La mitigazione del rischio

Massimiliano Graziani
massimiliano.graziani@cybera.it
https://www.linkedin.com/in/mgraziani/

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

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…

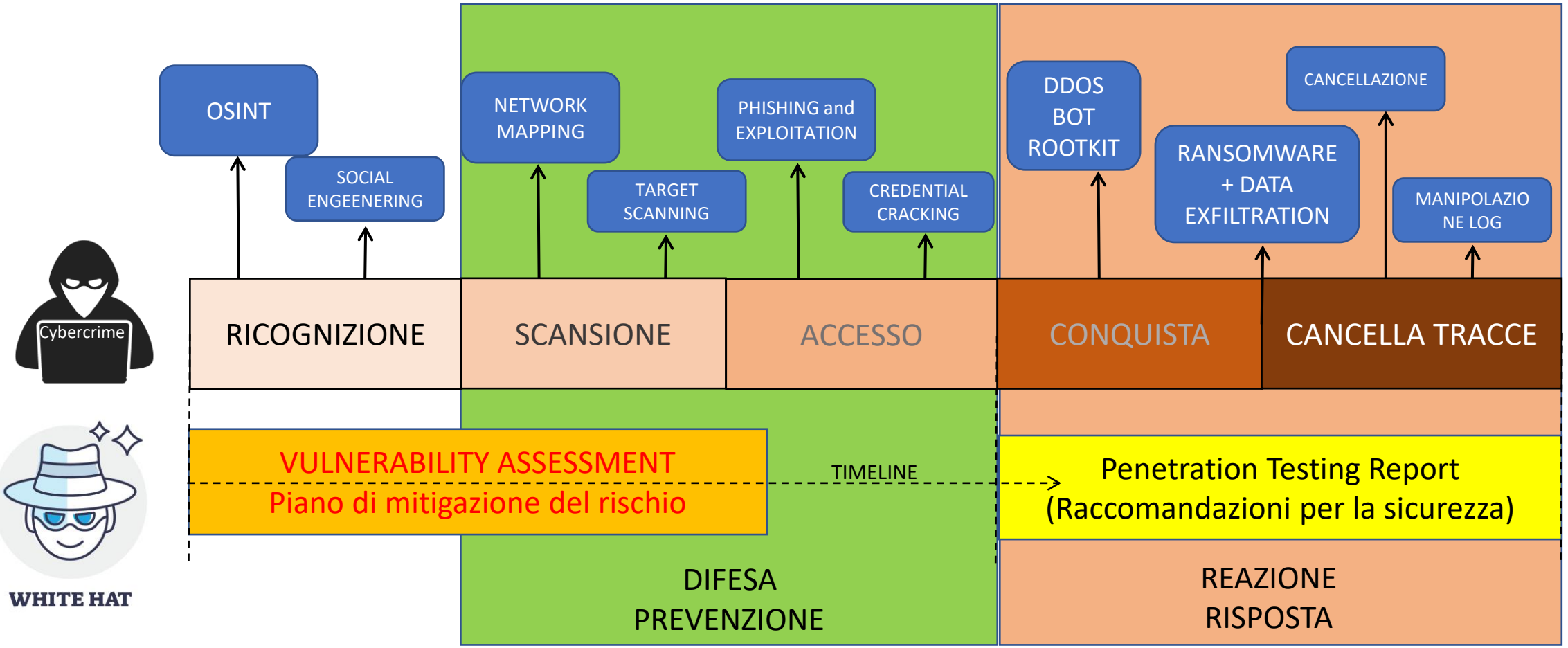
e non esisteva ancora il diritto d'Autore sul Software

Smette di sviluppare nel 2005 dove si dedica completamente a Cyber Security e AntifrodeFondatore 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 in

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

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

CONOSCI IL TUO NEMICO!



ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

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?

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

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!

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

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.

ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

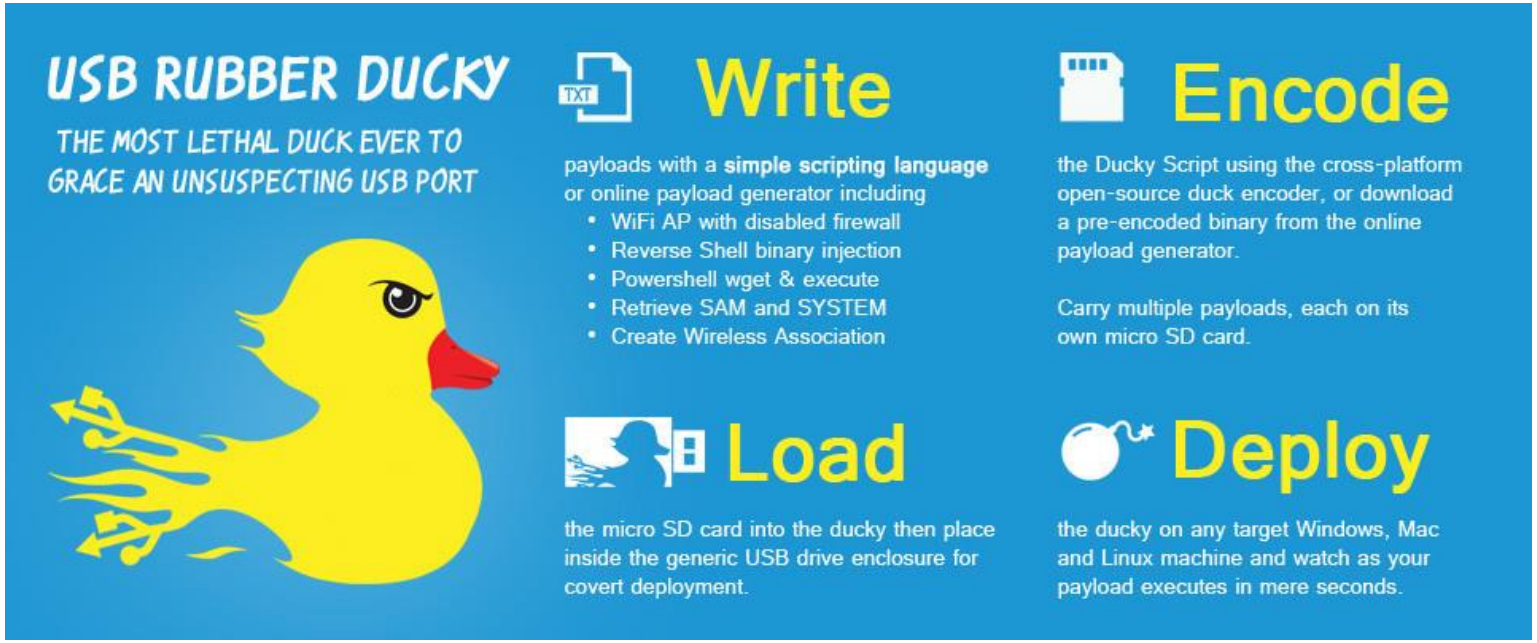
La seconda regola è iniziare ad evidenziare le vulnerabilità dei sistemi!

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!

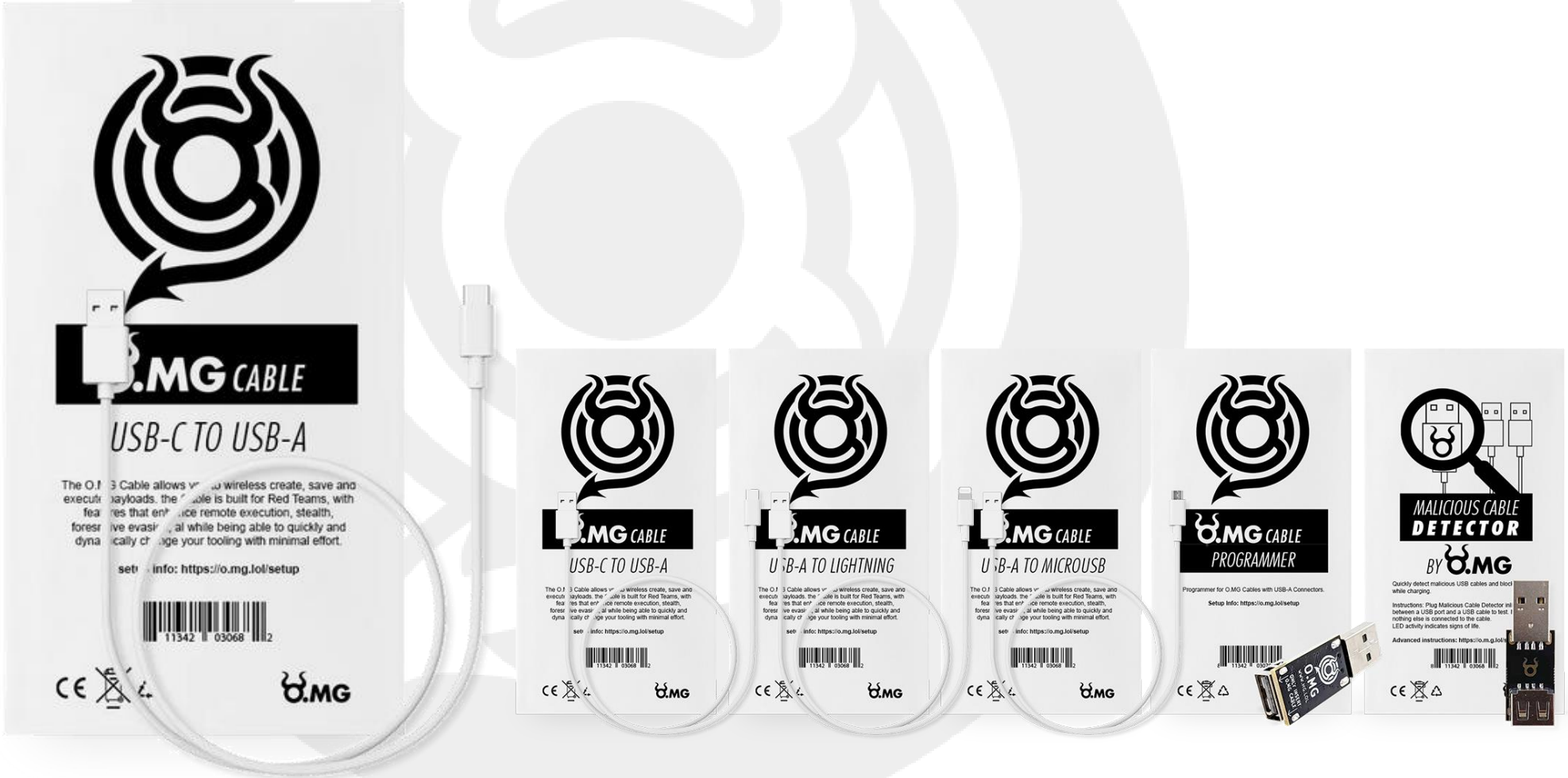
ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

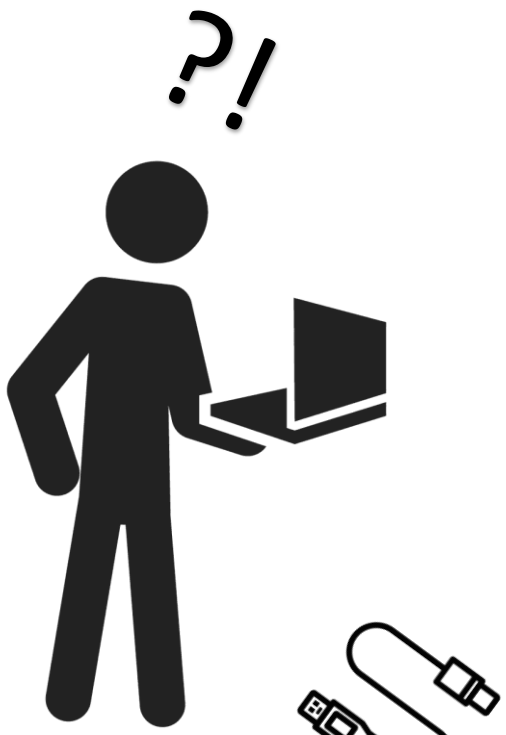
Siete tutti consapevoli che se trovate una chiavetta USB, non la dovete inserire dentro il vostro computer vero?

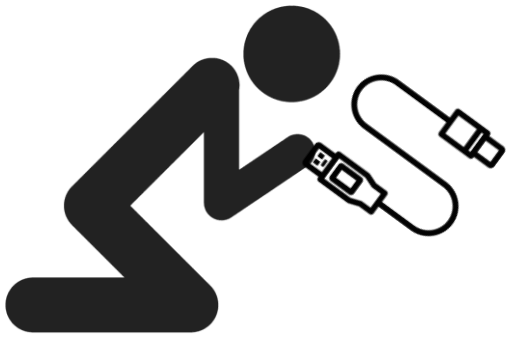


ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

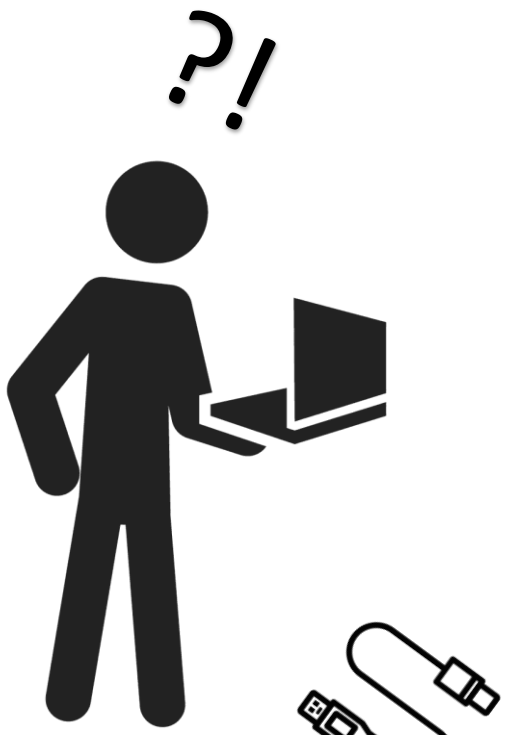
Qualcuno in sala ha trovato dei cavetti per caricare lo smartphone?

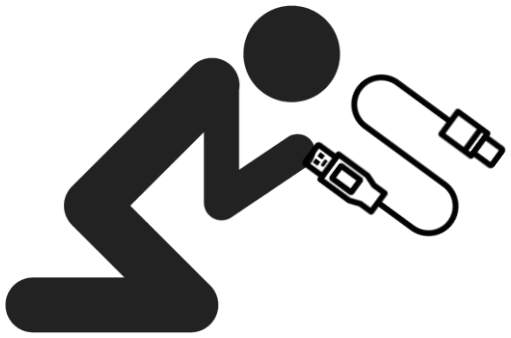


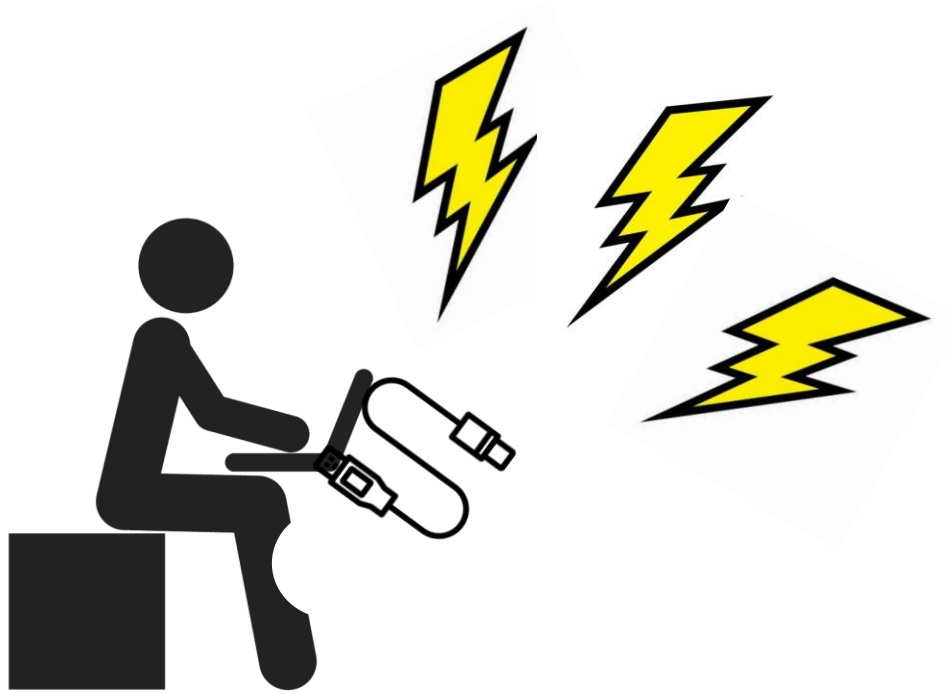




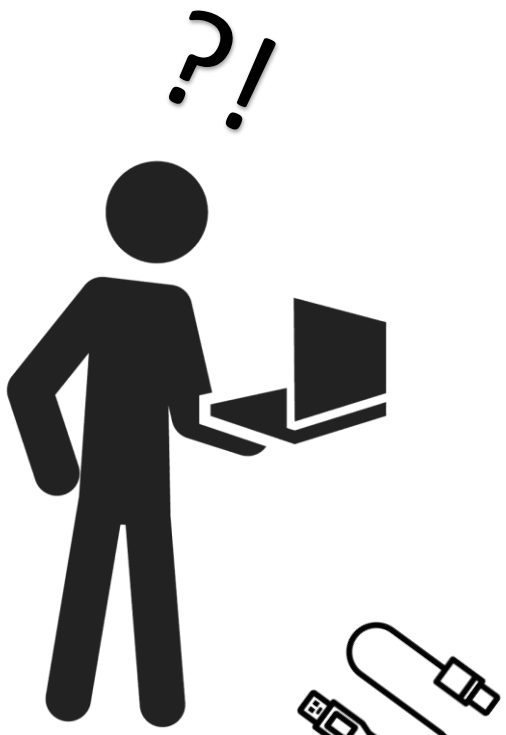
ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

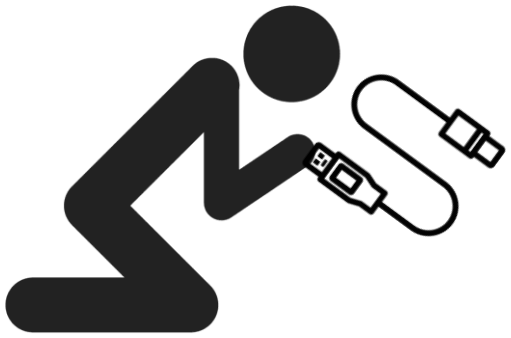


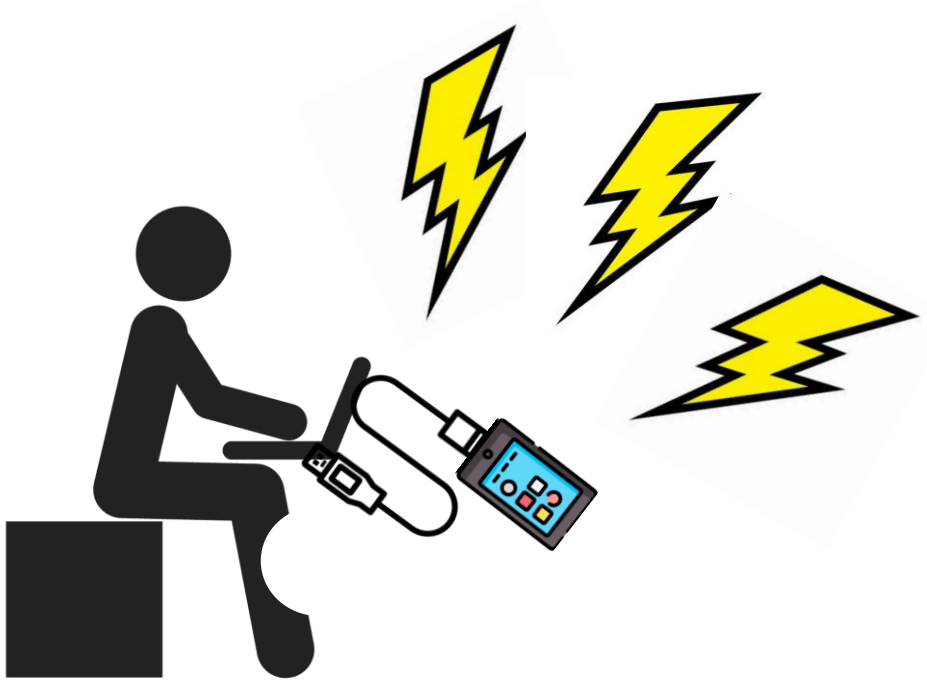




ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

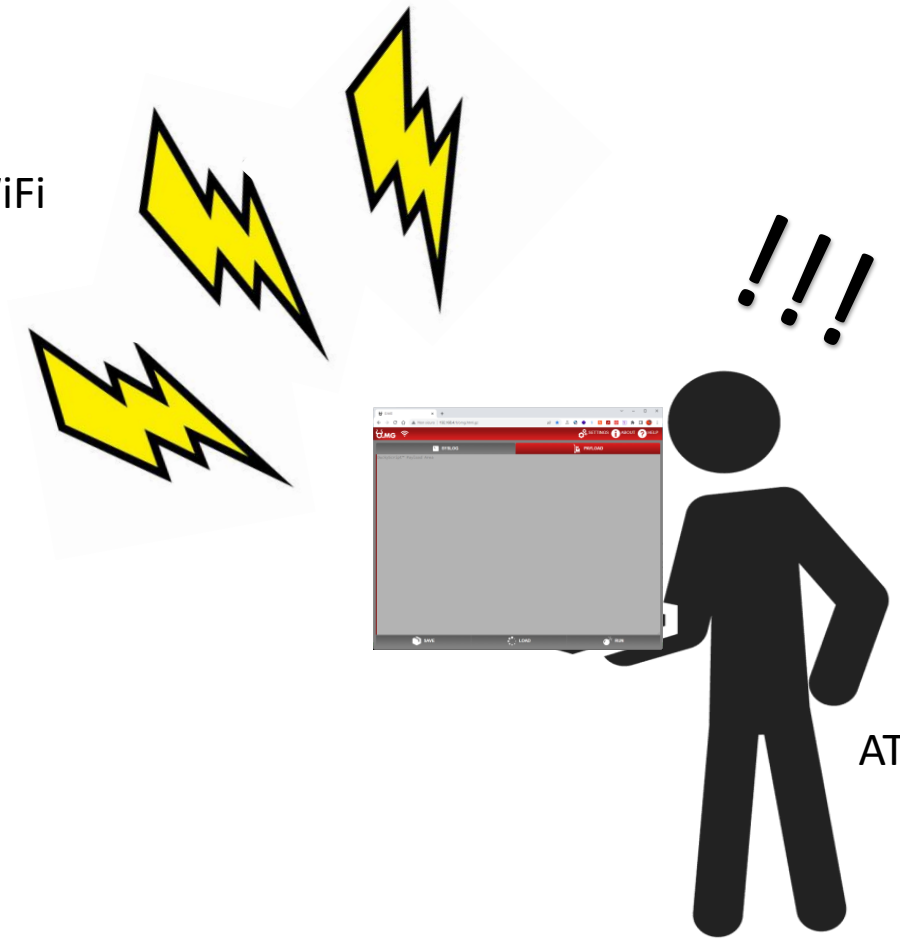






VITTIMA

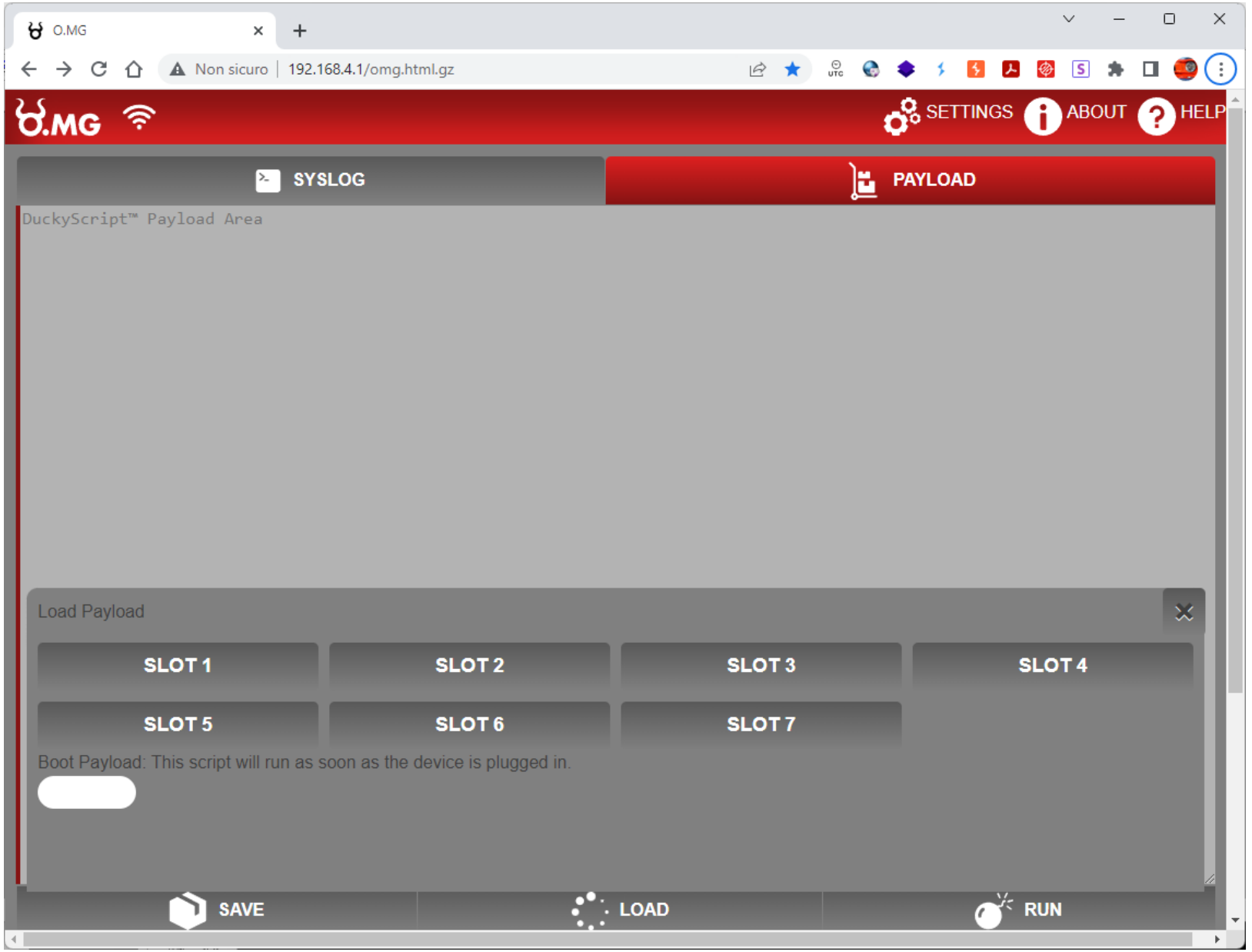
WiFi



ATTACCANTE

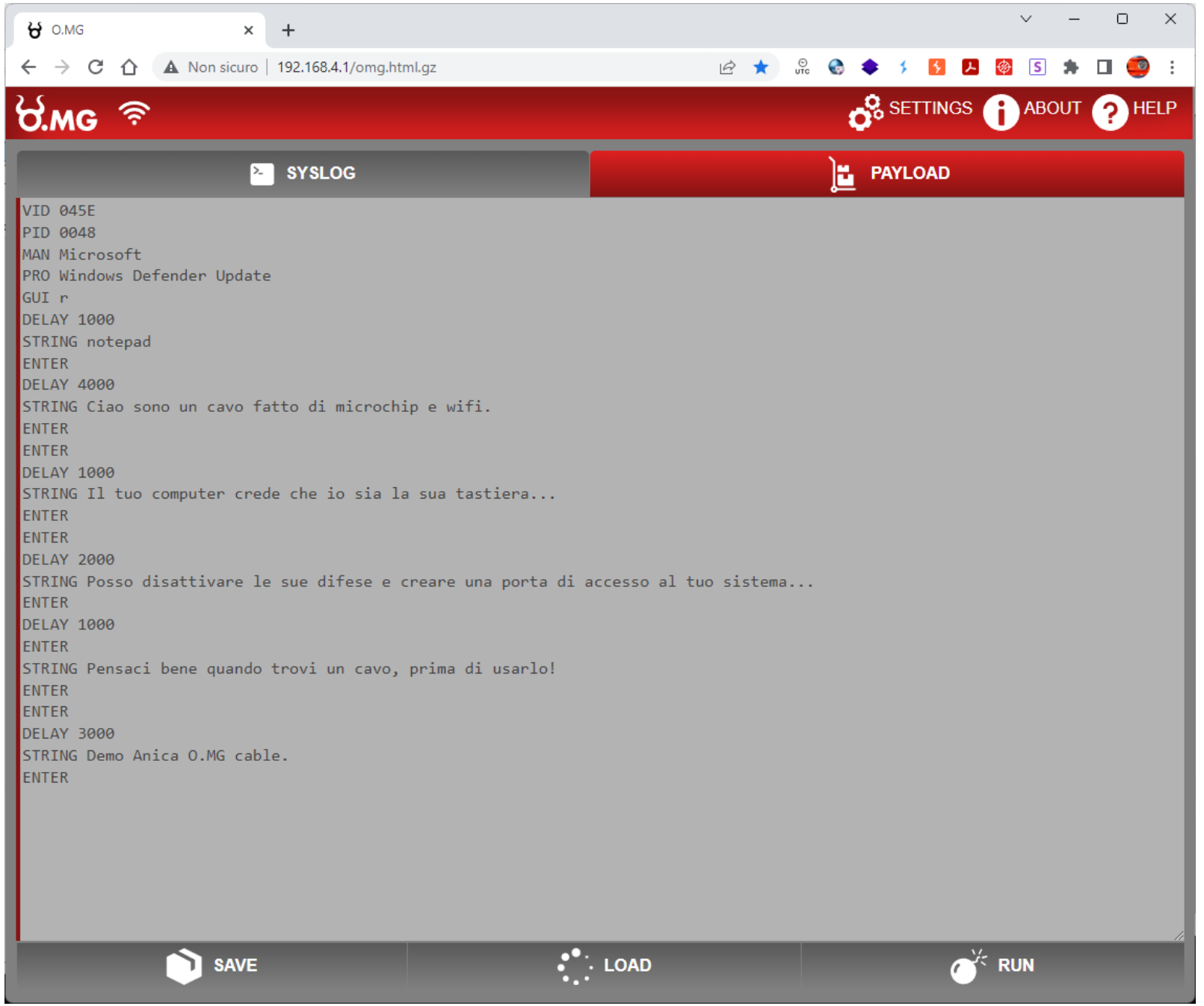
ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

INTERFACCIA WEB
CHE VEDE ATTACCANTE



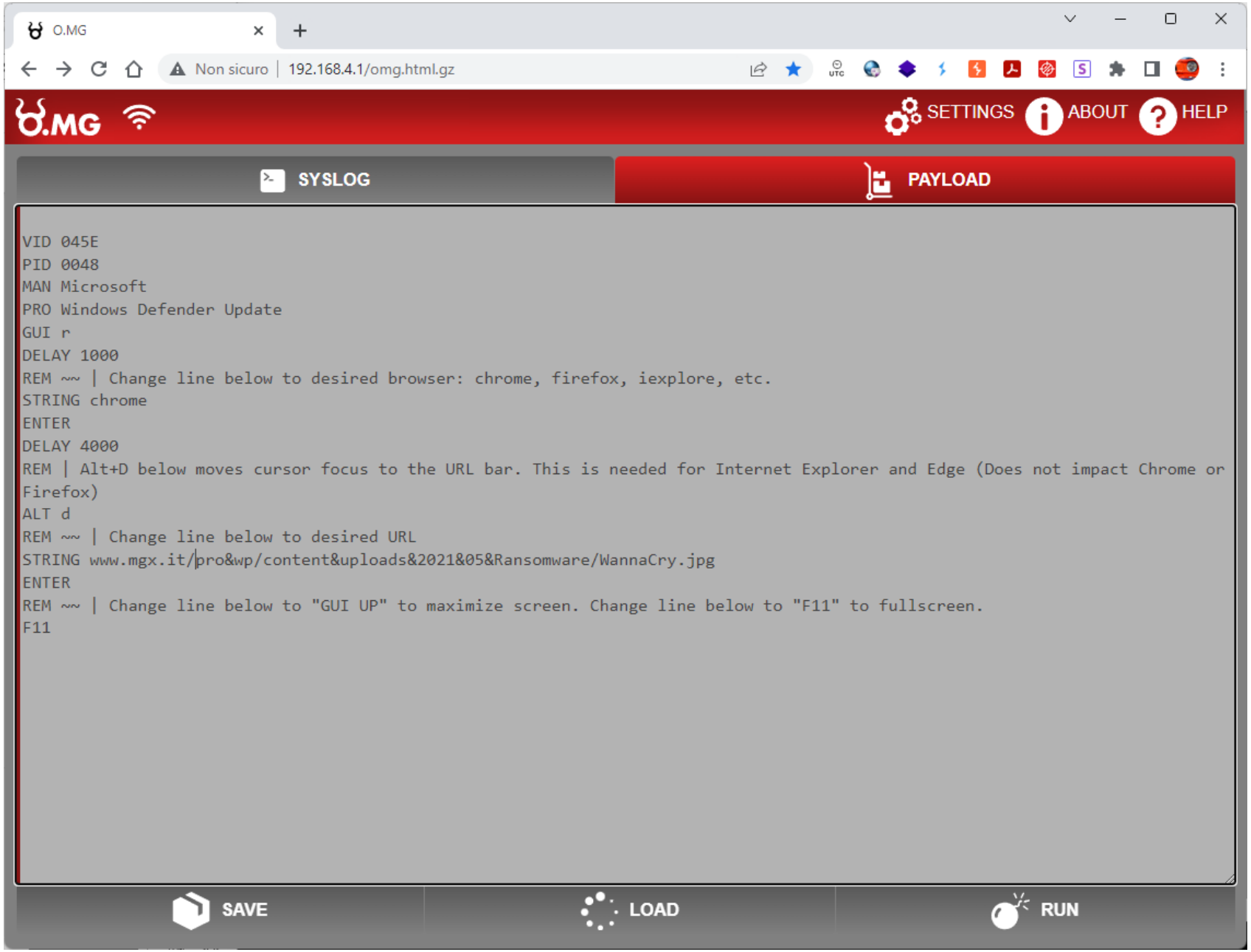
ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

ESEMPIO PRIMO PAYLOAD



ANICA
Associazione Nazionale Industrie Cinematografiche Audiovisive e Digitali

ESEMPIO SECONDO PAYLOAD



NON CI CREDETE?

2 MIN DEMO LIVE