

# La mitigazione del rischio

Massimiliano Graziani  
massimiliano.graziani@cybera.it

 <https://www.linkedin.com/in/mgraziani/>

© Alcune grafiche acquistate su licenza Adobe Stock

# WHOAMI



Massimiliano Graziani, Sottufficiale dell'Aeronautica Militare in congedo, con oltre 20 anni di esperienza nel settore Cyber Security è oggi CEO di Cybera Srl, si occupa di Cyber Security e Digital Forensics. Ha sviluppato software, videogiochi e le prime applicazioni multimediali nei primi anni 90. Sysop di Cobra BBS e Bikers Network BBS.

<https://www.cobrasoft.it> quando internet ancora non c'era...  
e non esisteva ancora il diritto d'Autore sul Software

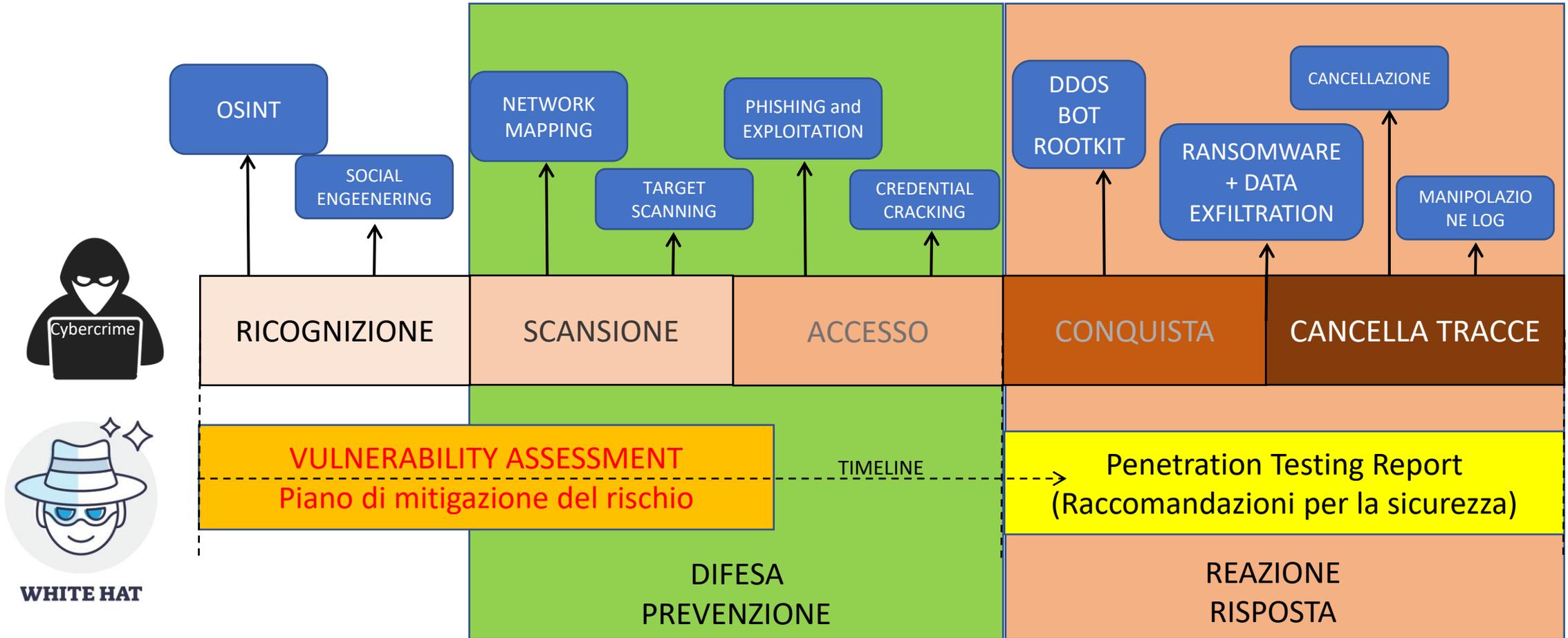
Smette di sviluppare nel 2005 dove si dedica completamente a Cyber Security e Antifrode Fondatore del Capitolo Italiano IISFA, OWASP e di ONIF.

Consulente in Digital Forensics presso la Procura della Repubblica e le Aziende Private.

Docente in materia di Digital Forensics pratica in Master e Corsi universitari e in alcuni reparti operativi istituzionali. Annovera oltre 10.000 follower su 

E' certificato CHFI, CEH, CFIP, CFE, CIFI, OPSA, CDFP, Bsi Lead Auditor BS7799-2:2002, ecc.

# CONOSCI IL TUO NEMICO!



Basterebbero anche misure di protezione minime?

**Certo! Se avete una porta blindata, ma lasciate la finestra aperta, secondo voi il ladro perderà tempo a scassinare la porta?**



# Quali sono le finestre aperte?

- Utenti non formati sulle minacce
- Vulnerabilità dei sistemi non aggiornati
- Account utenti, validi, contenuti nei Data Breach
- Informazioni sensibili disperse in rete
- Account condivisi con personale esterno
- Poca percezione del rischio sul proprio PC
- Fiducia assoluta da messaggi di estranei che dicono di essere il tuo “capo”
- ecc.

**GOOGLE**  
**HACKING-DATABASE**

Sembra incredibile eppure ci cascano quasi sempre!



Dopo aver protetto i sistemi perimetrali fisici, è ora di iniziare a creare lo Human Firewall!



Adeguare i comportamenti umani alle minacce, come? Addestrando continuamente il personale, anche simulando attacchi realistici, dotare gli utenti di password robuste che devono essere strettamente personali e non vanno condivise con nessun altro, da usare sempre con un secondo fattore di autenticazione, come ad esempio l'OTP, e aggiornare il sistema di deprovisioning degli utenti, quando un utente viene cessato, le sue credenziali non devono rimanere attive, ecc.

# La seconda regola è iniziare ad evidenziare le vulnerabilità dei sistemi!

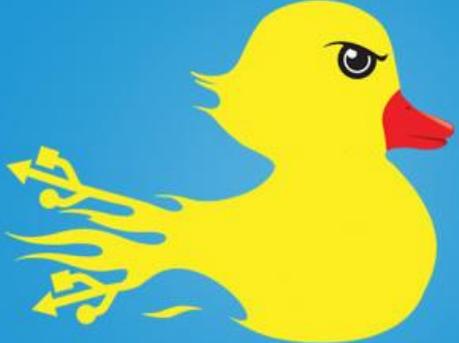
La maggior parte degli attacchi avviene sfruttando vulnerabilità conosciute e a volte vecchie di anni...



Adottare uno standard di riferimento come ISO 27001, è già un grande passo avanti!

# Siete tutti consapevoli che se trovate una chiavetta USB, non la dovete inserire dentro il vostro computer vero?

**USB RUBBER DUCKY**  
THE MOST LETHAL DUCK EVER TO GRACE AN UNSUSPECTING USB PORT



**Write**

payloads with a **simple scripting language** or online payload generator including

- WiFi AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

**Encode**

the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

Carry multiple payloads, each on its own micro SD card.

**Load**

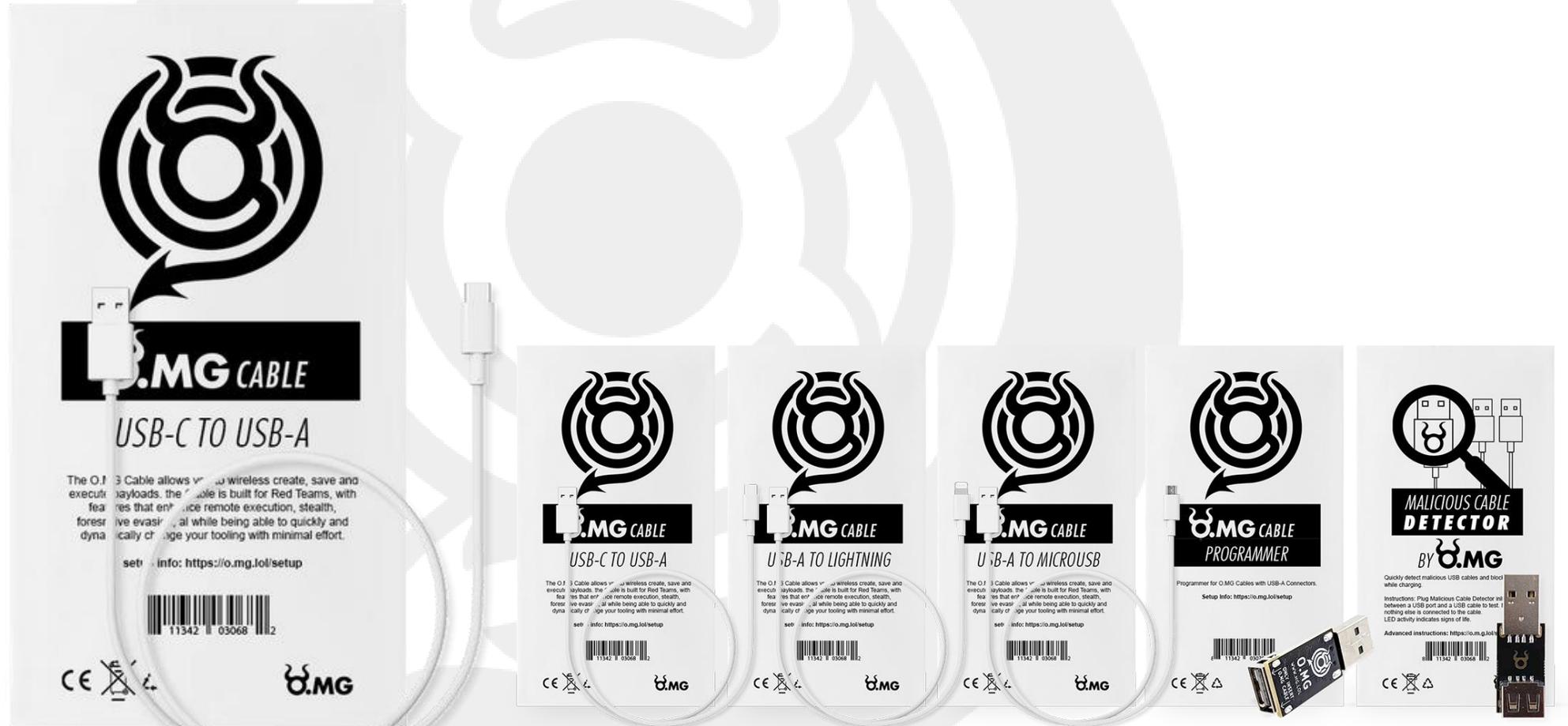
the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

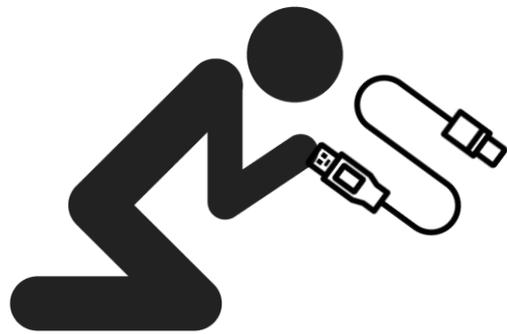
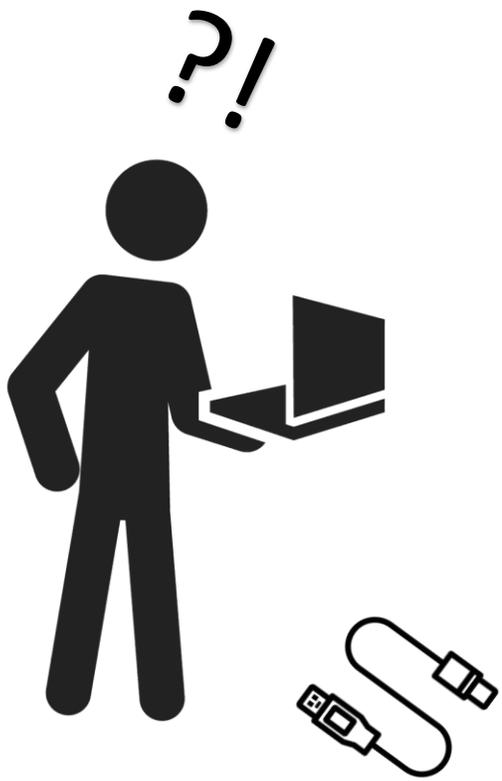
**Deploy**

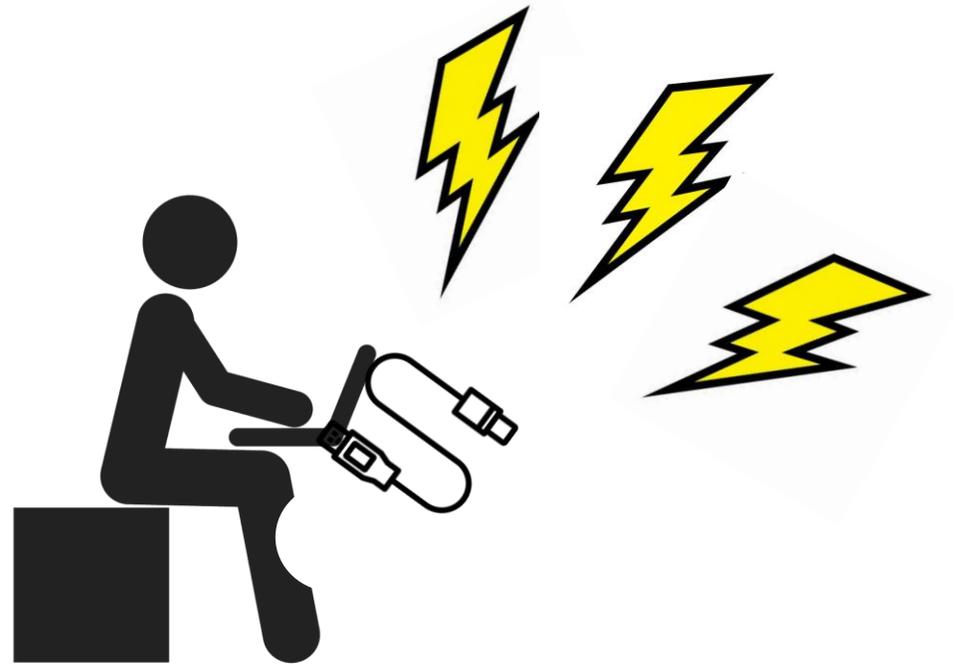
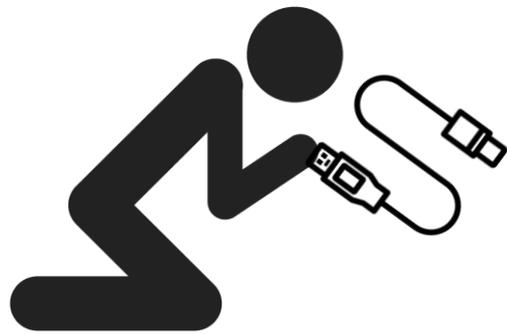
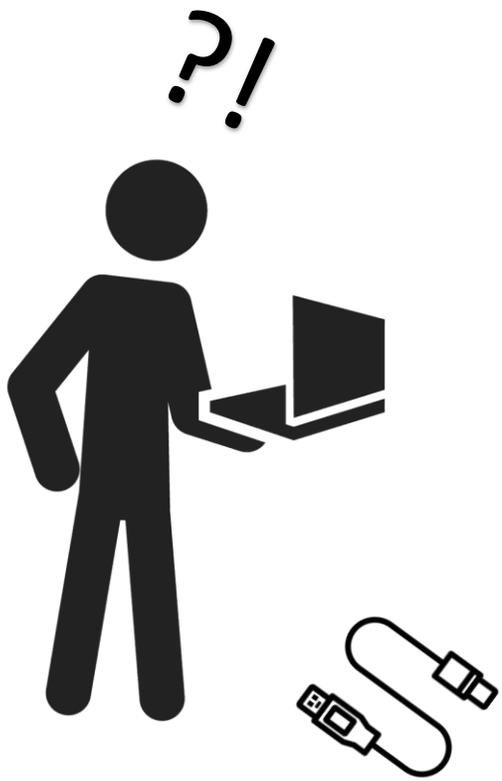
the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.

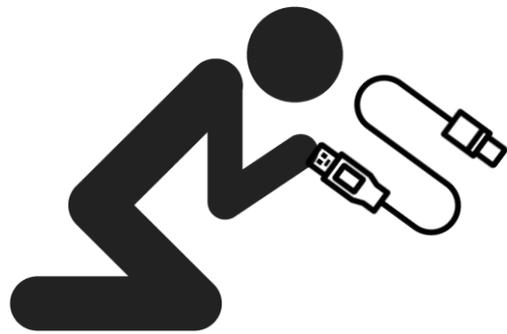
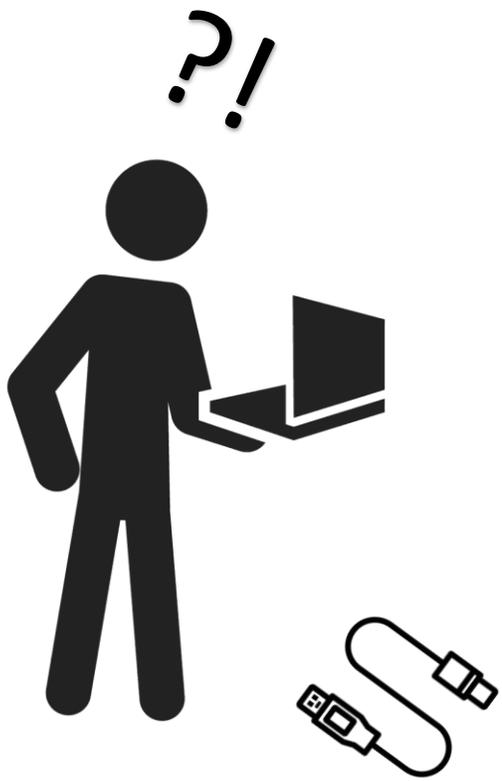


# Qualcuno in sala ha trovato dei cavetti per caricare lo smartphone?





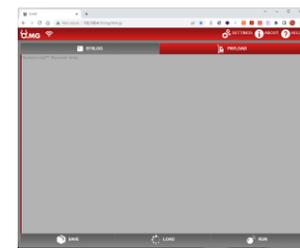
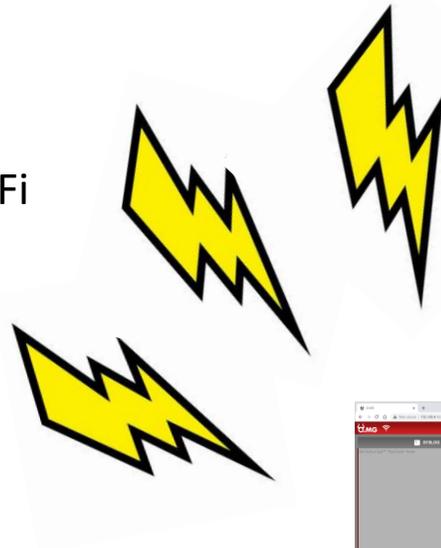






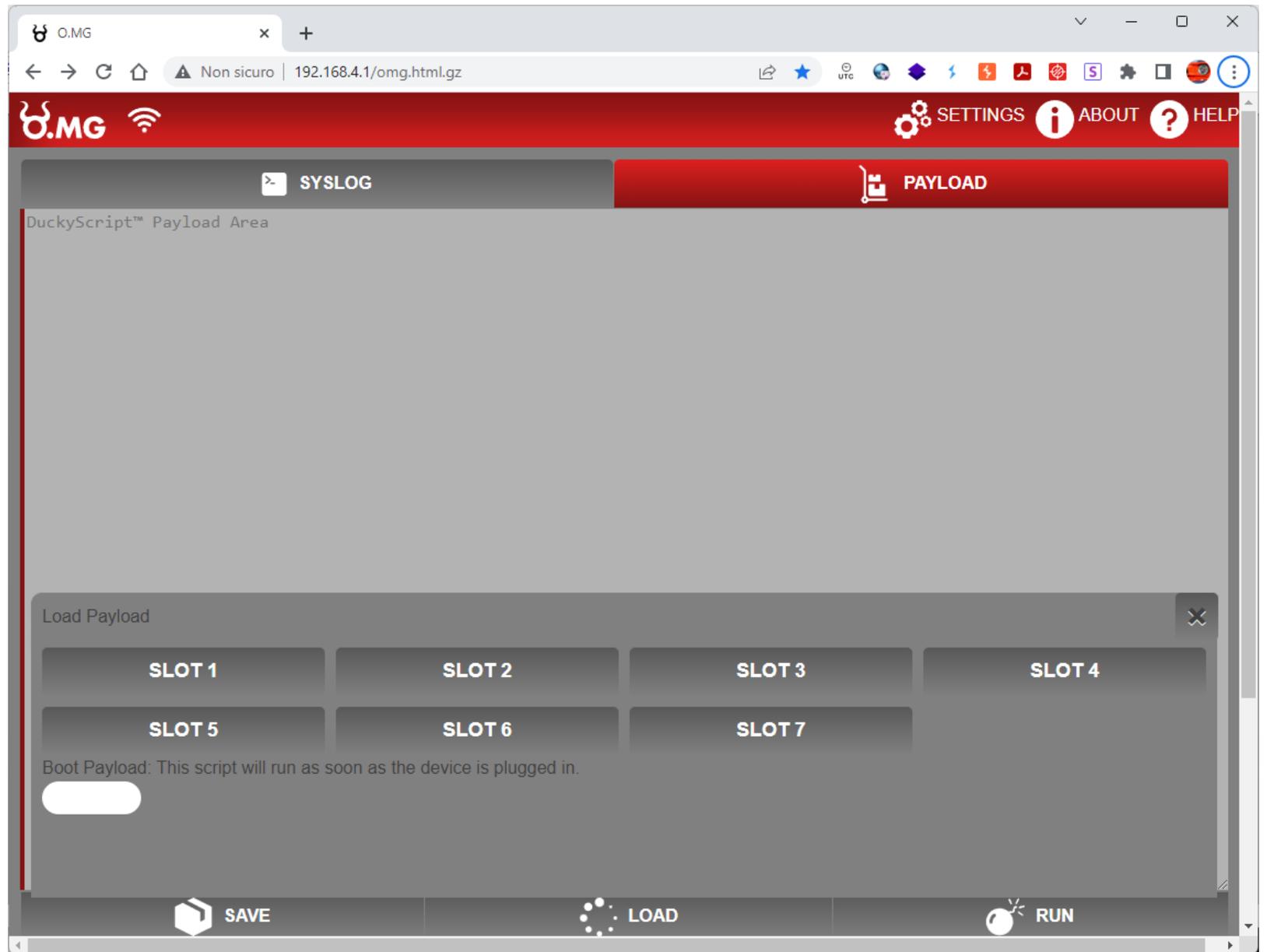
VITTIMA

WiFi



ATTACCANTE

## INTERFACCIA WEB CHE VEDE ATTACCANTE



## ESEMPIO PRIMO PAYLOAD

The screenshot shows a web browser window with the URL `192.168.4.1/omg.html.gz`. The page has a red header with the O.MG logo and navigation links for SETTINGS, ABOUT, and HELP. Below the header, there are two tabs: 'SYSLOG' (selected) and 'PAYLOAD'. The main content area displays a list of commands for a payload, including system information, delays, and strings. At the bottom, there are three buttons: 'SAVE', 'LOAD', and 'RUN'.

```
VID 045E
PID 0048
MAN Microsoft
PRO Windows Defender Update
GUI r
DELAY 1000
STRING notepad
ENTER
DELAY 4000
STRING Ciao sono un cavo fatto di microchip e wifi.
ENTER
ENTER
DELAY 1000
STRING Il tuo computer crede che io sia la sua tastiera...
ENTER
ENTER
DELAY 2000
STRING Posso disattivare le sue difese e creare una porta di accesso al tuo sistema...
ENTER
DELAY 1000
ENTER
STRING Pensaci bene quando trovi un cavo, prima di usarlo!
ENTER
ENTER
DELAY 3000
STRING Demo Anica O.MG cable.
ENTER
```

## ESEMPIO SECONDO PAYLOAD

The screenshot shows a web browser window with the address bar displaying "192.168.4.1/omg.html.gz". The page features a red header with the "O.M.G." logo and navigation links for "SETTINGS", "ABOUT", and "HELP". Below the header, there are two tabs: "SYSLOG" (selected) and "PAYLOAD". The main content area is a large text editor containing the following payload configuration:

```
VID 045E
PID 0048
MAN Microsoft
PRO Windows Defender Update
GUI r
DELAY 1000
REM ~~ | Change line below to desired browser: chrome, firefox, iexplore, etc.
STRING chrome
ENTER
DELAY 4000
REM | Alt+D below moves cursor focus to the URL bar. This is needed for Internet Explorer and Edge (Does not impact Chrome or Firefox)
ALT d
REM ~~ | Change line below to desired URL
STRING www.mgx.it/pro&wp/content&uploads&2021&05&Ransomware/WannaCry.jpg
ENTER
REM ~~ | Change line below to "GUI UP" to maximize screen. Change line below to "F11" to fullscreen.
F11
```

At the bottom of the interface, there are three buttons: "SAVE", "LOAD", and "RUN".

NON CI CREDETE?

2 MIN DEMO LIVE