Cybercrime

(aggiornamento 2021)

Prof. Michele Perilli
Università di Foggia
Dipartimento di Giurisprudenza

Introduzione

- Con le tecnologie digitali l'informazione si svincola dal supporto e diventa facile poter riprodurre un contenuto e trasferirlo altrove;
- Con la diffusione della rete Internet tutte le attività lavorative diventano net-centriche e quindi anche le attività illecite;
- Diventa difficile definire il confine territoriale di un'attività in rete.

Come ci difendiamo dal fenomeno

1. La Prevenzione

   (da parte dell'utente e della pubblica sicurezza);

2. La Repressione (Codice Penale).

Come ci difendiamo dal fenomeno

Prevenzione dal lato utente:

- Informare;
- Sensibilizzare;
- Responsabilizzare.

Come ci difendiamo dal fenomeno

Prevenzione dal lato della Polizia Postale e delle Comunicazioni:

- Monitoraggio della rete Internet;
- Data Retention: tenere traccia dei dati inerenti gli spostamenti degli utenti per quanto riguarda la navigazione (indirizzi IP, data-ora e durata della comunicazione, *log-file*).

La prima legge italiana contro il Cybercrime

Legge 547/93

"*Modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica*"

La Legge 547/93: le 4 macro-aree

1. *Frodi informatiche* (truffa su carte di credito);

2. *Falsificazioni (di documenti informatici);*

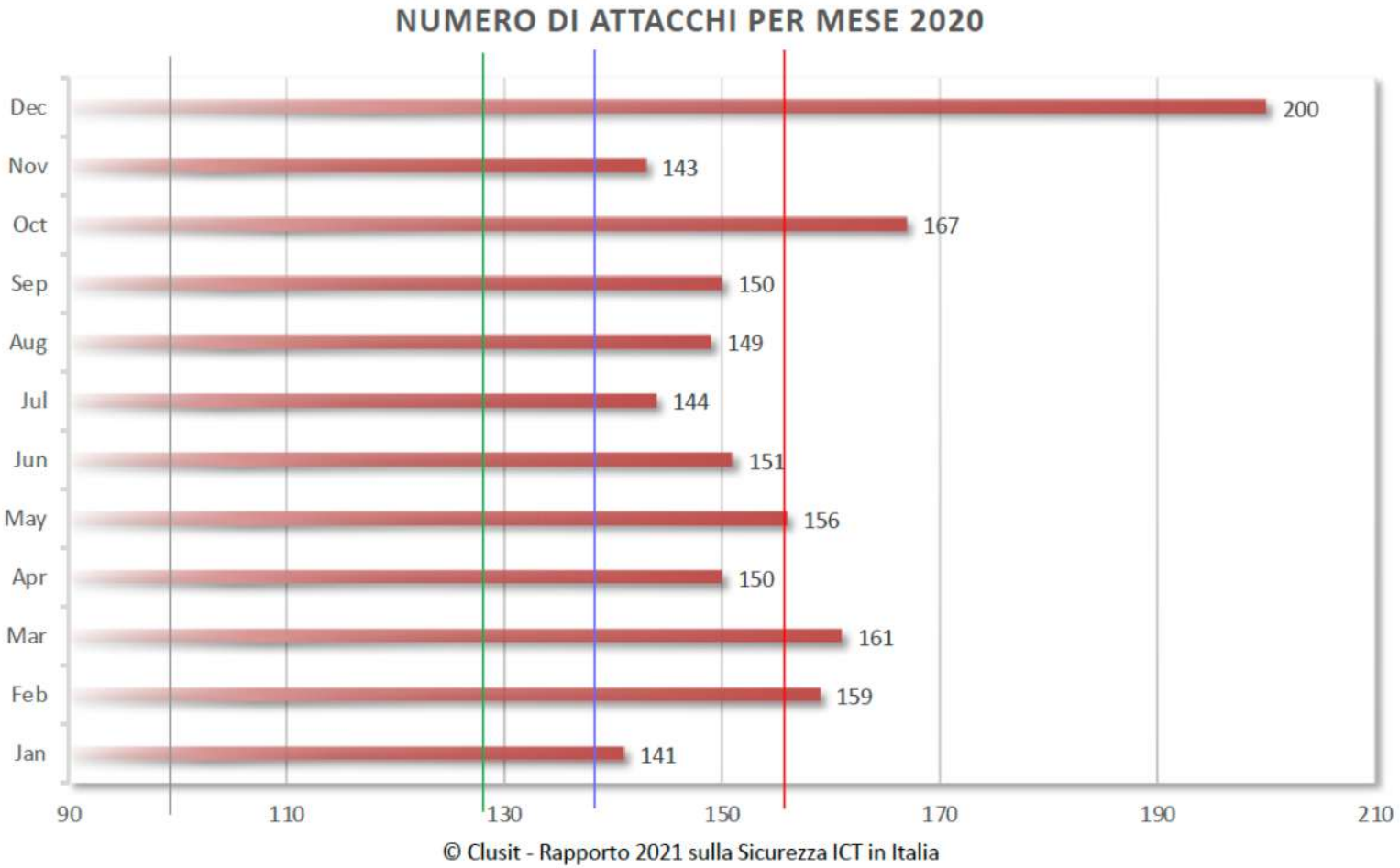
3. *Integrità dei dati e dei sistemi informatici:*
   - danneggiamento di Sistemi Informatici e telematici;
   - diffusione di programmi diretti a danneggiare o interrompere il funzionamento di un sistema informatico;

La Legge 547/93: le 4 macro-aree

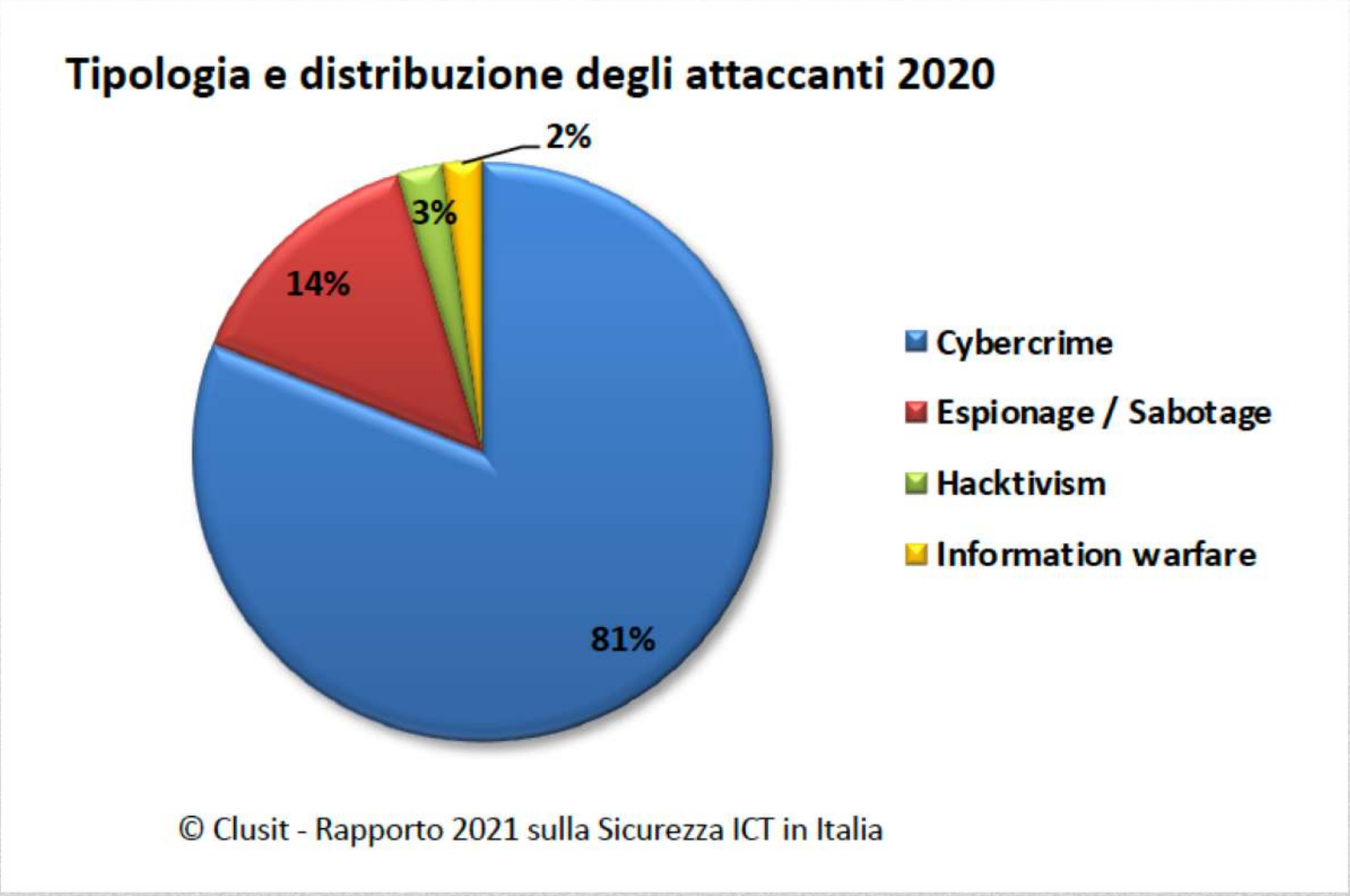
4. Riservatezza dei dati e delle comunicazioni informatiche:

- accesso abusivo ad un sistema informatico o telematico;
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.

il rapporto CLUSIT 2021: il punto della situazione



il rapporto CLUSIT 2021



Alcune definizioni

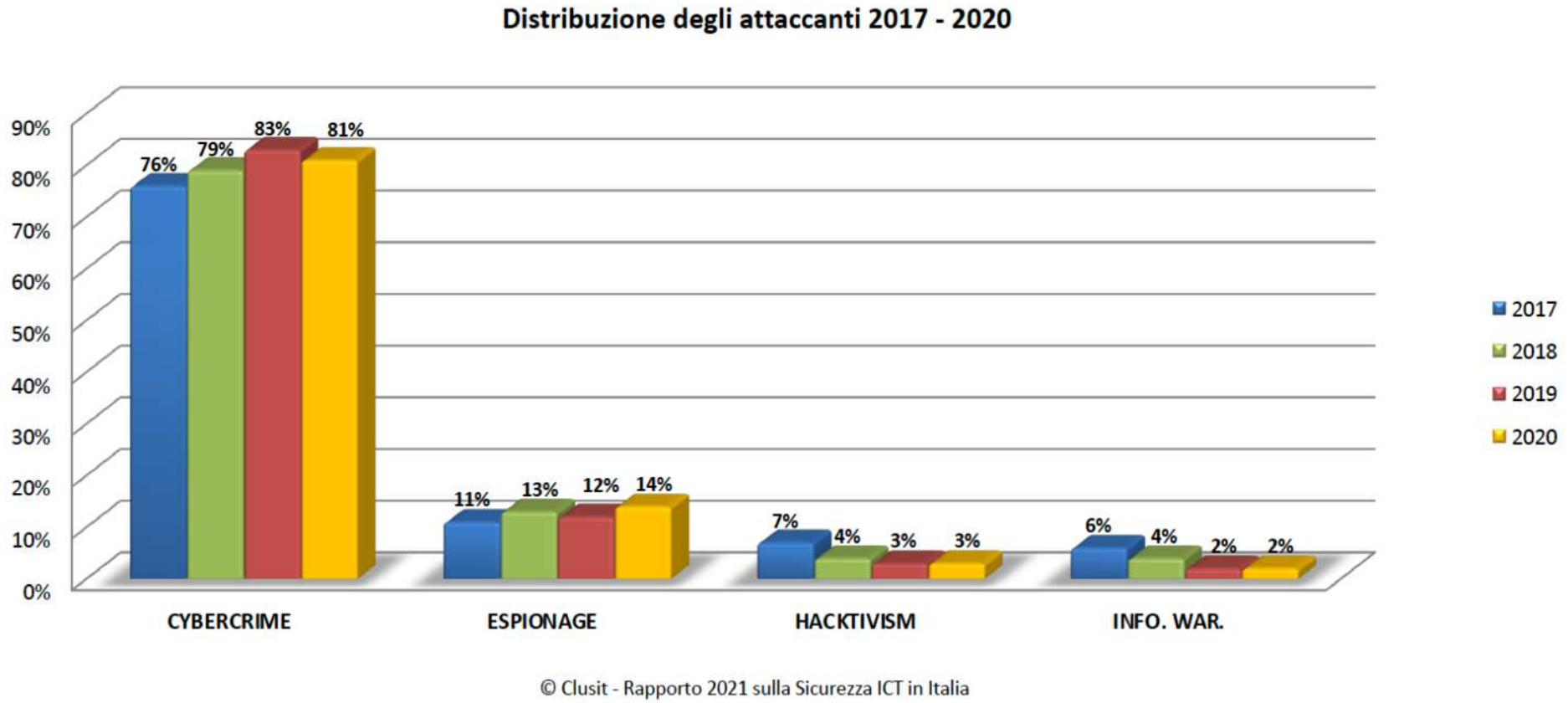
Cyber warfare: è la guerra cibernetica, si traduce nell'alterare e distruggere informazioni e sistemi informatici nemici.

Esempi possono essere gli eventi di vandalismo web atti a modificare e sporcare pagine web ("*Deface*") oppure gli attacchi per mettere fuori uso i server (attacchi DoS, "*Denial of Service")*

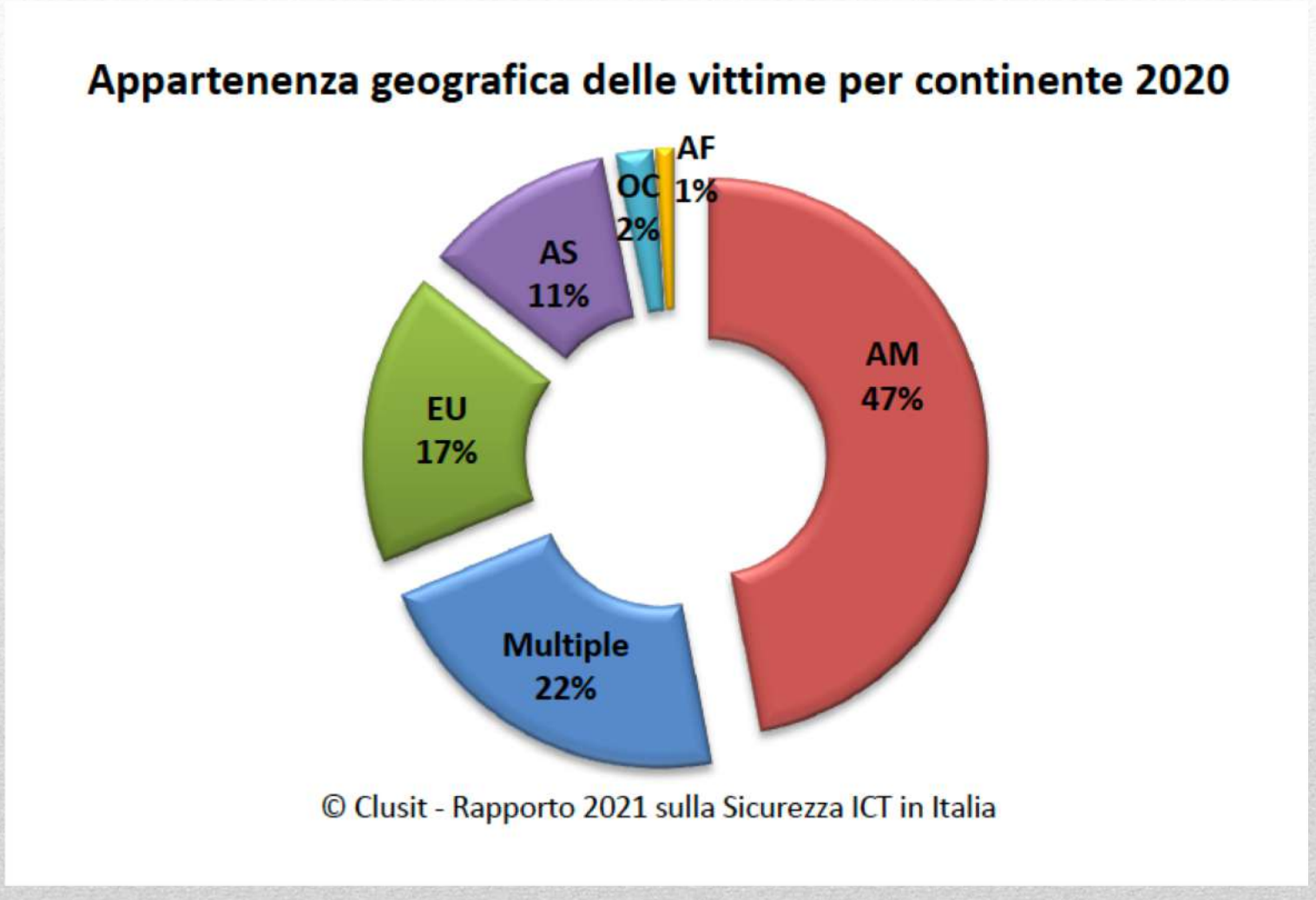
Alcune definizioni

Hacktivism: è la fusione di due parole, *"hacking" e "activism", consiste nell'*attacco ad un sistema informatico con il fine della protesta (esempi sono gli attacchi di Anonymous)

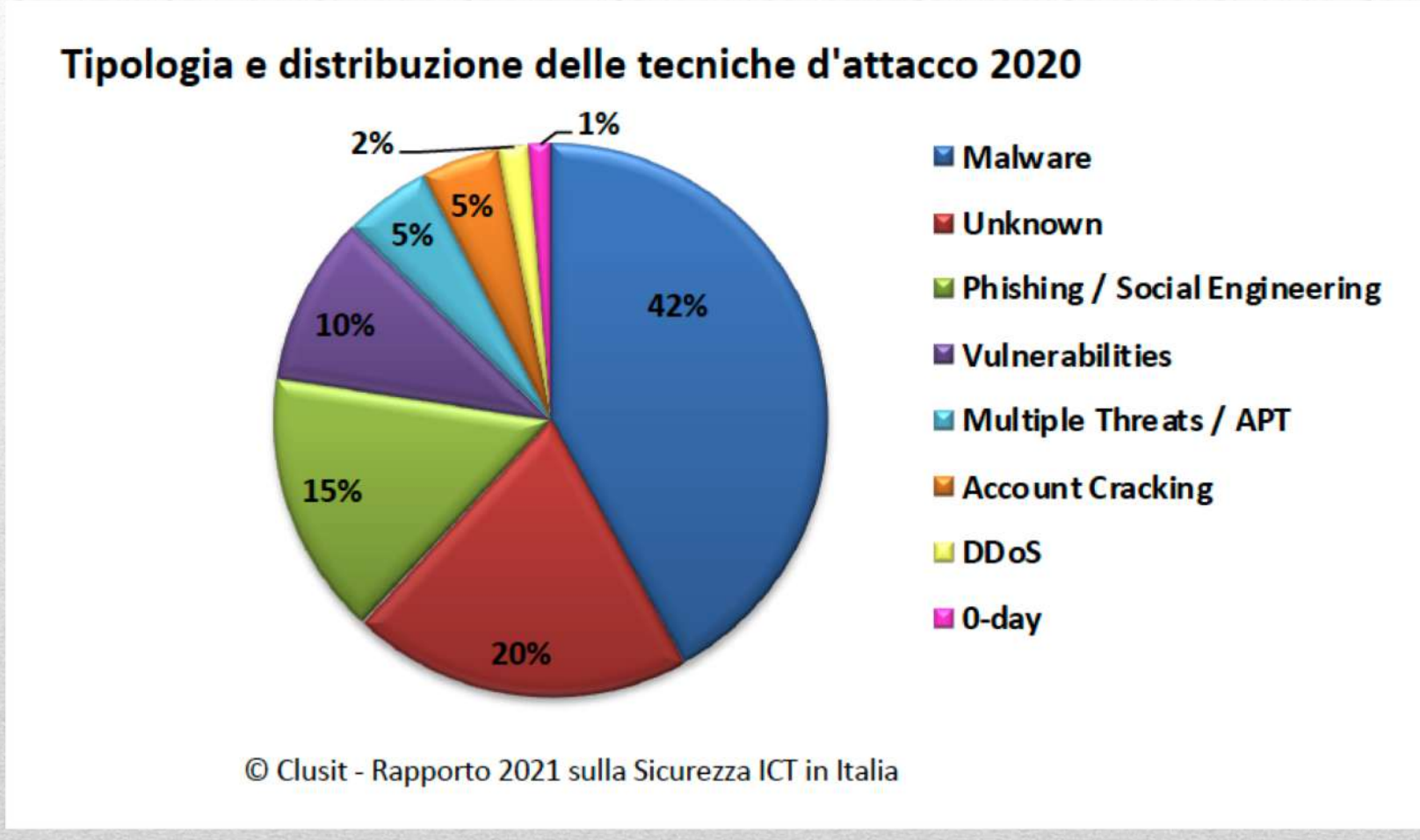
il rapporto CLUSIT 2021



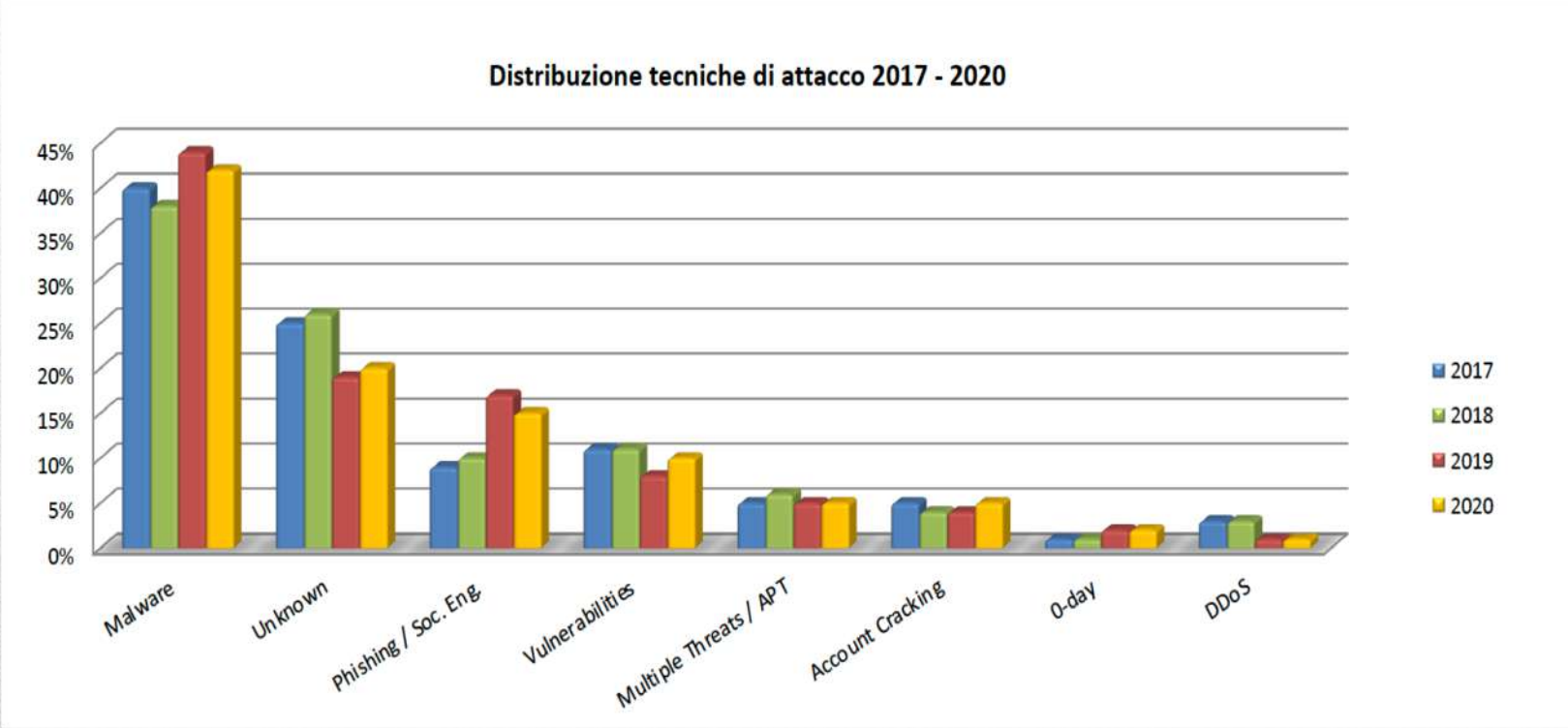
il rapporto CLUSIT 2021



il rapporto CLUSIT 2021



il rapporto CLUSIT 2021



Cos'è un attacco DoS (Denial of Service)

- Il significato italiano è

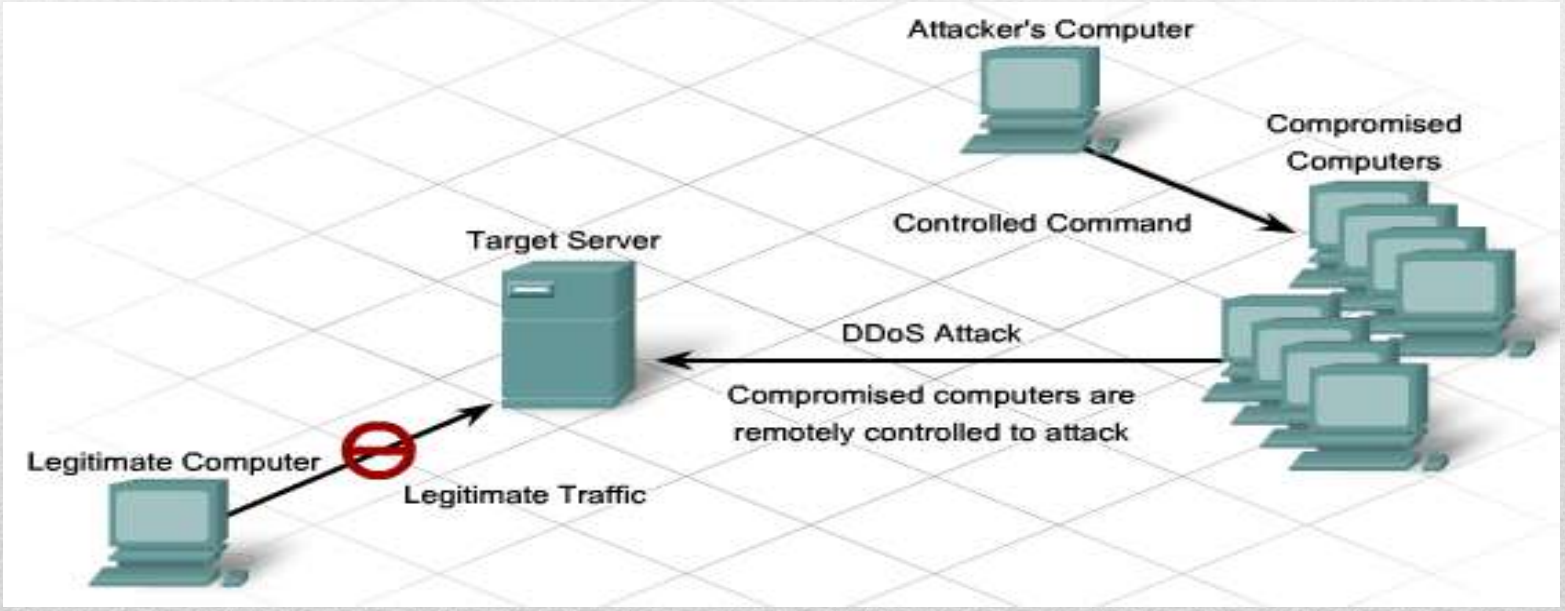
  "**la negazione del servizio**"
- consiste nell'attaccare un sistema in modo da renderlo inutilizzabile, consumando tutte le sue risorse;

L'attacco DoS

- L'hacker attacca il server occupando tutte le sue risorse, in modo che quest'ultimo si rende indisponibile alla richiesta di servizio di un utente reale;
- Di solito i server possono soddisfare un numero massimo di utenti contemporaneamente, accettando un numero massimo di connessioni simultanee;
- L'hacker le satura tutte causando il Diniego del Servizio all'utente reale.

L'evoluzione di un attacco DoS: il DDoS, l'attacco DoS di "*massa*".

E' un'estensione dell'attacco DoS: l'hacker gestisce un numero di computer da lui compromessi per sferrare un attacco di massa al server.



Passiamo ora all'aspetto investigativo

- Come si fa ad individuare da quale sistema e da quale punto della rete Internet un hacker è entrato ?
- Quali sono gli strumenti che gli investigatori hanno a disposizione per individuare i responsabili di un attacco ?

Alcune nozioni: l'indirizzo IP

- Ogni dispositivo che naviga su Internet deve avere l'indirizzo IP. Questo indirizzo deve essere unico in modo da individuare univocamente il dispositivo su tutta la rete Internet. E' conferito dall'ISP (Internet Service Provider)
- L'indirizzo può essere fisso o dinamico;
- L'indirizzo fisso è assegnato ad ogni server;
- A chi si collega da casa (dispositivo con funzione di client) viene assegnato un indirizzo occasionale, quello disponibile in quel momento offerto dall'ISP.

Il DNS: Domain Naming System
"il sistema dei nomi di dominio"

Quando richiediamo l'accesso ad un sito web tipo www.unifg.it, la rete Internet, per raggiungere il server dell'Università degli Studi di Foggia, ha bisogno dell'indirizzo IP del server corrispondente. Tale corrispondenza viene fornita dal cosiddetto server DNS.

Immaginate cosa significa attaccare un server DNS e cambiare tutte le corrispondenze dei domini dei server con i relativi indirizzi.

Il log-file: le tracce degli accessi

- È il giornale di bordo di un sistema informatico, spesso si parla di web-log;
- Contiene la registrazione cronologica delle operazioni man mano che vengono eseguite;
- Consente di stabilire a che ora ed in che giorno un determinato utente si è collegato alla rete tramite un provider;
- Ci dice quanto tempo l'utente è rimasto connesso alla rete e con quale indirizzo IP;
- Ci dice a quali siti l'utente ha avuto accesso, cosa ha scaricato, quali chat o newsgroup ha frequentato;

Iniziamo l'attività investigativa: il tracciamento

Per tracciamento si intende l'insieme della l'attività messe in campo durante l'investigazione, finalizzate ad individuare l'autore di un reato commesso in rete. Vediamone i passi.

E' determinante ai fini investigativi definire a priori se parliamo di un'attività investigativa per un reato già commesso o un reato ancora in atto.

La nostra ipotesi di reato

Ipotizziamo che è stato sferrato un attacco al sito dell'Università degli Studi di Foggia: www.unifg.it e l'indagine inizia quando l'attacco si è già concluso.

I passi:

1) Informata l'A.G. sul reato commesso ed ottenuta l'autorizzazione a procedere tramite decreto del Pubblico Ministero, si chiedono le seguenti informazioni al proprietario del sito:

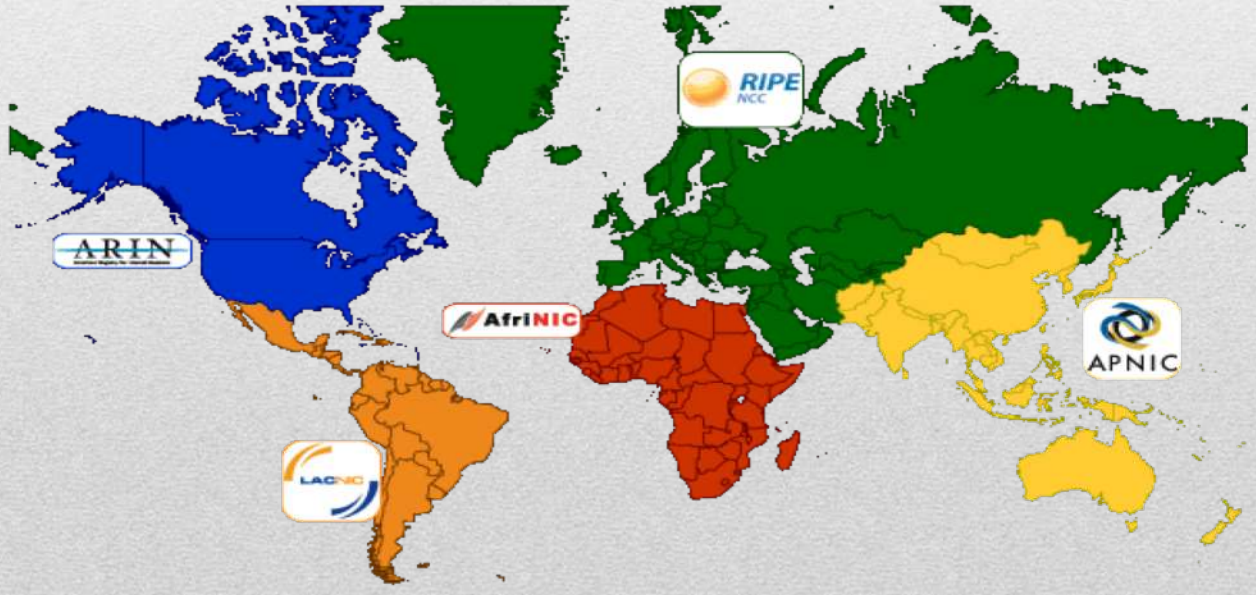
La nostra ipotesi di reato

- Data e ora dell'attacco;
- Id operazione, di solito un codice che identifica l'operazione all'interno del portale;
- **Indirizzo IP del client** che ha sferrato l'attacco;
- I dati personali inseriti al momento della registrazione del sito (se si tratta di accesso ad un sito con registrazione).

2) Ottenuto l'indirizzo IP dell'attaccante si dovrà ora rintracciare (attività di tracciamento) a quale dispositivo corrisponde quell'indirizzo.
3) Parte ora l'indagine di tracciamento

Il tracciamento dell'indirizzo IP: premessa

I blocchi degli indirizzi IP nel mondo sono divisi tra i vari Regional Internet Registries, i quali a loro volta li dividono in sotto-blocchi di indirizzi ai National Internet Registries, i quali li distribuiscono ai vari ISP (Internet Service Provider).



Il tracciamento dell'indirizzo IP

4) Una volta acquisita la corrispondenza tra l'indirizzo IP e l'ISP, l'investigatore chiede all'autorità giudiziaria di accedere ai file di log del Provider per ricercare l'indiziato.
5) Nel file di log si evince il numero telefonico dell'utenza associata in quell'istante a quell'indirizzo IP e quindi all'intestatario del contratto.
6) A questo punto tutti potrebbero pensare che il caso è chiuso, **ma…**

La nostra ipotesi di reato

Potrebbe accadere che:

- I documenti utilizzati per il contratto telefonico siano falsi;
- L'utenza telefonica sia stata intestata ad un soggetto a cui sono stati rubati i documenti;
- Il titolare dell'utenza sia deceduto e i dati dell'utenza non sono stati aggiornati;
- L'indirizzo IP trovato non appartiene ad un'utenza residenziale ma ad un Internet Point che non ha richiesto alcun dato identificativo al proprio cliente;
- L'utente telefonico identificato non ha adottato misure minime di sicurezza per la propria rete Wi-Fi (rete non protetta da password).

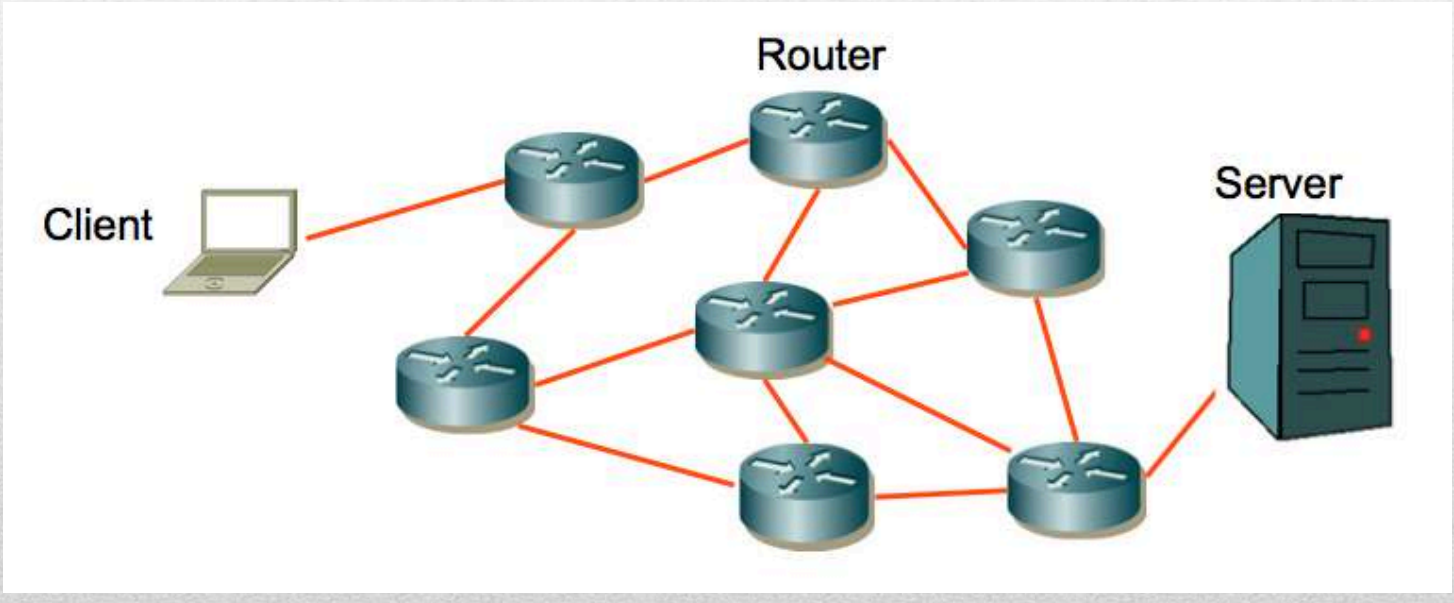
Il problema dell'occultamento delle tracce: Antiforensics

Per attività *"Antiforensics"* si intendono tutte le tecniche che servono ad eludere l'investigazione come:

- Data hiding, occultare i dati con tecniche crittografiche;
- Distruzione dei dati, che può riguardare log-file, tracce di navigazione, washing di vario tipo del sistema operativo;
- Corruzione e modifica dei dati sulla rete (modifica dei pacchetti di dati);
- Occultamento/mascheramento dell'indirizzo IP.

La rete Tor (The Onion Router)

Gli ISP gestiscono dei dispositivi denominati Routers (instradatori, che cercano la rotta). Hanno il compito di trovare la migliore strada per consegnare a destinazione i pacchetti di dati dell'utente.



La rete Tor (The Onion Router)

- La rete ***Tor*** è costituita da un numero elevato di router gestiti da volontari i quali definiscono percorsi casuali e crittografati tra i diversi routers.
- Pertanto le informazioni trasmesse all'interno della rete non sono tracciabili ed è quindi impossibile risalire al mittente;
- La rete ***Tor*** impedisce a chiunque osservi la connessione di sapere quali siti si stanno visitando, in quanto questi dati sono protetti da tecniche crittografiche;
- La rete ***Tor*** consente di accedere ai siti con IP reindirizzato, o meglio cambiato più volte (mascheramento dell'indirizzo IP);
- La rete ***Tor*** consente inoltre l'anonimato anche ai server, in modo da renderli non localizzabili.

La rete Tor (The Onion Router)