsoft Docs website open to the 'SetPrinter' function page. The page displays the function's syntax and parameters. A code editor window shows the implementation of the function in C++:

```
DWORD __cdecl FUN_00409460(LPSTR PrinterName, DWORD param_2, LPBYTE param_3)
{
    BOOL Success;
    DWORD DVar1;
    HANDLE PrinterHandle;
    PRINTER_DEFAULTS PrinterDefaults;

    PrinterHandle = (HANDLE)0x0;
    PrinterDefaults.pDatatype = (LPSTR)0x0;
    PrinterDefaults.pDevMode = (LPDEVMODE)0x0;
    PrinterDefaults.DesiredAccess = 4;
    Success = OpenPrinterA(PrinterName, &PrinterHandle, (LPPRINTER_DEFAULTS)&PrinterDefaults);
    if (Success == 0) {
        DVar1 = GetLastError();
        printf(_"Failed to open printer _err=%td_0040fb08, DVar1);
        return DVar1;
    }
    Success = SetPrinterA(PrinterHandle, 0, param_3, param_2);
    if (Success == 0) {
        DVar1 = GetLastError();
        printf(_"Failed to control printer _cmd=%_0040fad0, param_2, DVar1);
        CloseHandle(PrinterHandle);
        return DVar1;
    }
    printf(_"Controlling _ts_ _success_ _0040fac0, PrinterName);
    ClosePrinter(PrinterHandle);
    return 0;
}
```

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 Bangladeschs Ziel eines Cyber-Angriffs. Die Akteure dahinter hatten vor eine Milliarde US-Dollar zu stehen – einer der spektakulärsten Bankraube überhaupt.

Wir wissen alle, dass wir im Internet Spuren hinterlassen. Ähnlich verhält es sich mit böstigen 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) skizzieren. 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
