Sicurezza e Vulnerabilità delle Reti

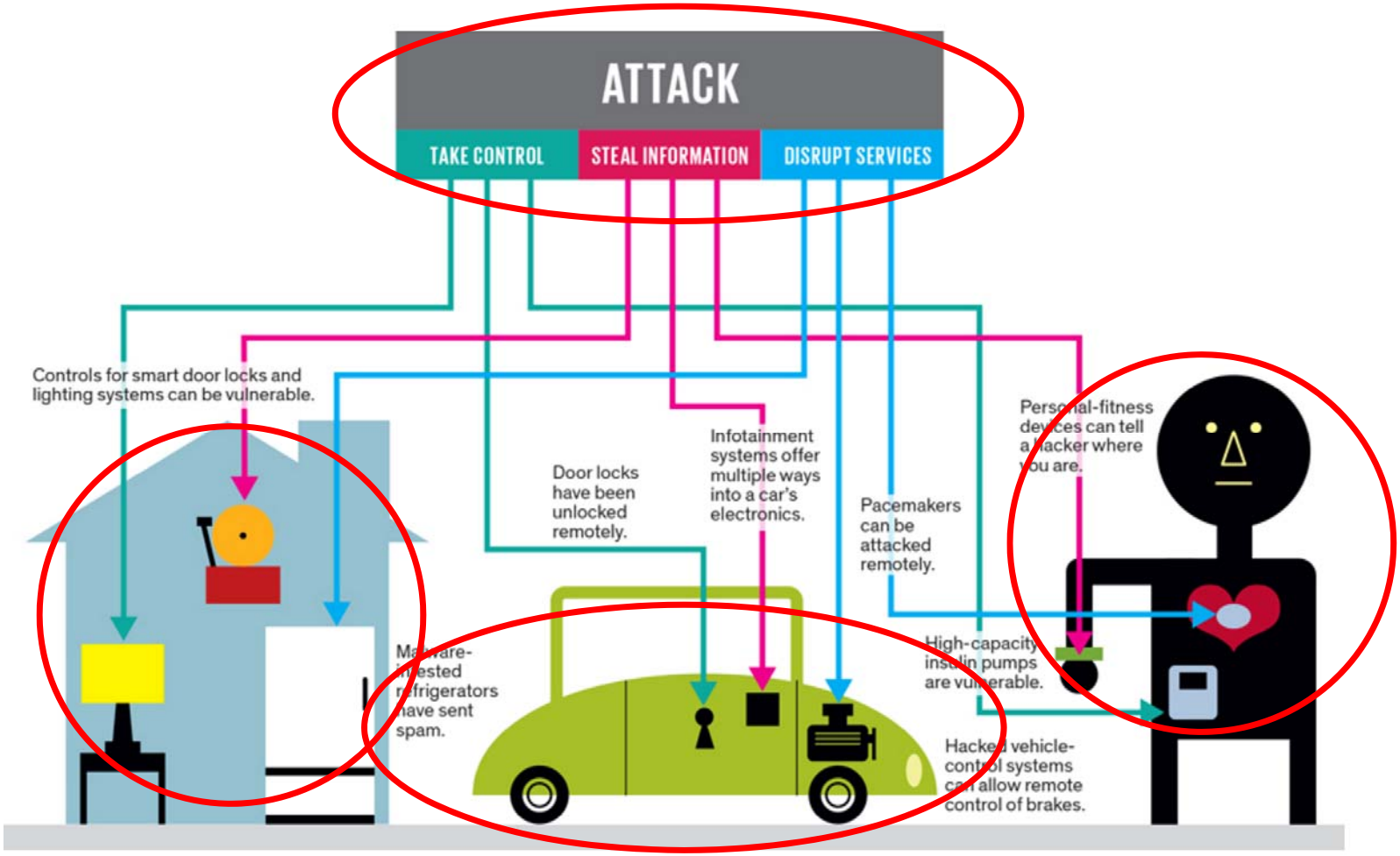
Mario Di Mauro, Ph.D.

Dip. Di Ingegneria dell'Informazione, Electtrica e Matematica Applicata (DIEM), Università di Salerno, (mdimauro@unisa.it)

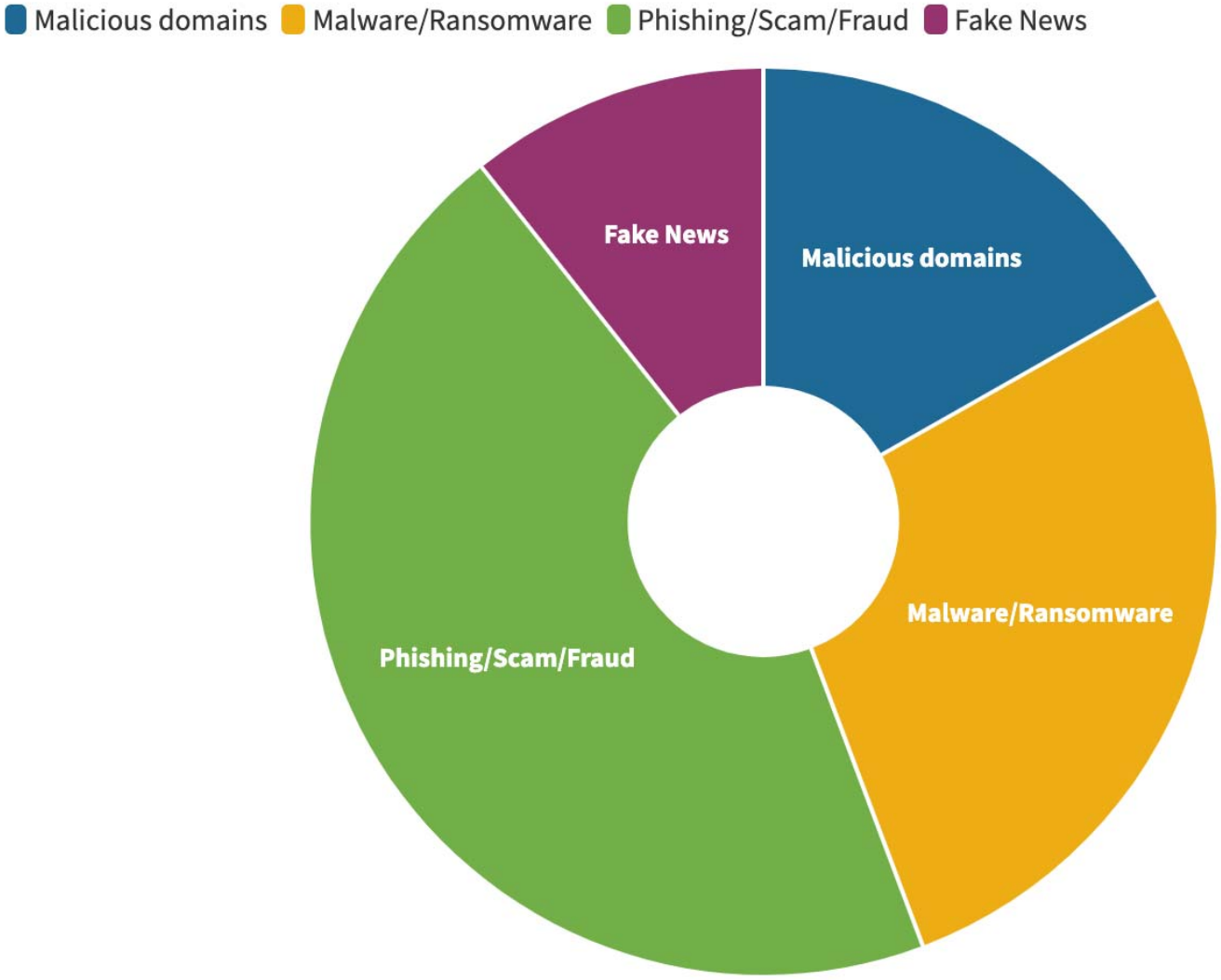
Ordine degli Ingegneri di Salerno

GdL Cyber Security

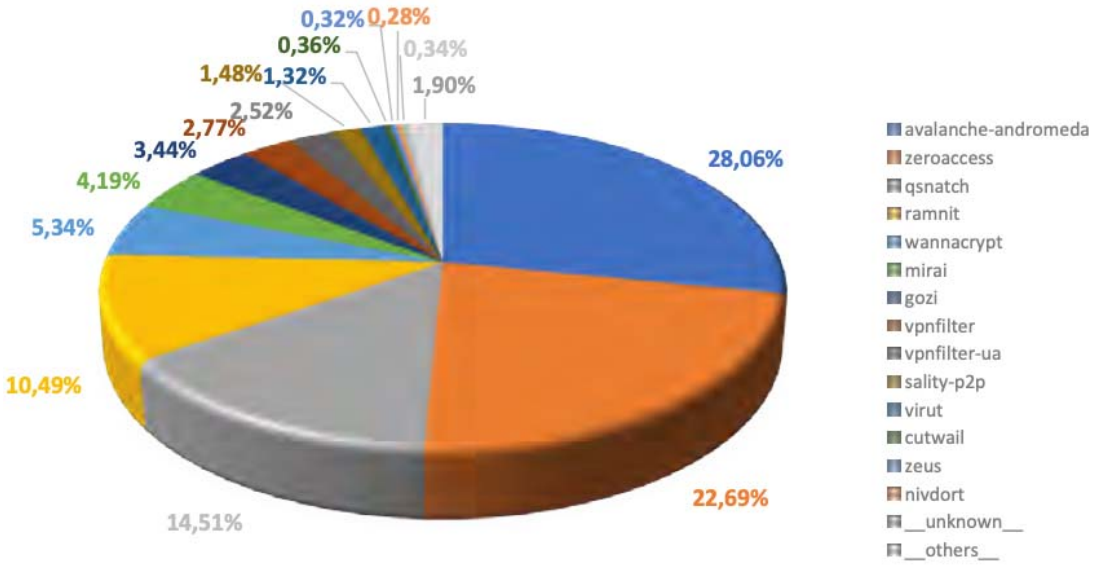
		Characteristics	Weaknesses
Web & Mobile Applications		➢ Closed/Open platforms ➢ High data volume handling ➢ Variable policies	➢ Code ➢ Lack of testing ➢ Weak user/third party authent.
Cloud		➢ Public/Private/Hybrid Cloud	➢ Code ➢ Policy Management
Communications		➢ 2G,3G,LTE,5G ➢ DSL, WiFi, Bluetooth, LWPAN ➢ IP, MQTT, HTTP	➢ Radio vulnerabilities ➢ Protocol vulnerabilities
IoT sensors / Actuators		➢ Limited power ➢ Low bandwidth ➢ Constrained capabilities	➢ Policy management ➢ No updates / poor hardware ➢ Denial of Service
Gateways / Smart Edges		➢ Different commun. prot.	➢ Design faults ➢ Inability to update ➢ Software bugs
Data Types		➢ Sensitive data (video, audio, location, personal info)	➢ Users ➢ Policy management ➢ Data storage



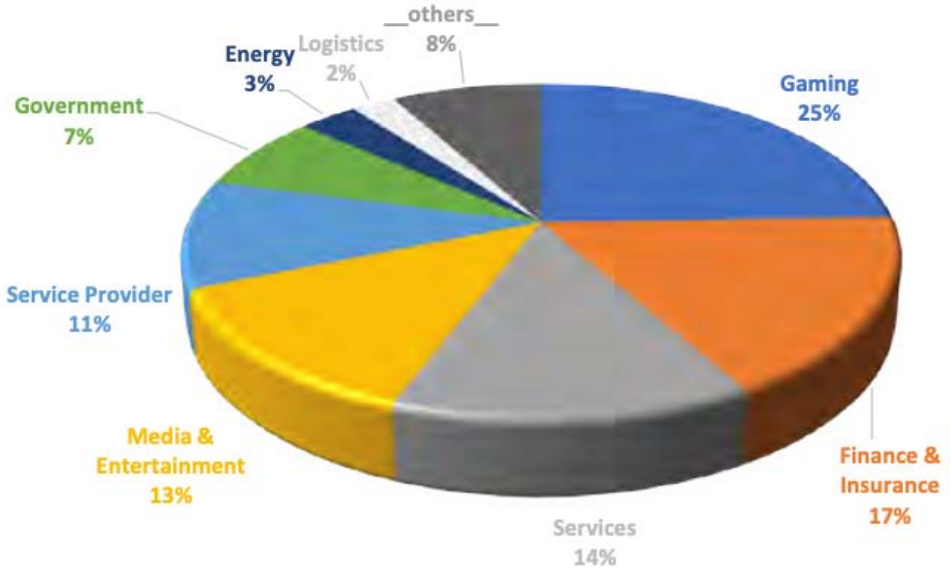
Source: IEEE Spectrum



Distribuzione di attacchi di rete nel mondo durante il periodo Covid-19
(*Fonte*: Rapporto Interpol 2020)



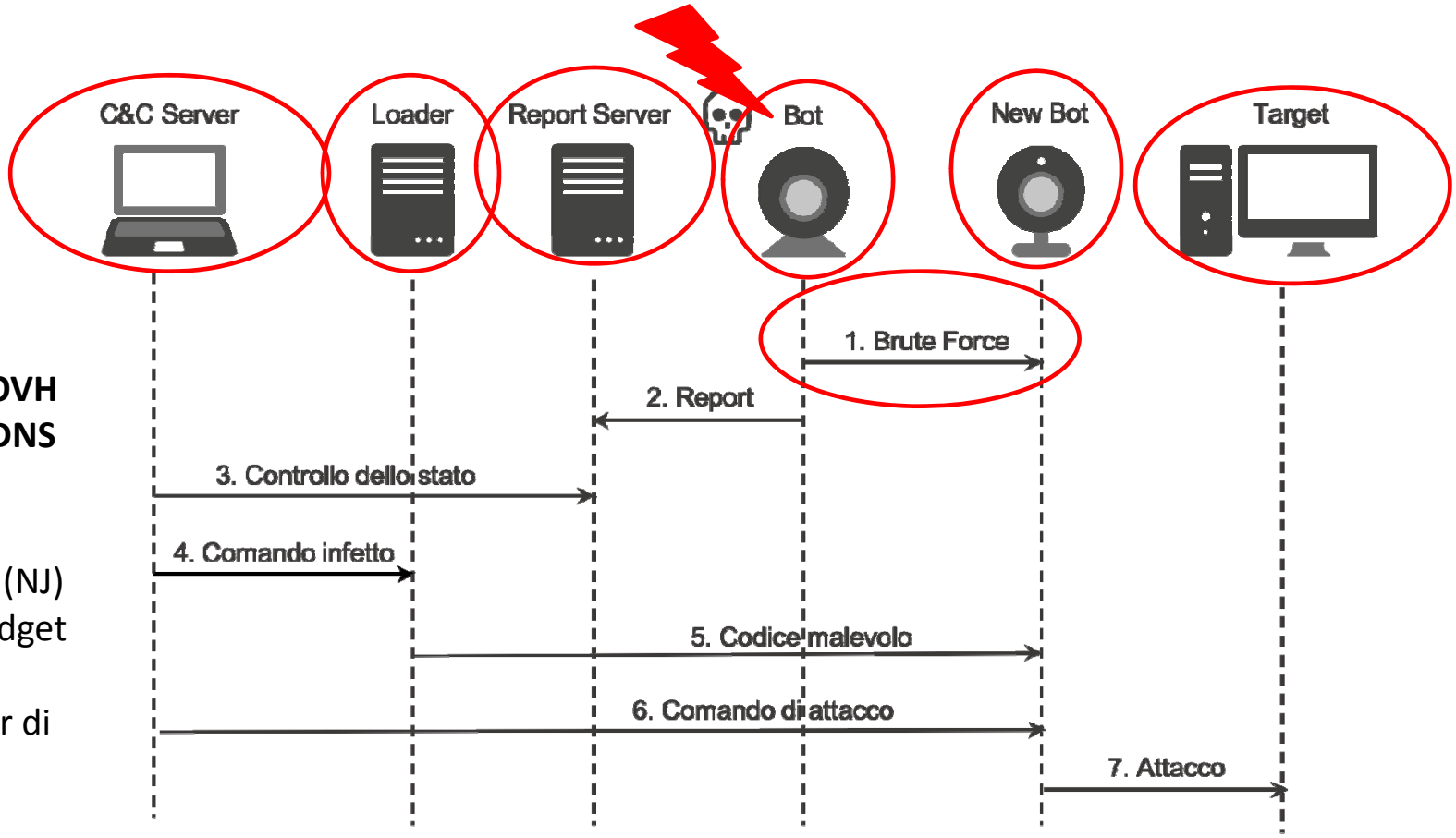
Tipi di Malware (*Fonte*: Rapporto Clusit 2020)



Target di attacchi DDoS (*Fonte*: Rapporto Clusit 2020)

MIRAI
IoT Malware

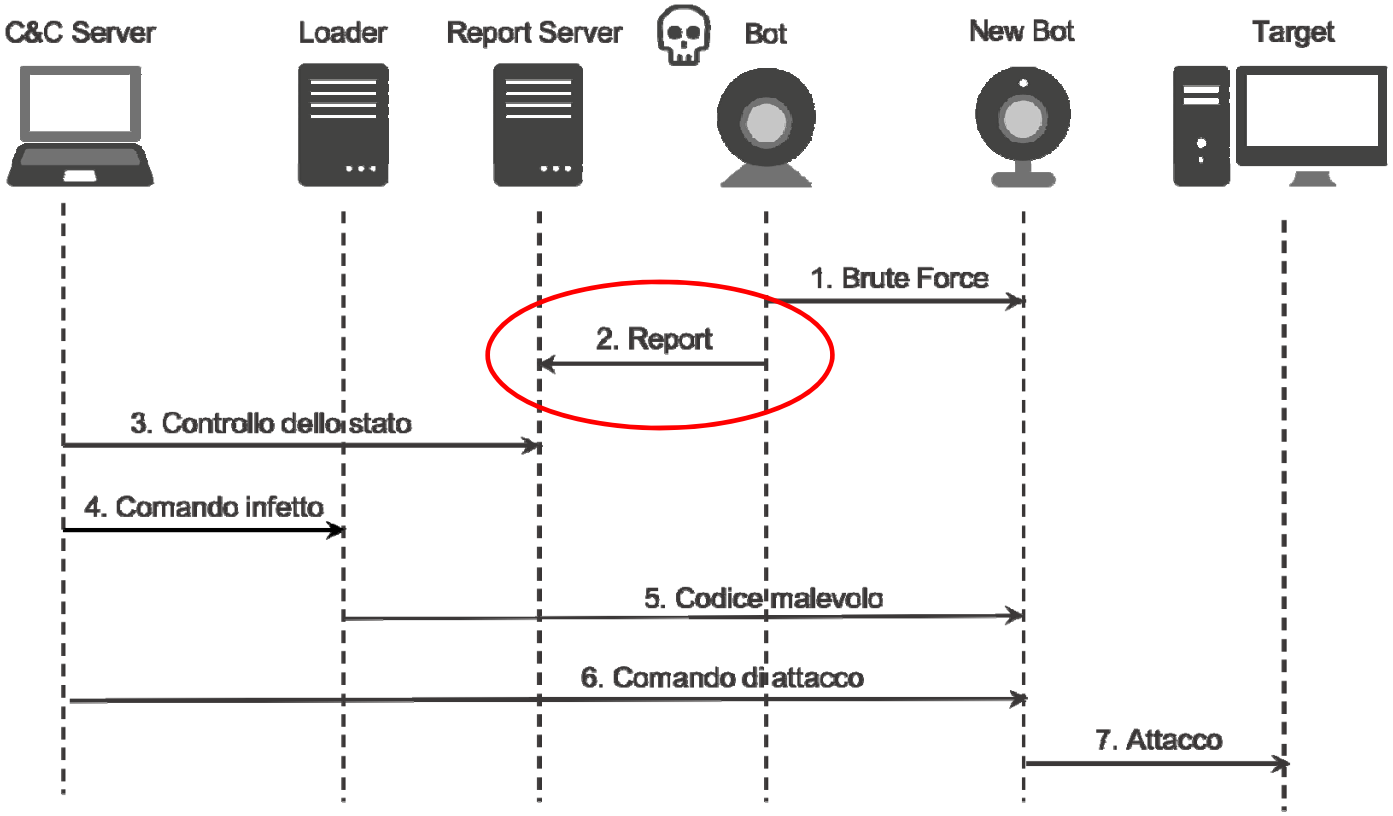
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 1: BF Attack with 62 couples user/pwd

MIRAI
IoT Malware

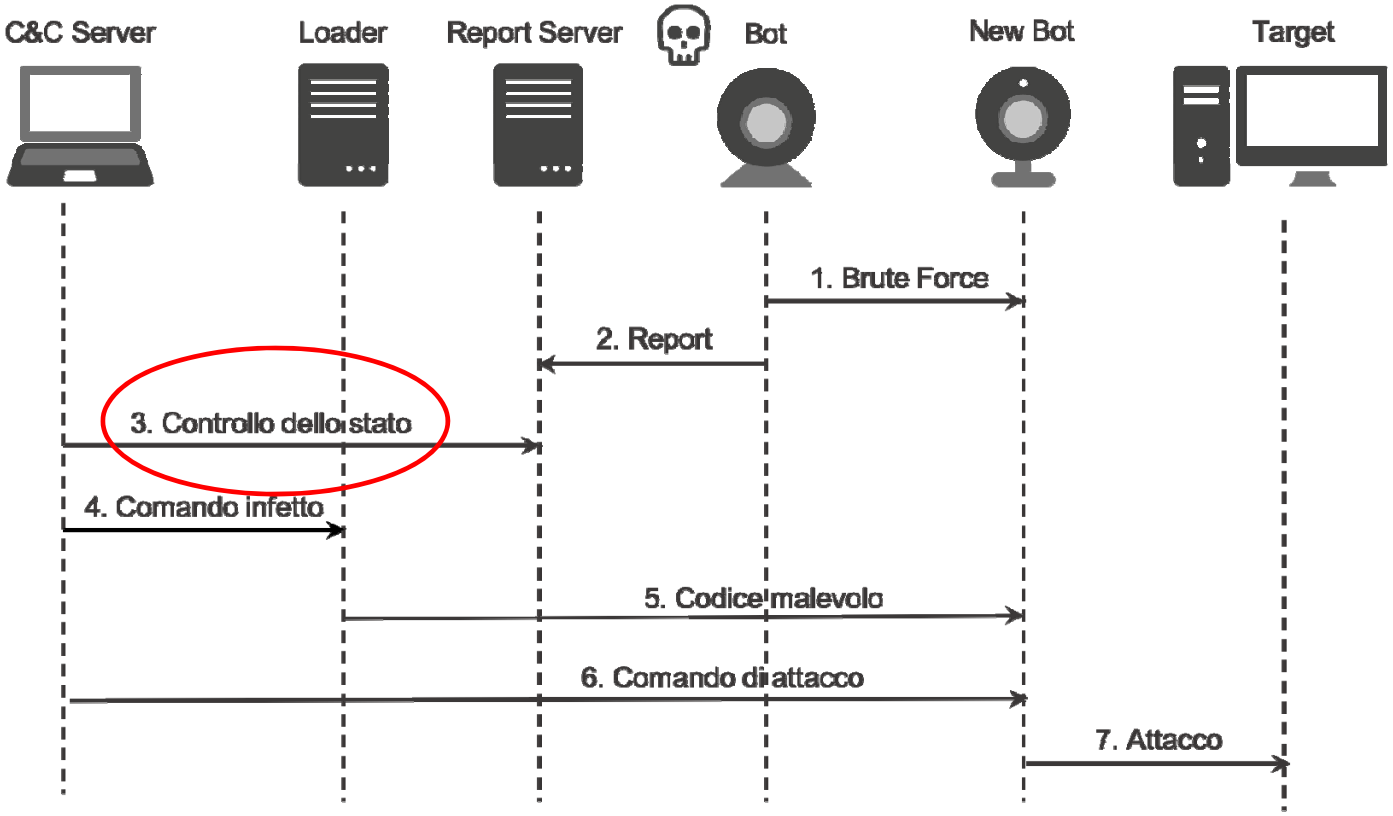
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 2: Features of infected device are retained

MIRAI
IoT Malware

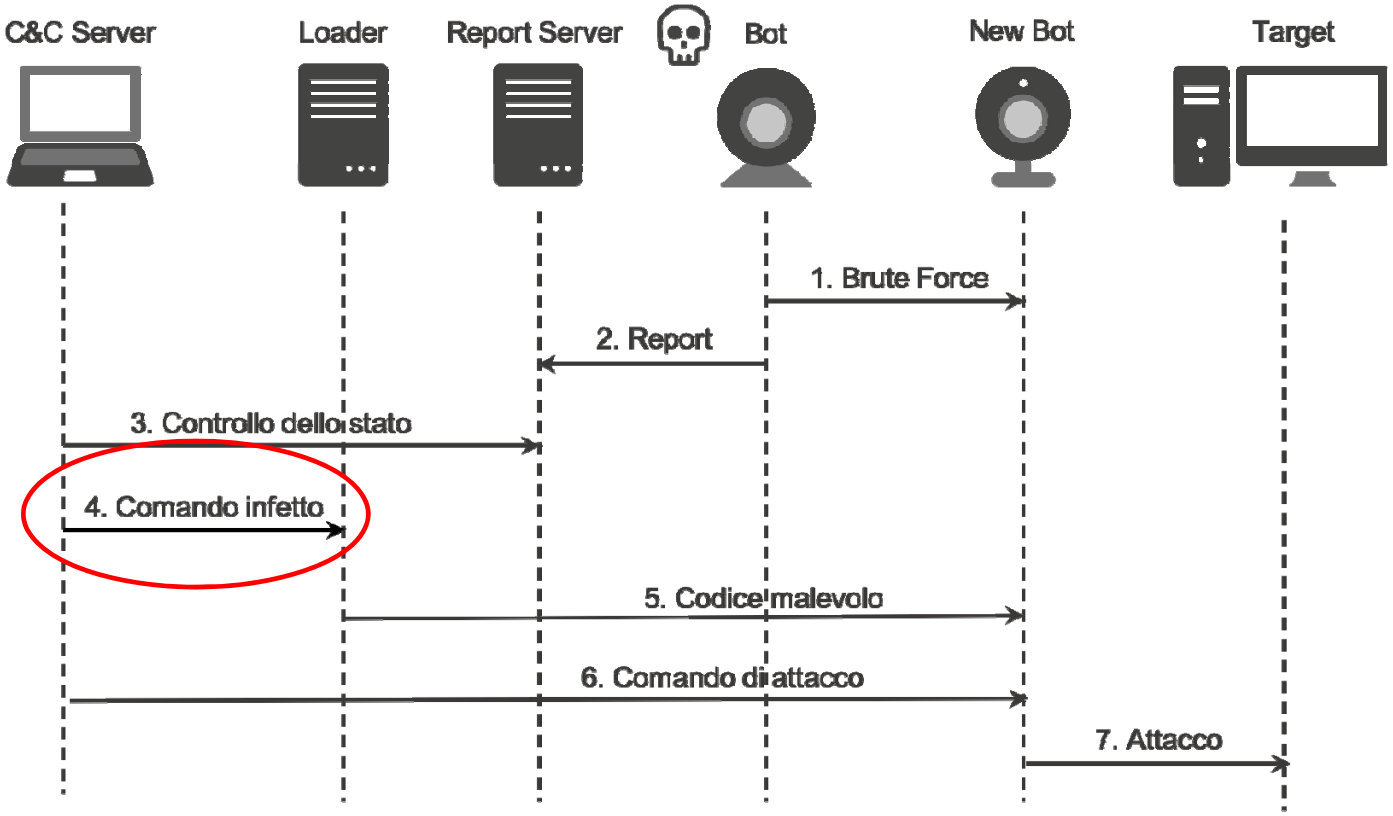
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 3: Status of new infected device is checked

MIRAI
IoT Malware

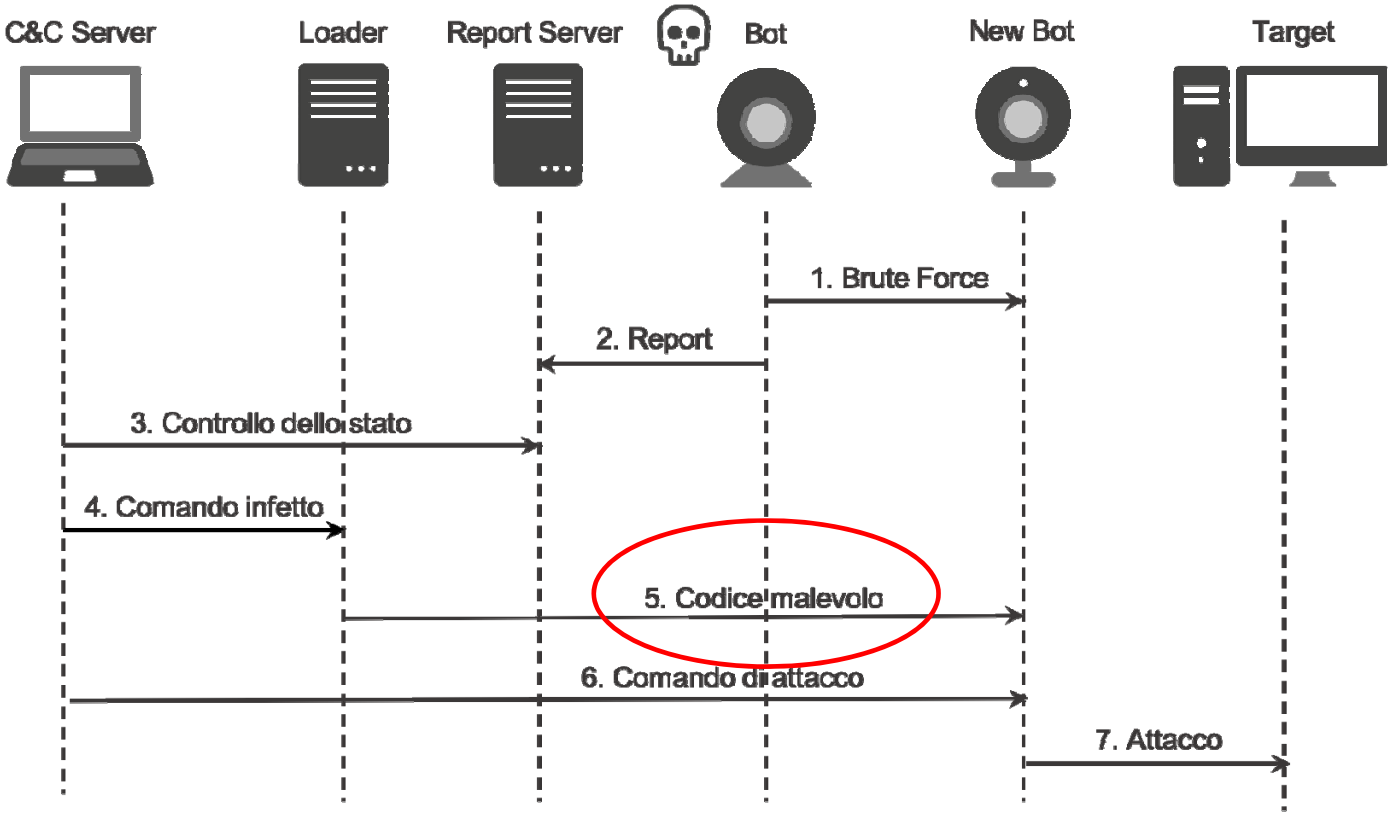
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 4: «Loader» sends to infected device some instructions

MIRAI
IoT Malware

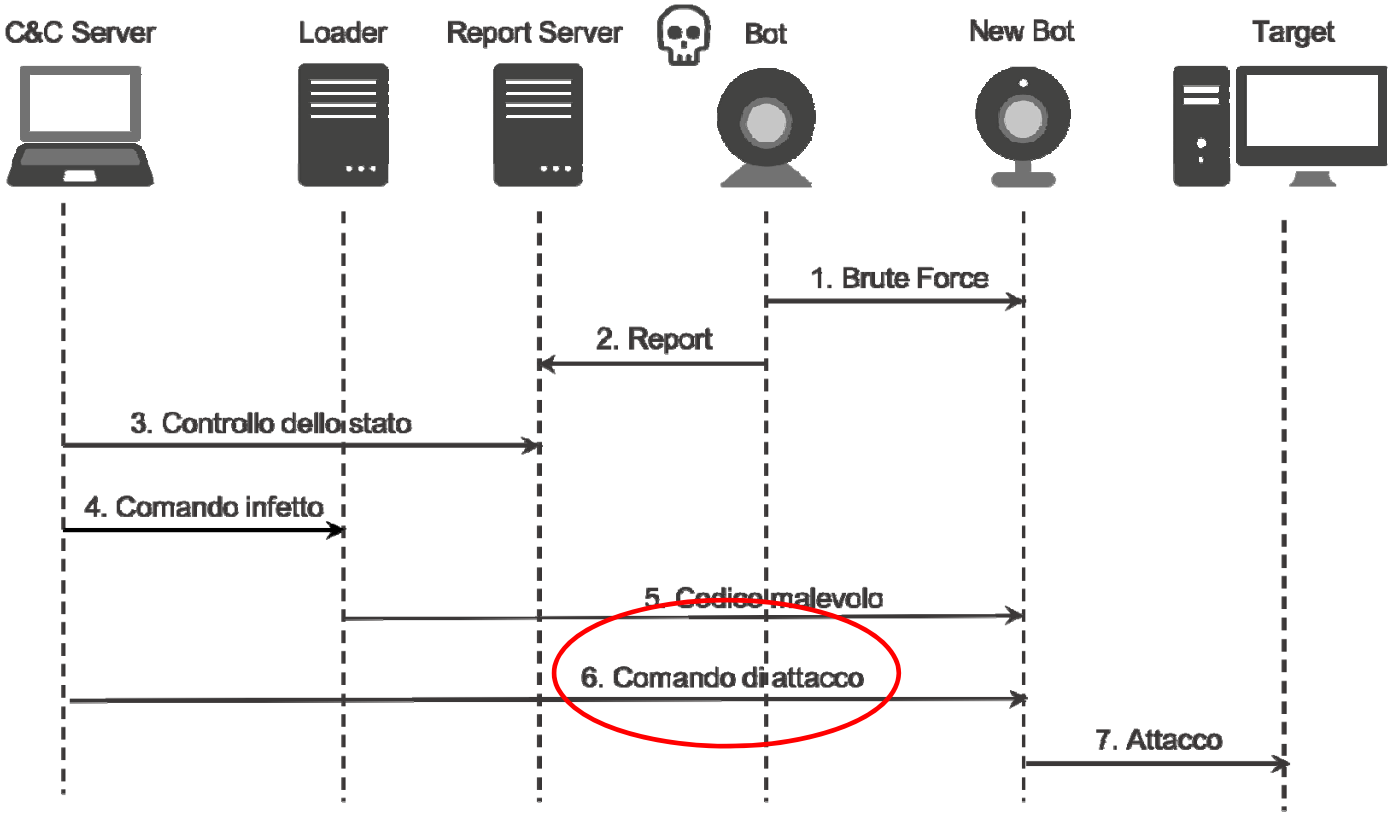
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 5: Loader forces the infected device to download malicious code

MIRAI
IoT Malware

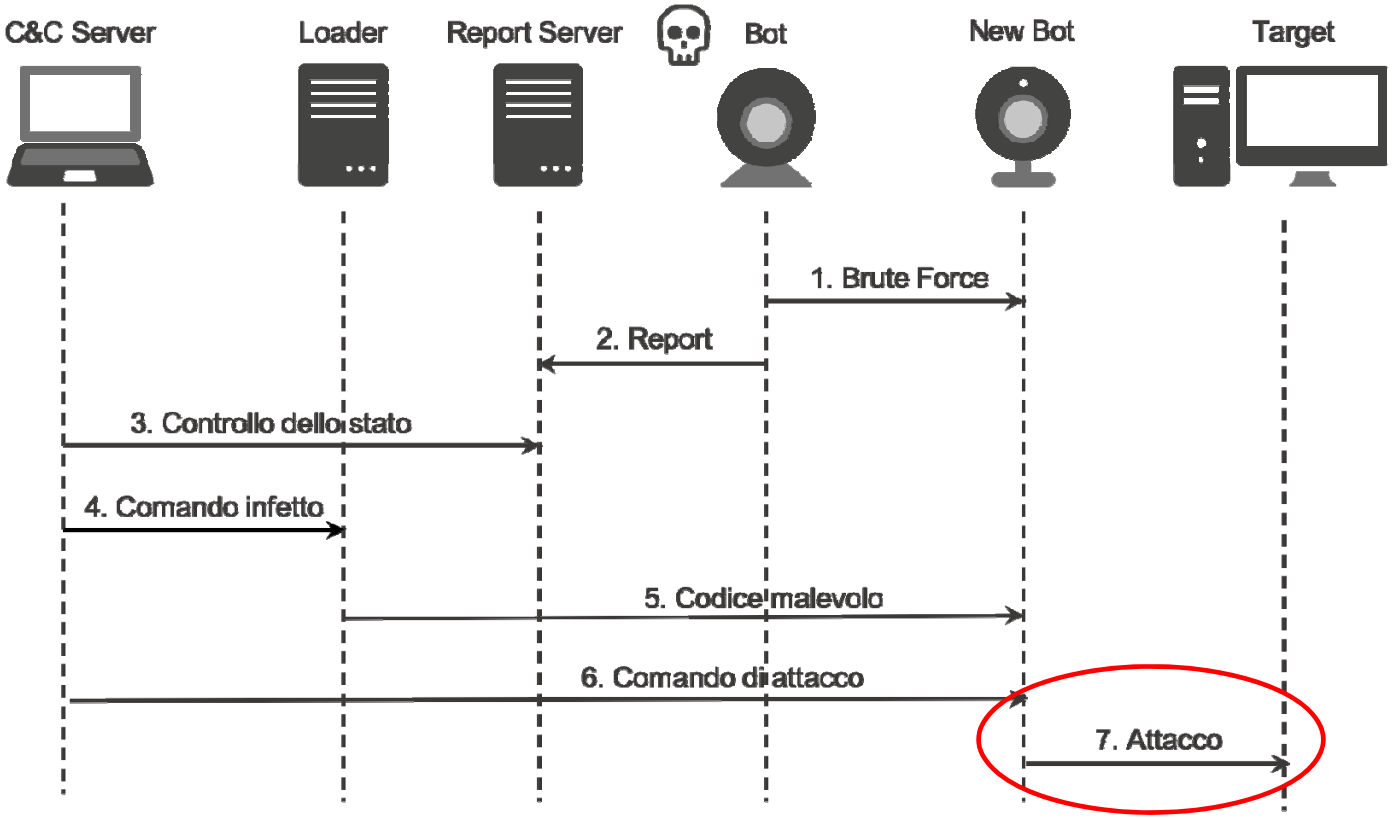
- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 6: C&C sends instructions to launch an attack

MIRAI
IoT Malware

- **DDoS** da 1Tbit/sec contro **OVH**
- Multiple **DDoS** contro **DynDNS** (Github, Netflix, Airbnb,Reddit,Twitter)
- **DDoS** contro **Rutgers Univ.** (NJ) – 1 mln di $ aumento di budget in security
- **DDoS** contro 900.000 router di **Deutsche Telekom**



Step 7: The botnet is ready to launch the attack

Contromisure e nuovi trend

- Potenziare le difese (antivirus di rete, access scanning, IDS) all'*edge* (il punto più «vicino» in cui i dati dei dispositivi distribuiti sono raccolti ed elaborati)
- Adozione di *best practises* ben codificate ed eventualmente normate (es. GDPR)
- Intervento della *Robotic Process Automation* (RPA) nella gestione di attività di routine che comprendono anche processi di sicurezza e conformità
- Utilizzo di tecniche di *Artificial Intelligence* (AI) e *Machine Learning* (ML) a supporto dei sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS)

Grazie per l'attenzione!

Mario Di Mauro, Ph.D.

Dip. Di Ingegneria dell'Informazione, Electtrica e Matematica Applicata (DIEM), Università di Salerno, (mdimauro@unisa.it)

Ordine degli Ingegneri di Salerno