Dispensa e video per FAD: stima durata del lavoro complessivo pari a 4 ore.

Verifica con test a risposta multipla in data da definire alla fine della sospensione delle attività didattiche

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

Prof.ssa Agnese Di Donato

Video
MODULO 5 SEZIONE 2_MALWARE
https://www.youtube.com/watch?v=52TfD2Zn7iI
Durata: 24:21 min

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

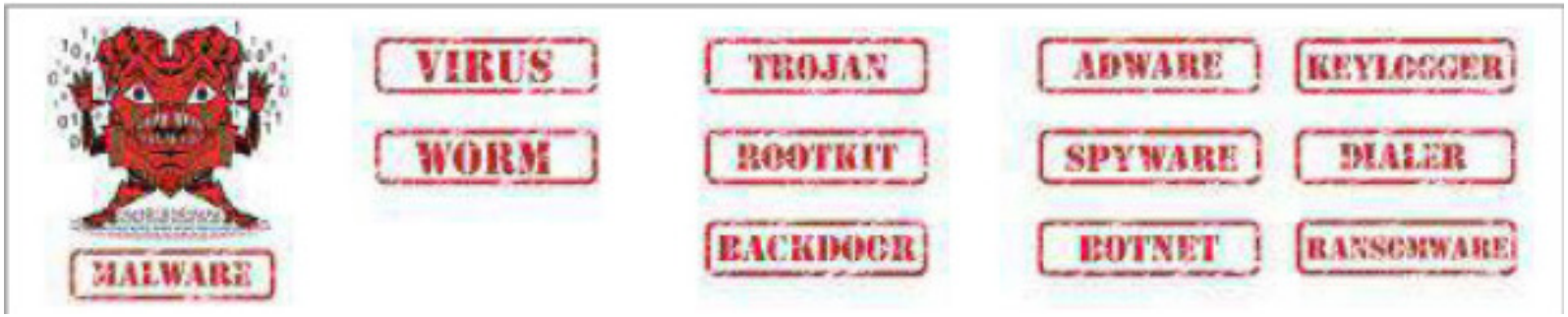
1. CONCETTI DI SICUREZZA
2. MALWARE
3. SICUREZZA IN RETE
4. CONTROLLO DI ACCESSO
5. USO SICURO DEL WEB
6. COMUNICAZIONI
7. GESTIONE SICURA DEI DATI

NUOVA ECDL
MODULO IT SECURITY
Syllabus 2.0

SEZIONE 2
MALWARE

Prof.ssa Agnese Di Donato

SEZIONE 2 – MALWARE
TEMA 2.1 TIPI E METODI



I malware agiscono…

Interruzione dei servizi! (DoS – Denial of Services o DDoS – Distributed Denial of Services)

…rendendo indisponibili i servizi di sicurezza (crittografia,…)

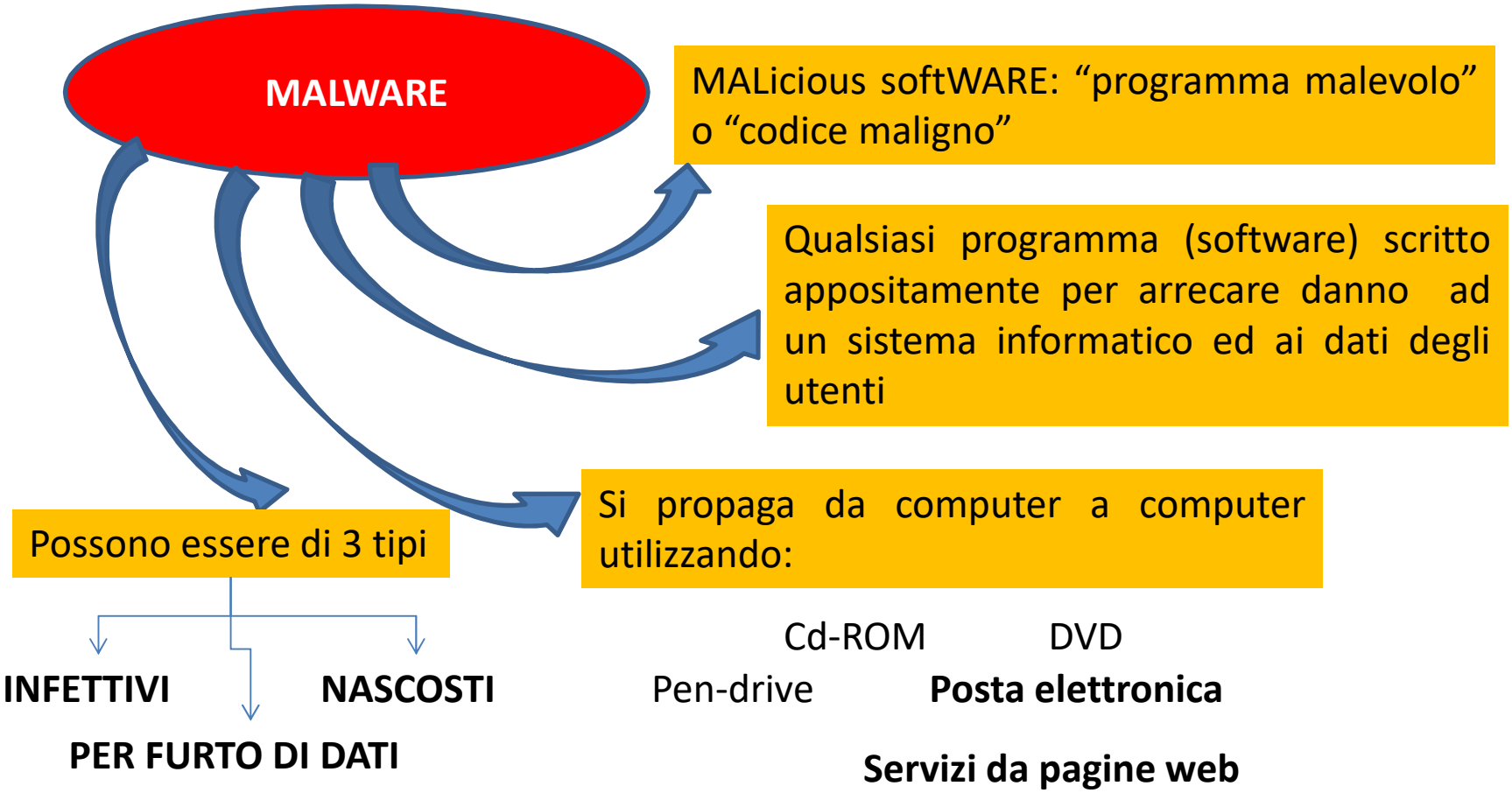
Furto di dati ed informazioni!

…rubando password e chiavi di rete

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer



SEZIONE 2 – MALWARE

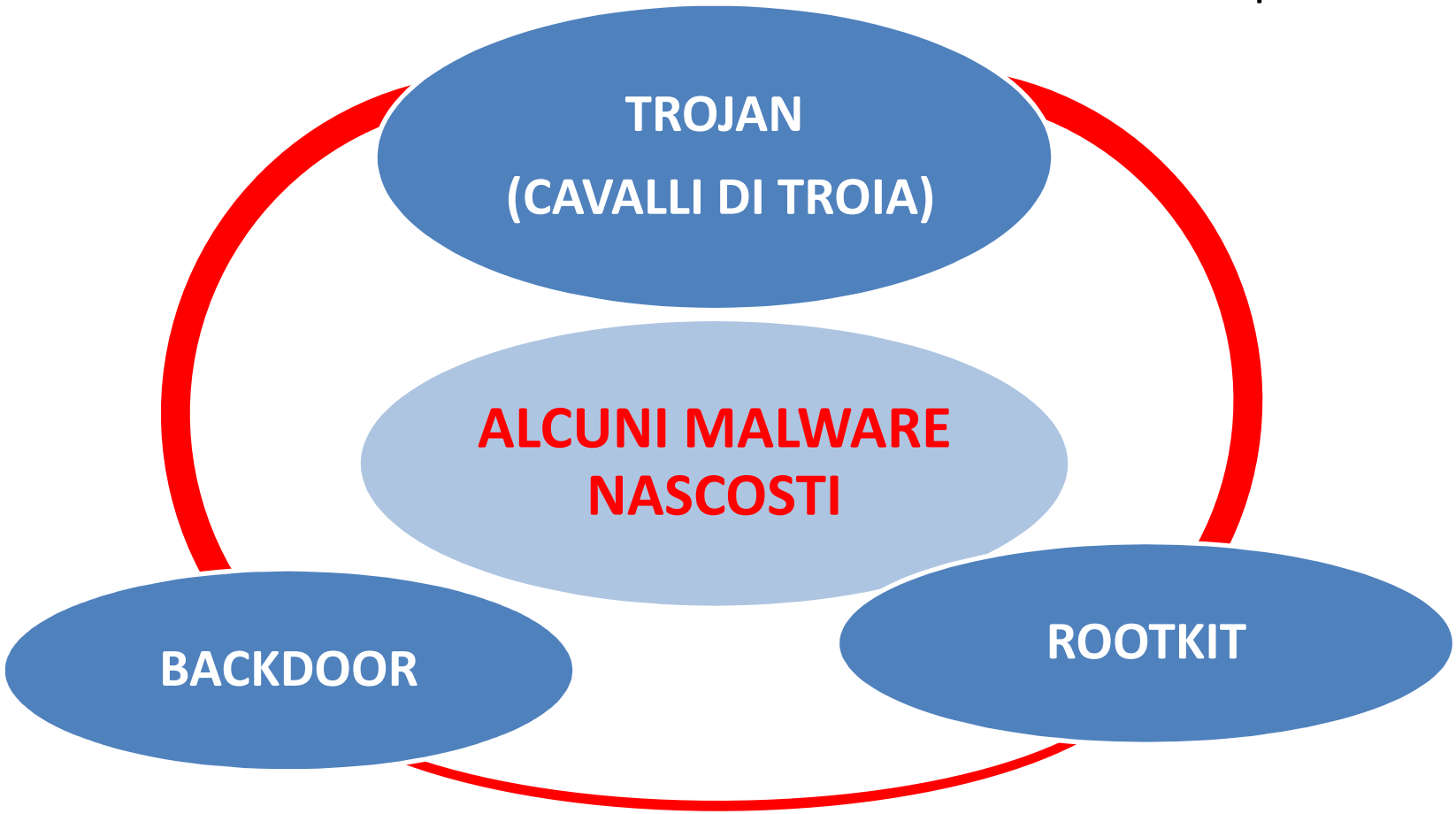
TEMA 2.1 TIPI E METODI

Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer

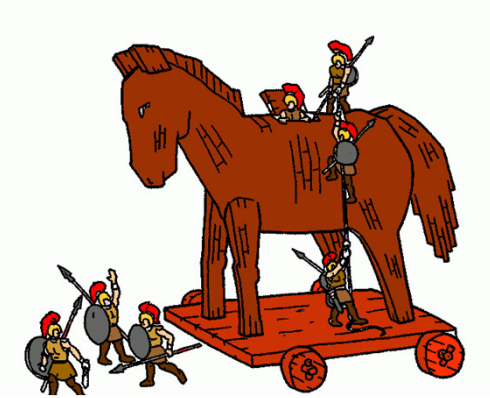


SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer

TROJAN



File nascosti in programmi apparentemente innocui scaricati dall’utente (es. giochi gratuiti,…). Utilizzati da cracker per diffondere virus o per ottenere il controllo dei computer remoti

SEZIONE 2 – MALWARE

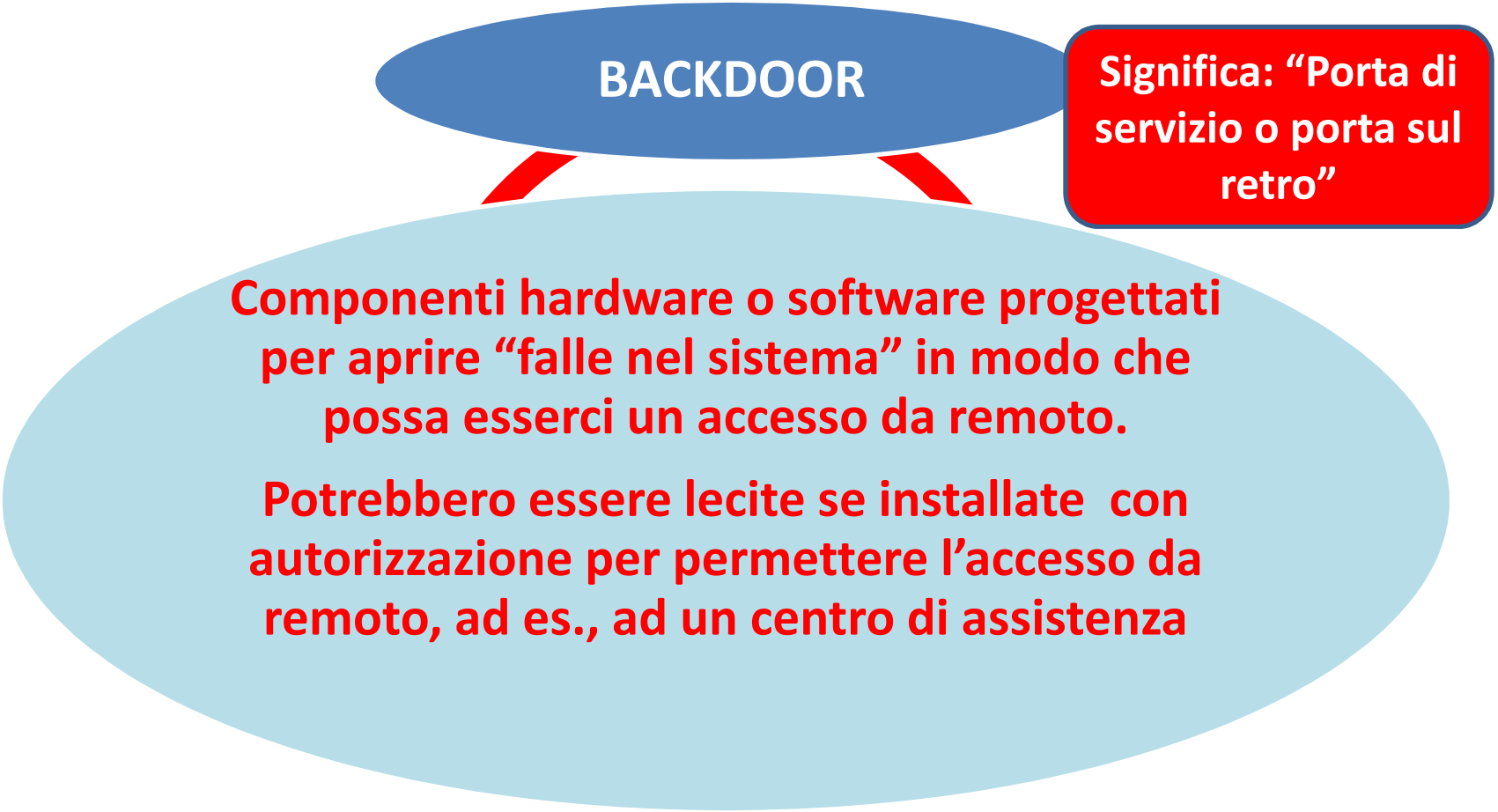
TEMA 2.1 TIPI E METODI

Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

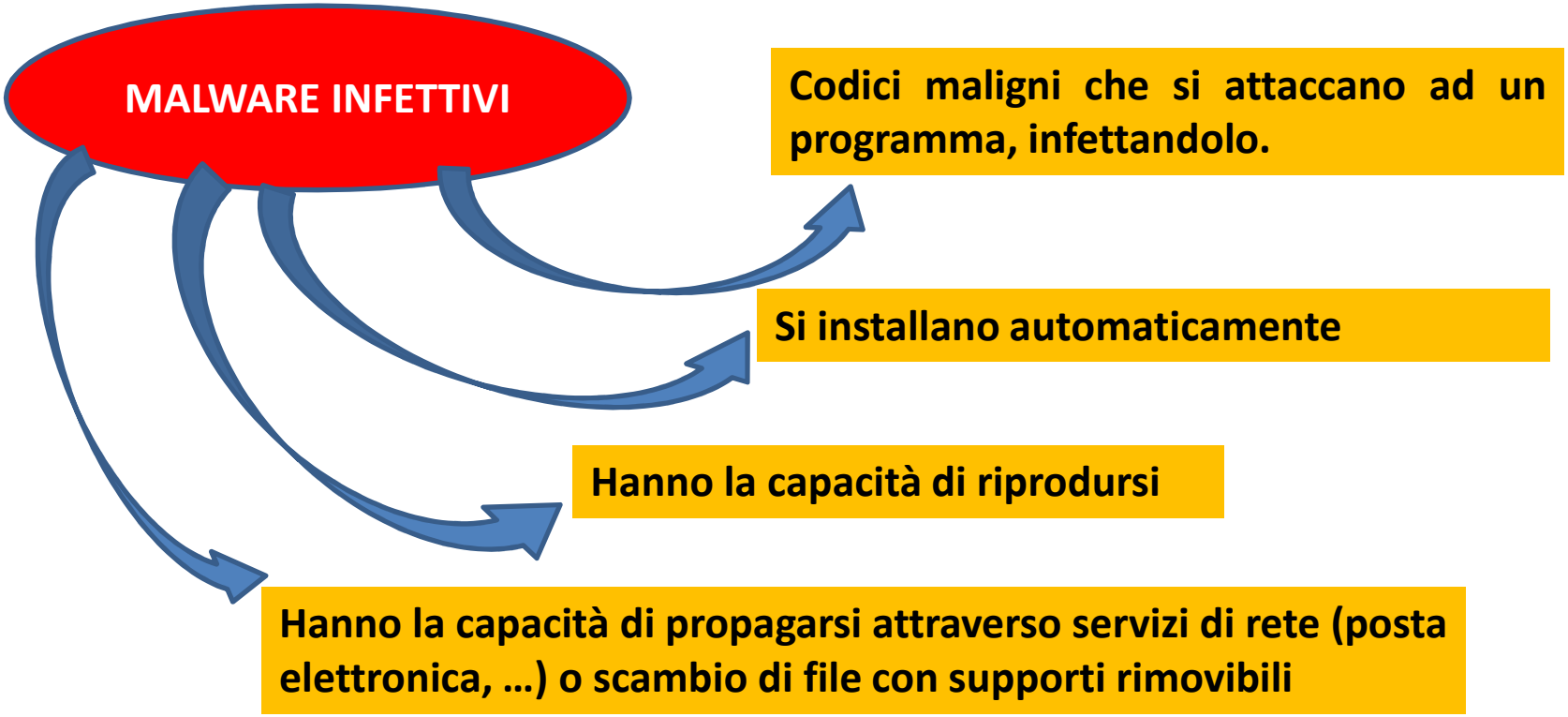
Argomento 2.1.1 Comprendere il termine “malware”. Riconoscere come il malware si nasconde nei computer



SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

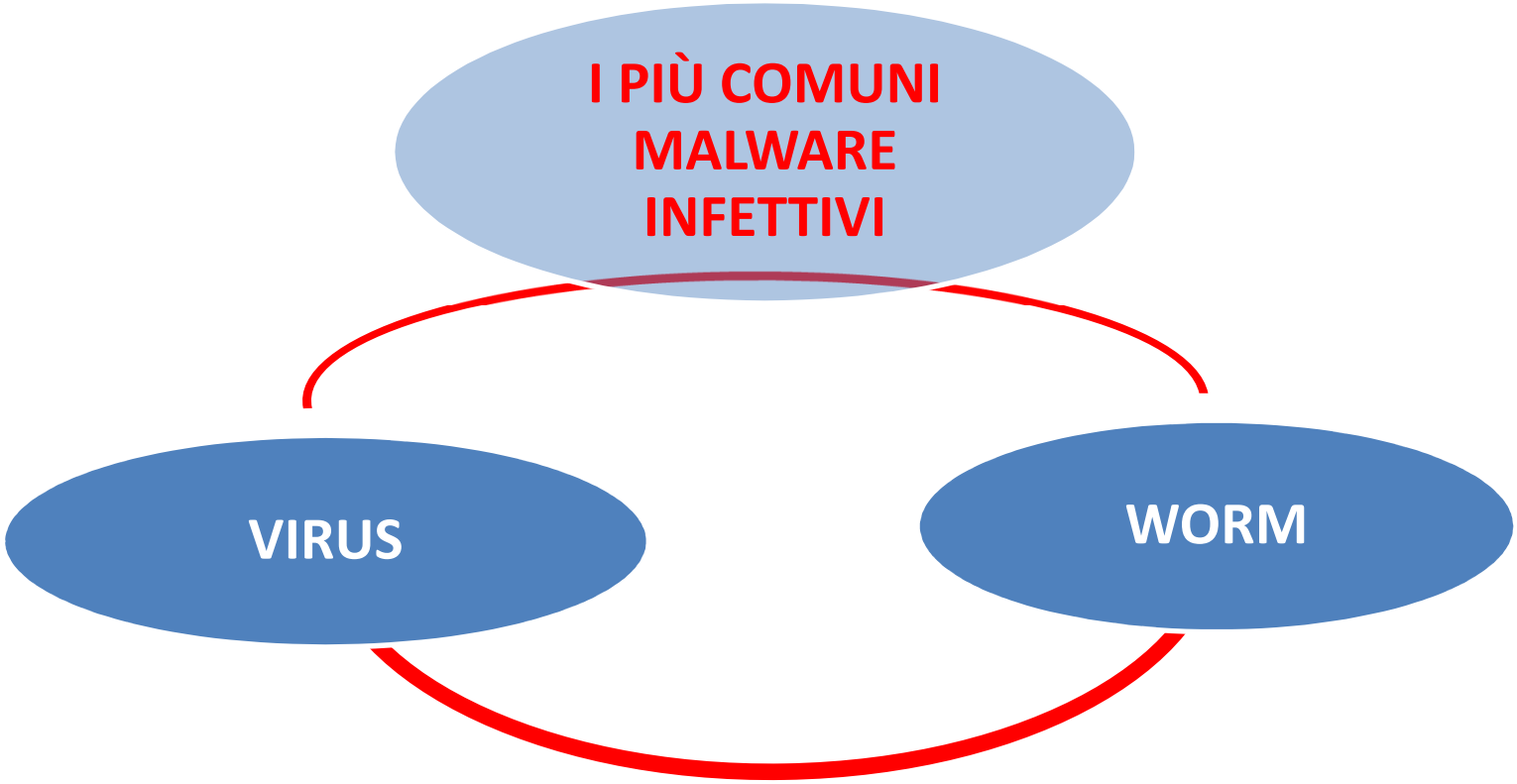
Argomento 2.1.2 Riconoscere i tipi di malware infettivo e capire come funzionano



SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.2 Riconoscere i tipi di malware infettivo e capire come funzionano



SEZIONE 2 – MALWARE

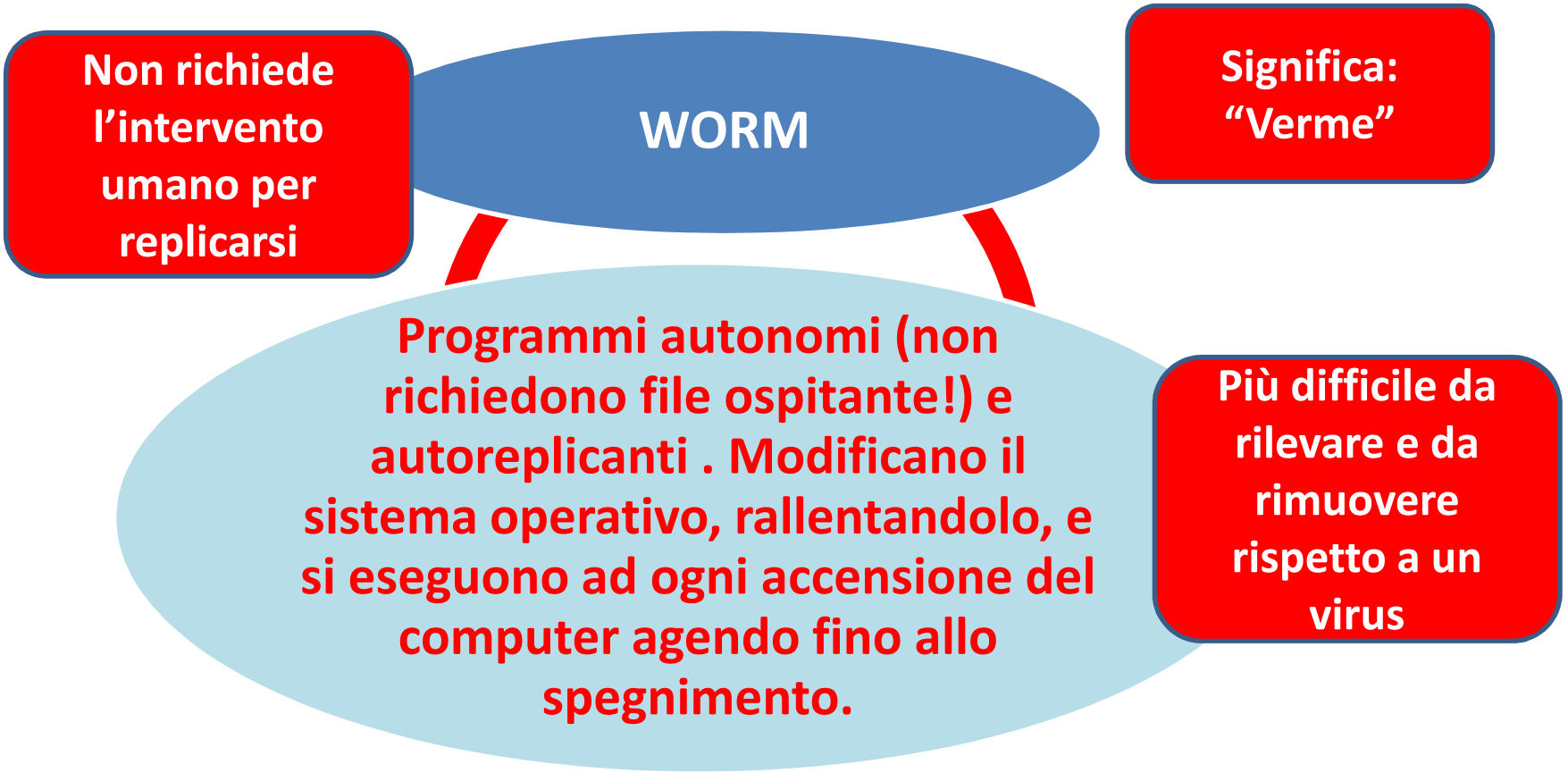
TEMA 2.1 TIPI E METODI

Argomento 2.1.2 Riconoscere i tipi di malware infettivo e capire come funzionano

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.2 Riconoscere i tipi di malware infettivo e capire come funzionano



SEZIONE 2 – MALWARE

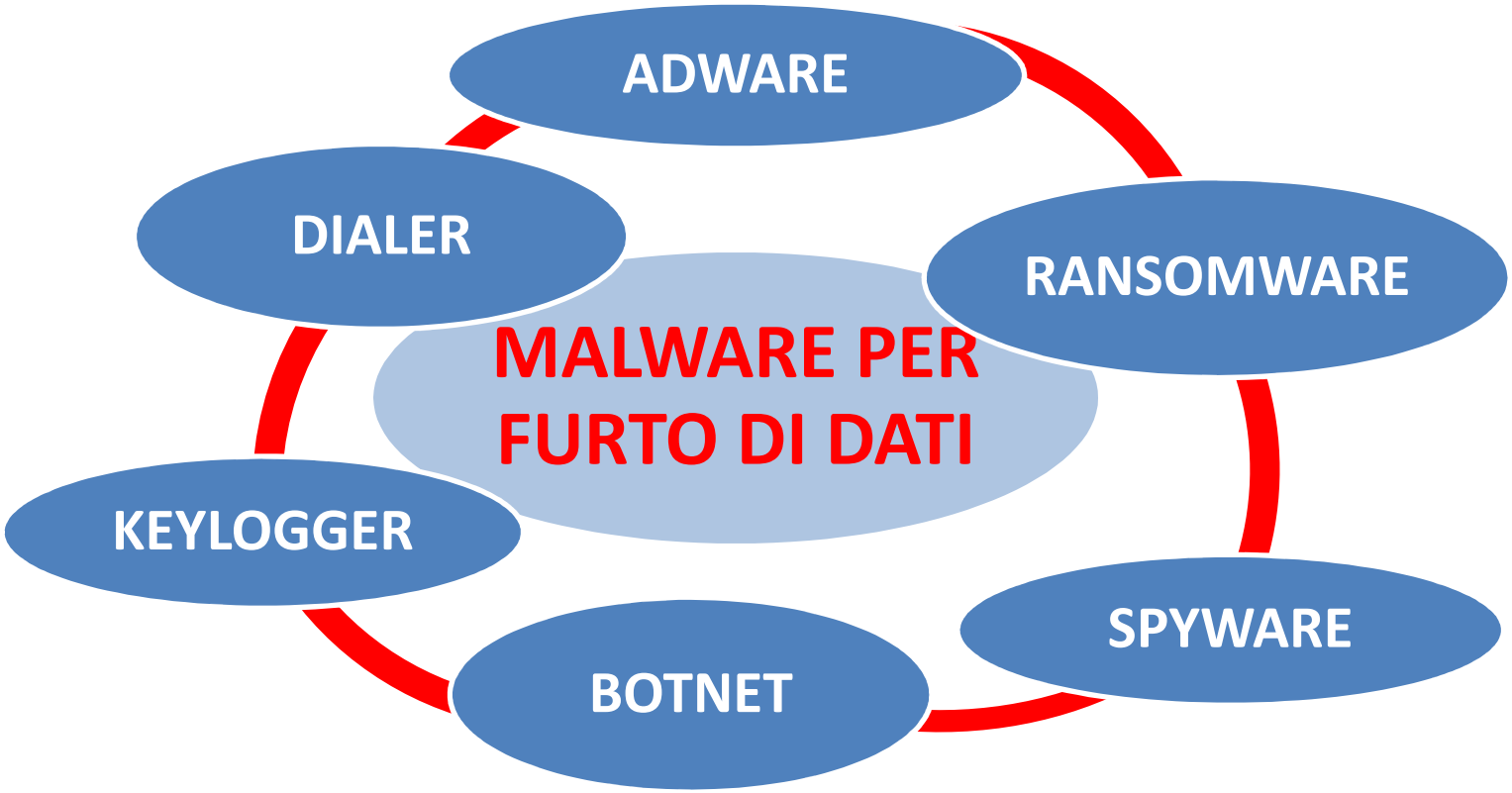
TEMA 2.1 TIPI E METODI

Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

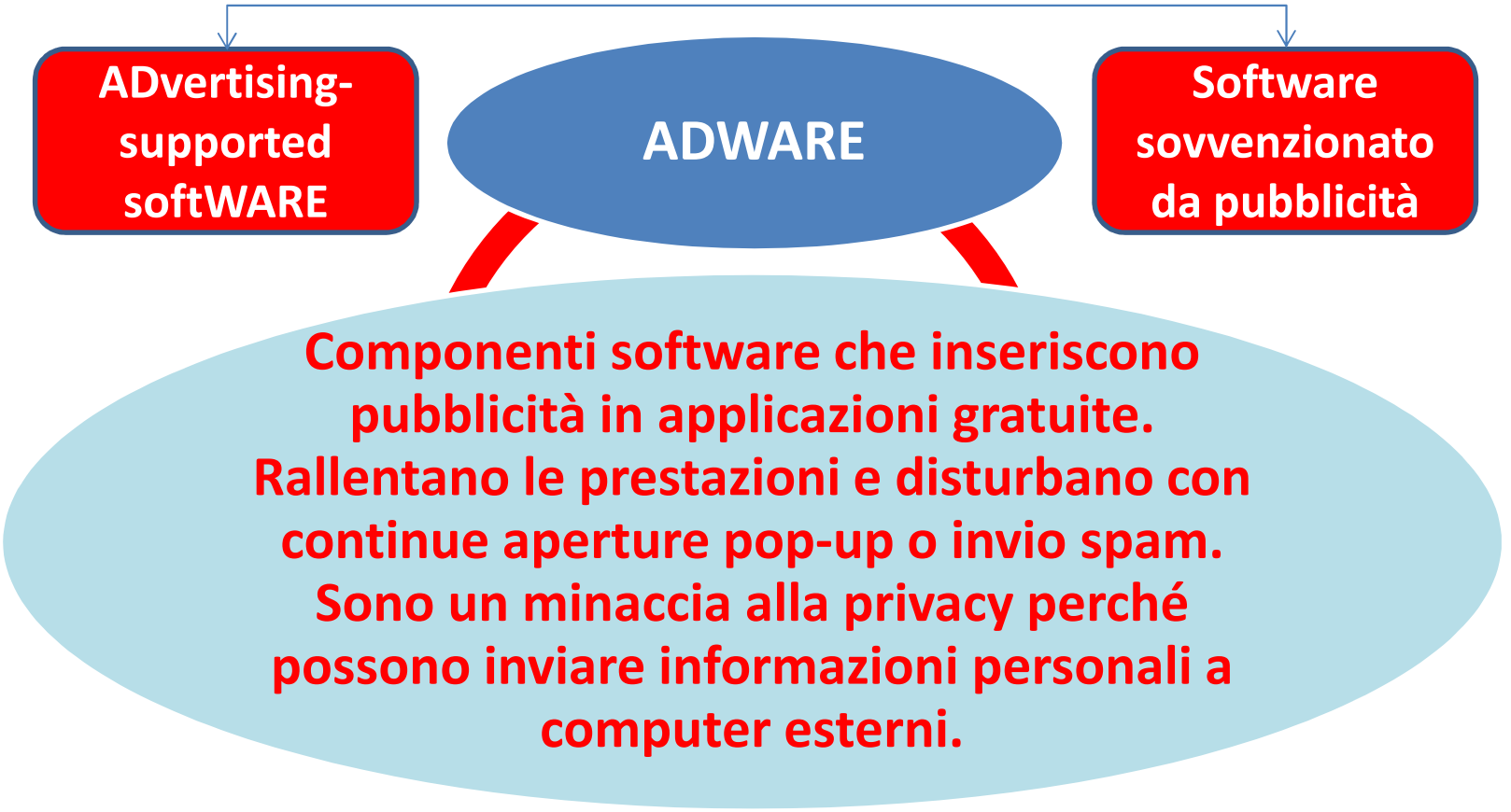
Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano



SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

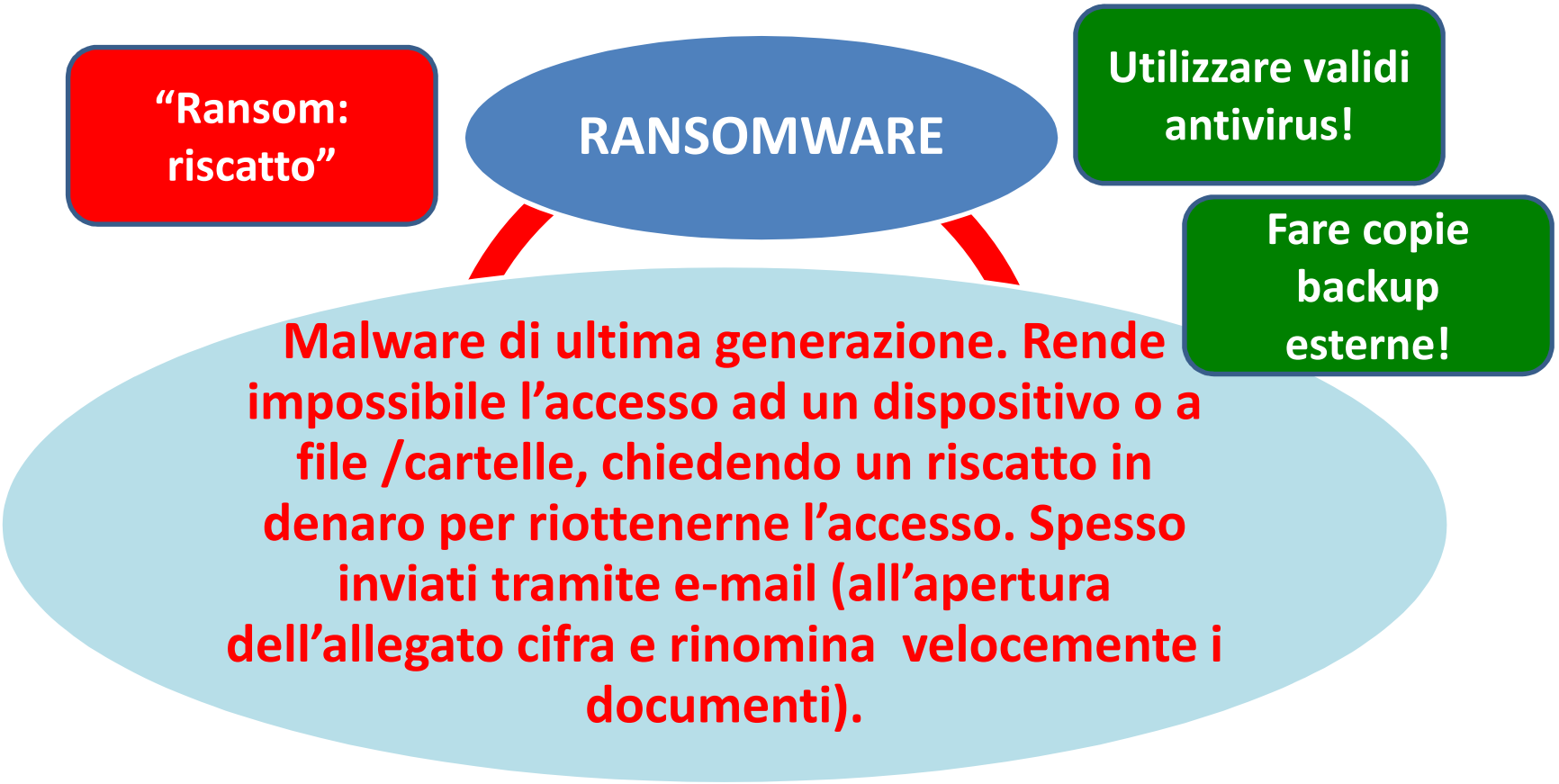
Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano



SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano



SEZIONE 2 – MALWARE

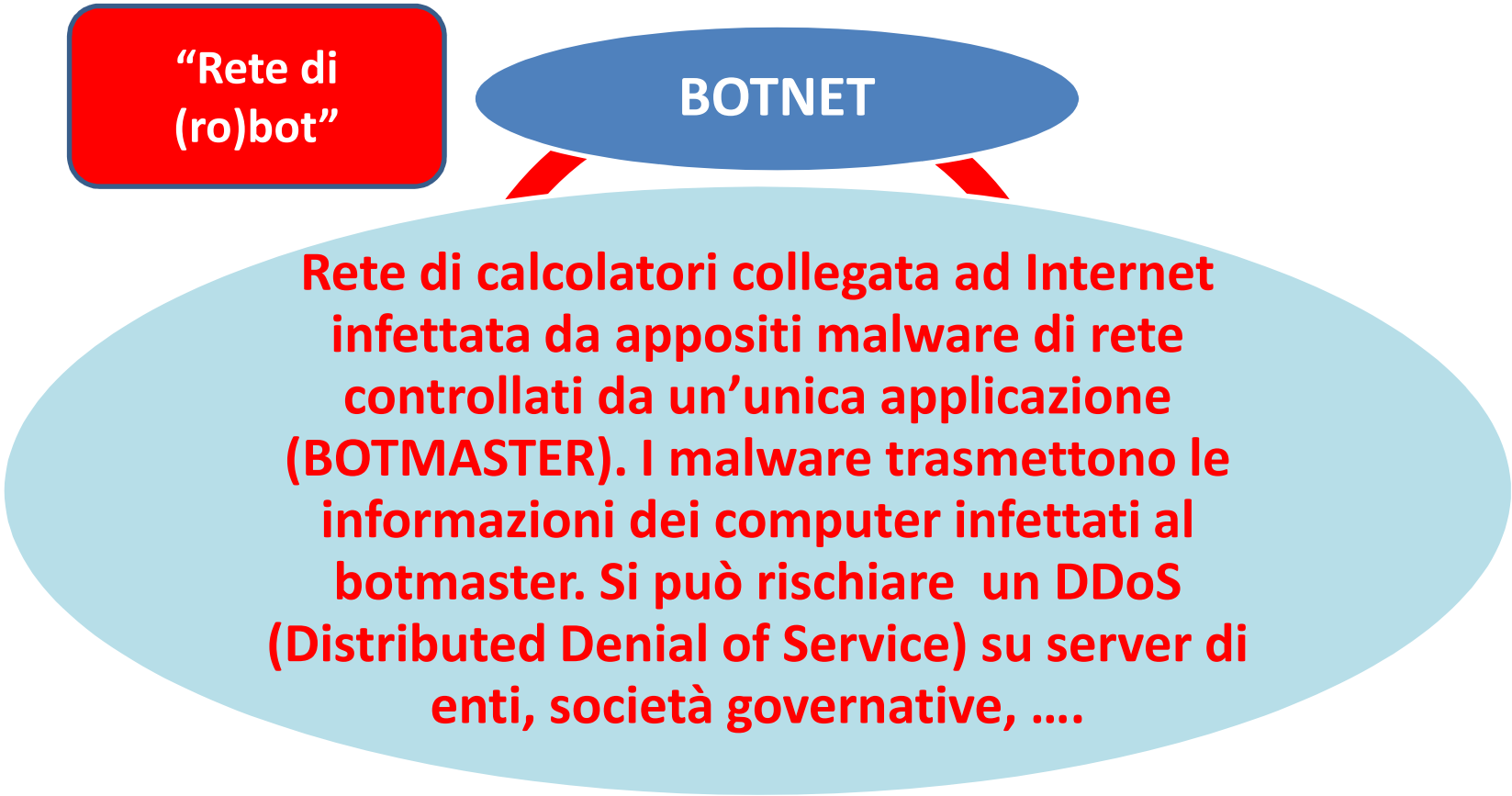
TEMA 2.1 TIPI E METODI

Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano



SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano

"KEYstroke LOGGER: registratore della battitura"

KEYLOGGER

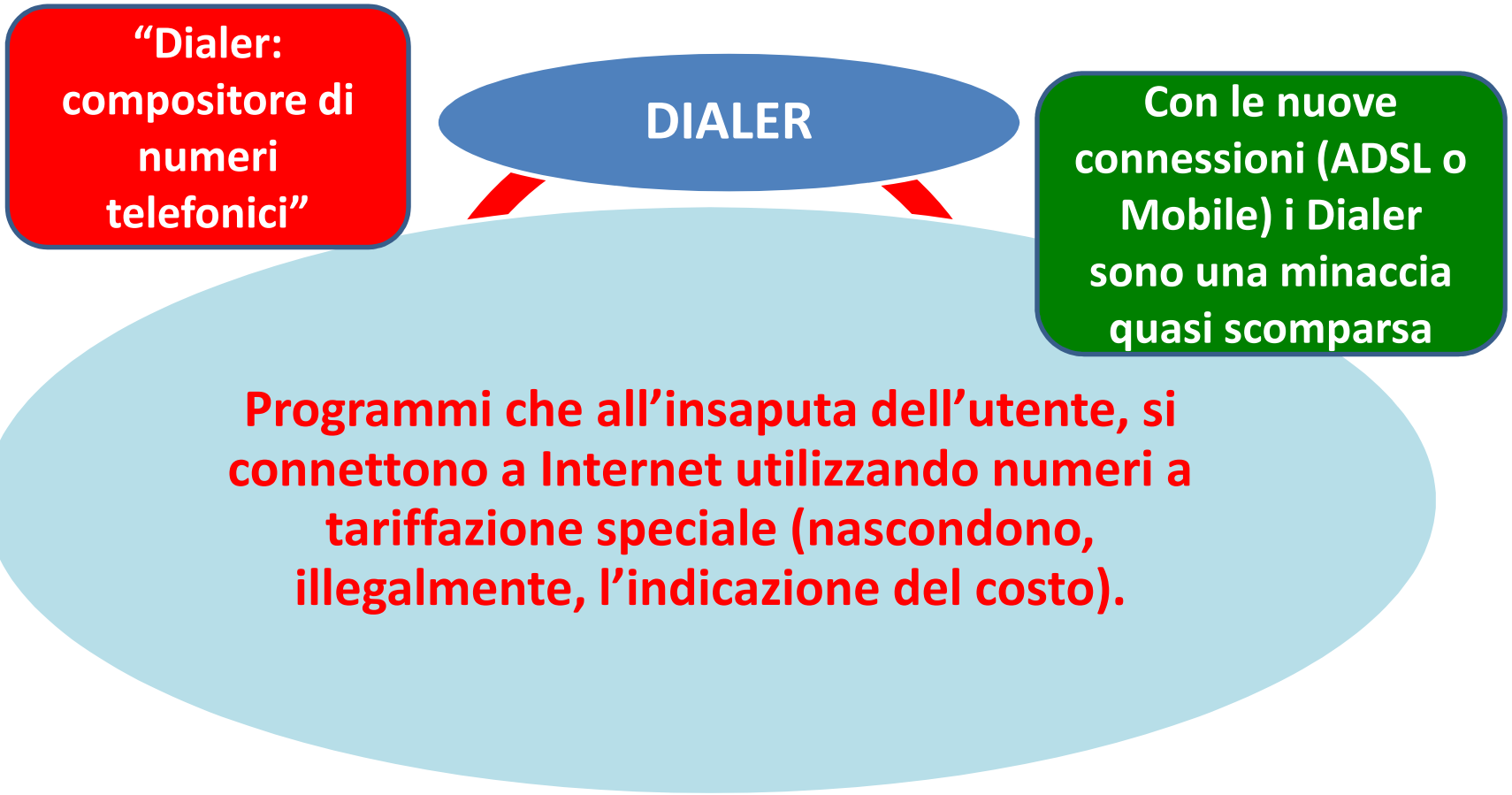
Software (applicazioni o driver di periferica) o hardware in grado di registrare ogni tasto che viene digitato, per carpire informazioni quali password, numeri di carte di credito, PIN dei bancomat,…

Si installano attraverso virus, worm e malware nascosti.

SEZIONE 2 – MALWARE

TEMA 2.1 TIPI E METODI

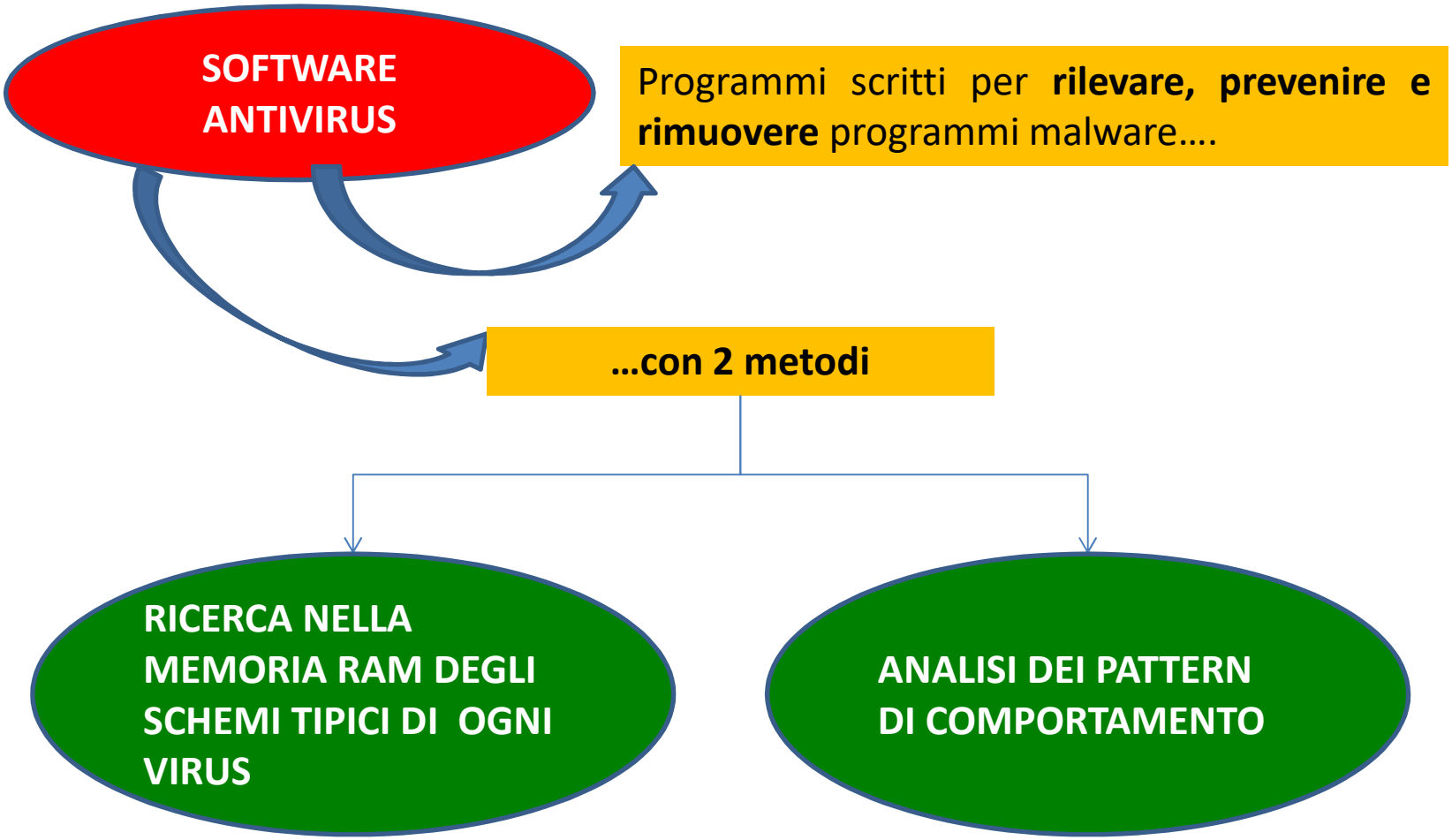
Argomento 2.1.3 Riconoscere i tipi di malware per furto di dati, profitto/estorsione e capire come operano



SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta



SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta

RICERCA NELLA MEMORIA RAM DEGLI SCHEMI TIPICI DI OGNI VIRUS

Ogni malware è caratterizzato dal suo schema, ovvero da una sua precisa serie di istruzioni

Gli schemi dei malware conosciuti sono memorizzari in un archivio del software antivirus (archivio delle “firme”).

All’avvio del sistema il software antivirus esegue la scansione della memoria RAM e, in caso di problemi, li notifica, altrimenti rimane in esecuzione controllando le attività del sistema (protezione “real time”)

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta

RAM

◀ Fisicamente la RAM è costituita da chip (circuiti integrati) inseriti su schedine rettangolari (schede SIMM), a loro volta inserite in appositi supporti (slot) sulla scheda madre. ▶

L'acronimo RAM deriva da *Random Access Memory* (memoria ad accesso casuale). Si tratta di una memoria di lettura/scrittura in cui transitano i dati in ingresso e in uscita dalla CPU.

Definita con la sigla CPU (*Central Processing Unit*), l'unità centrale di elaborazione è il cervello della macchina: un circuito integrato (microprocessore) in cui avvengono i processi di elaborazione.

La RAM fa parte della memoria centrale del computer

I programmi installati sono memorizzati nell'hard disk e, a ogni loro utilizzo, vengono caricati nella RAM affinché la CPU possa reperire velocemente le istruzioni necessarie per eseguire le elaborazioni richieste. Se la RAM non ha una capacità sufficiente a contenere i dati in fase di elaborazione e le istruzioni dei programmi, queste ultime devono essere lette ogni volta nell'hard disk e il tempo di accesso aumenta, rallentando così le prestazioni del computer.

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta

ANALISI DEI PATTERN DI COMPORTAMENTO

Il software antivirus analizza il comportamento dei programmi in esecuzione per cercare comportamenti sospetti, tipici dei malware (RICERCA EURISTICA).

“Pattern: schema, modello”

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta

Un antivirus non può essere efficace al 100%!

LIMITI DEI SOFTWARE ANTIVIRUS

Riconoscono soltanto i pattern, le firme e le definizioni presenti nel loro archivio.

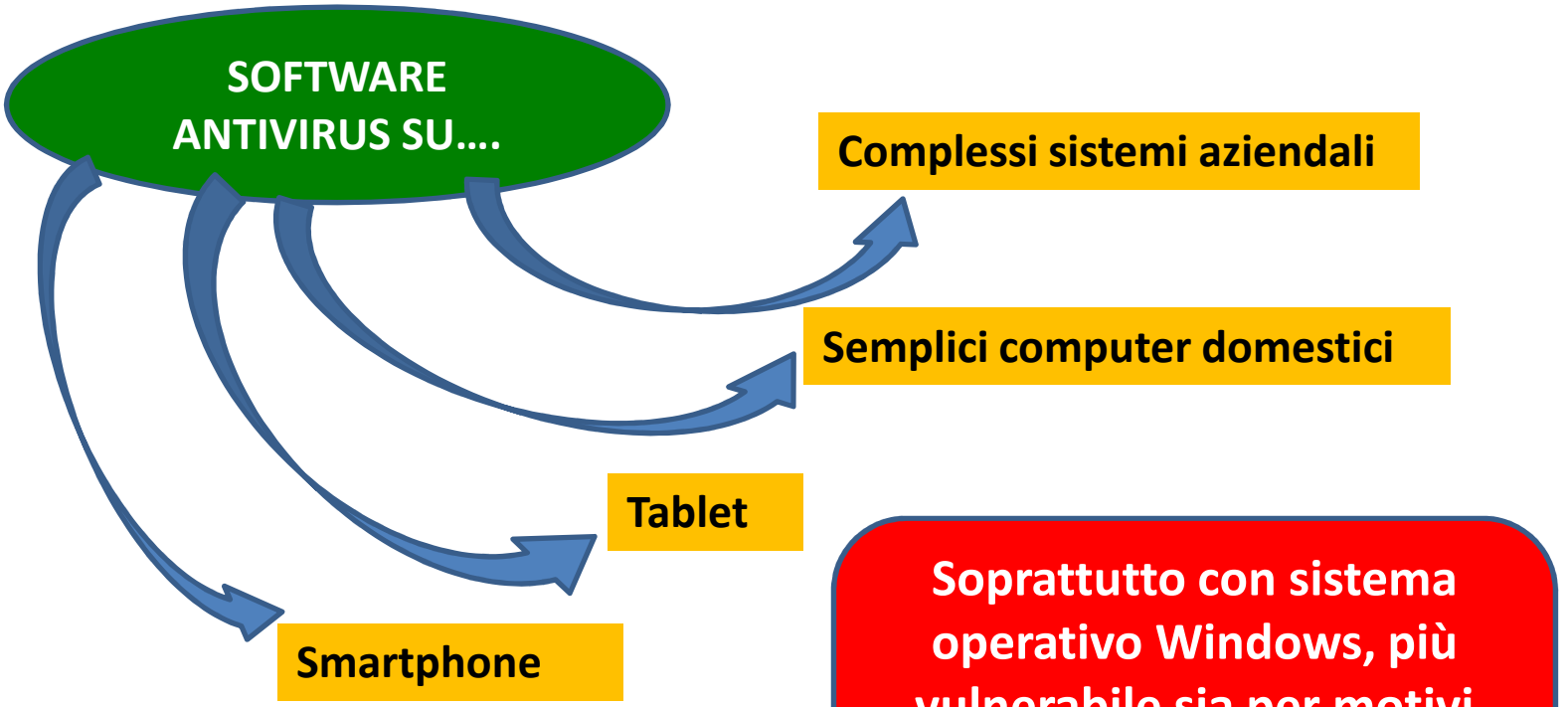
Riconoscono i malware dopo che hanno già infettato un file .

Possono presentarsi i “FALSI POSITIVI” ovvero l’antivirus riconosce come malware un file che in realtà non lo è (ad es. una macro innocua, che presenta alcune istruzioni presenti anche in un malware)

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

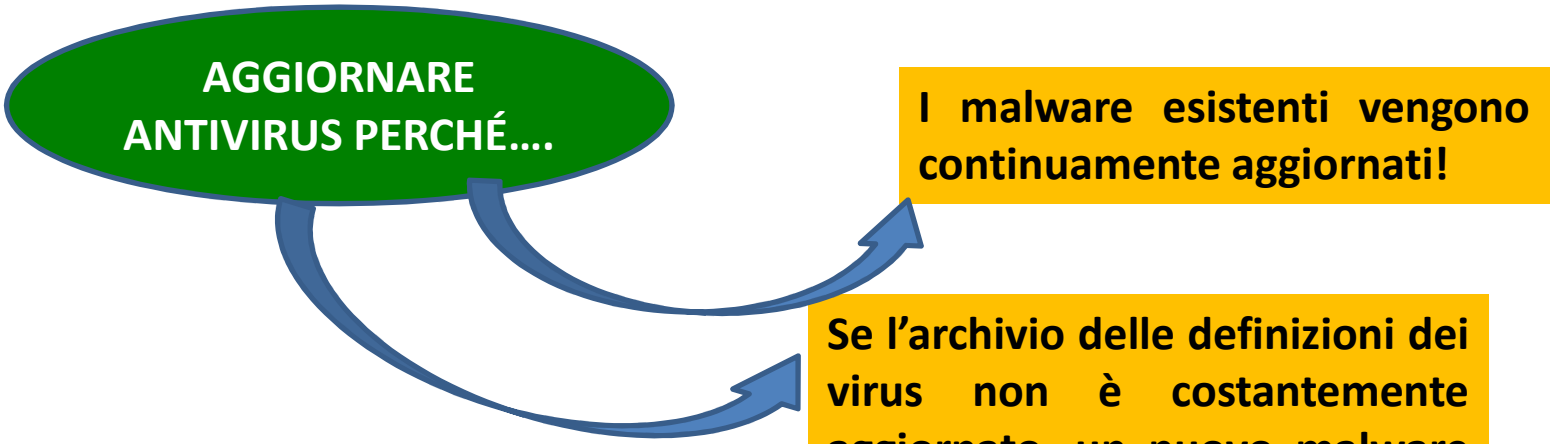
Argomento 2.2.2 Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici



SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.3 Comprendere l'importanza di aggiornare regolarmente i software



Gli antivirus effettuano spesso e automaticamente gli aggiornamenti delle definizioni.

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.3 e 2.2.5 Comprendere l'importanza di aggiornare regolarmente i software per evitare i rischi associati

SEZIONE 2 – MALWARE

TEMA 2.2 PROTEZIONE

Argomento 2.2.4 Eseguire e pianificare scansioni di specifiche unità con software antivirus

Gli antivirus effettuano automaticamente le operazioni di scansione della memoria e dei file.

È sempre bene però ….

Scansionare manualmente file e cartelle sospetti (file scaricati da rete, allegati di e-mail,…)

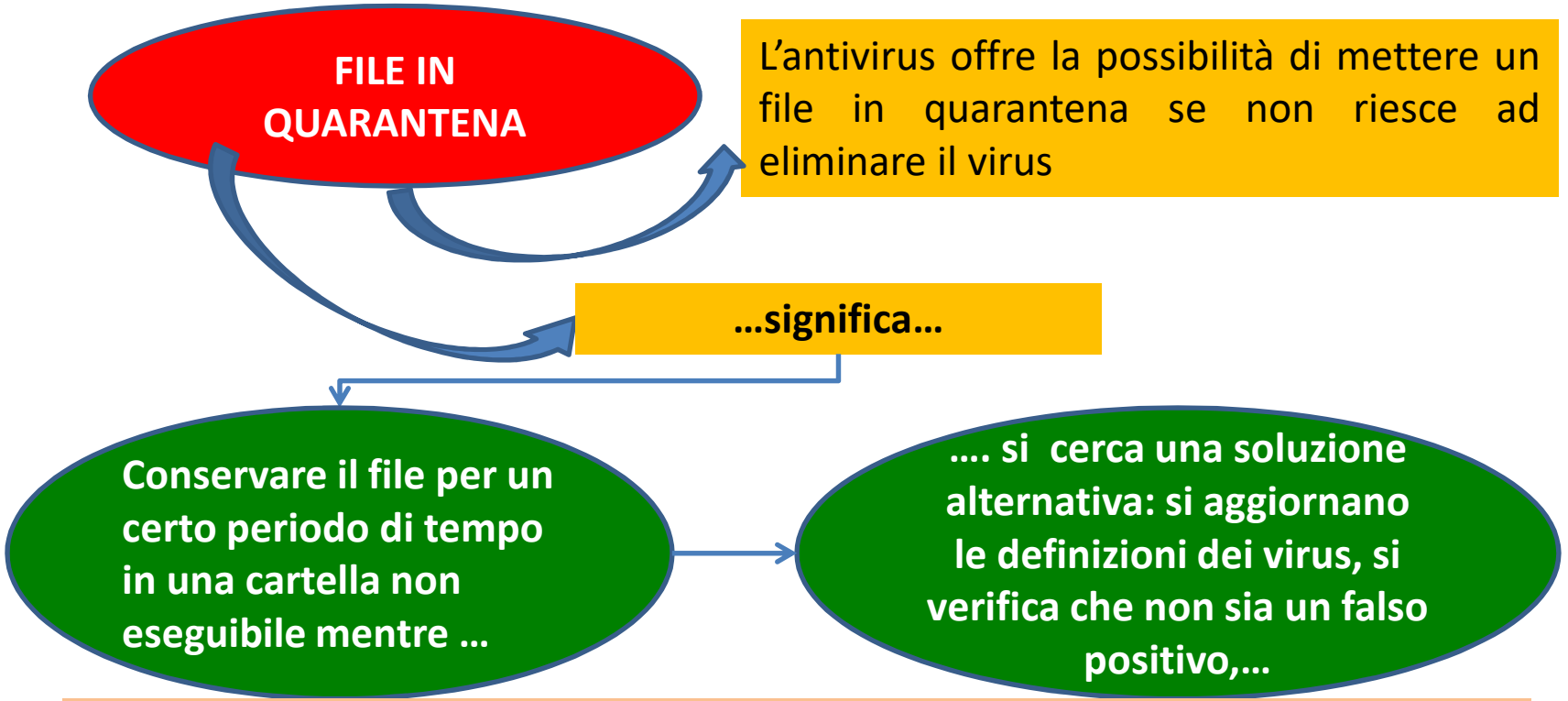
Programmare scansioni periodiche di file e cartelle, o di interi dischi, nei momenti di inutilizzo del computer

A seconda del software antivirus utilizzato possono esserci piccole differenze, ma, in genere, basta cliccare con il tasto destro sulla specifica unità e scegliere la voce di "Avvio scansione"

SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.1 e 2.3.2 Comprendere il termine “quarantena” ed il suo effetto. Eliminare file infetti/sospetti

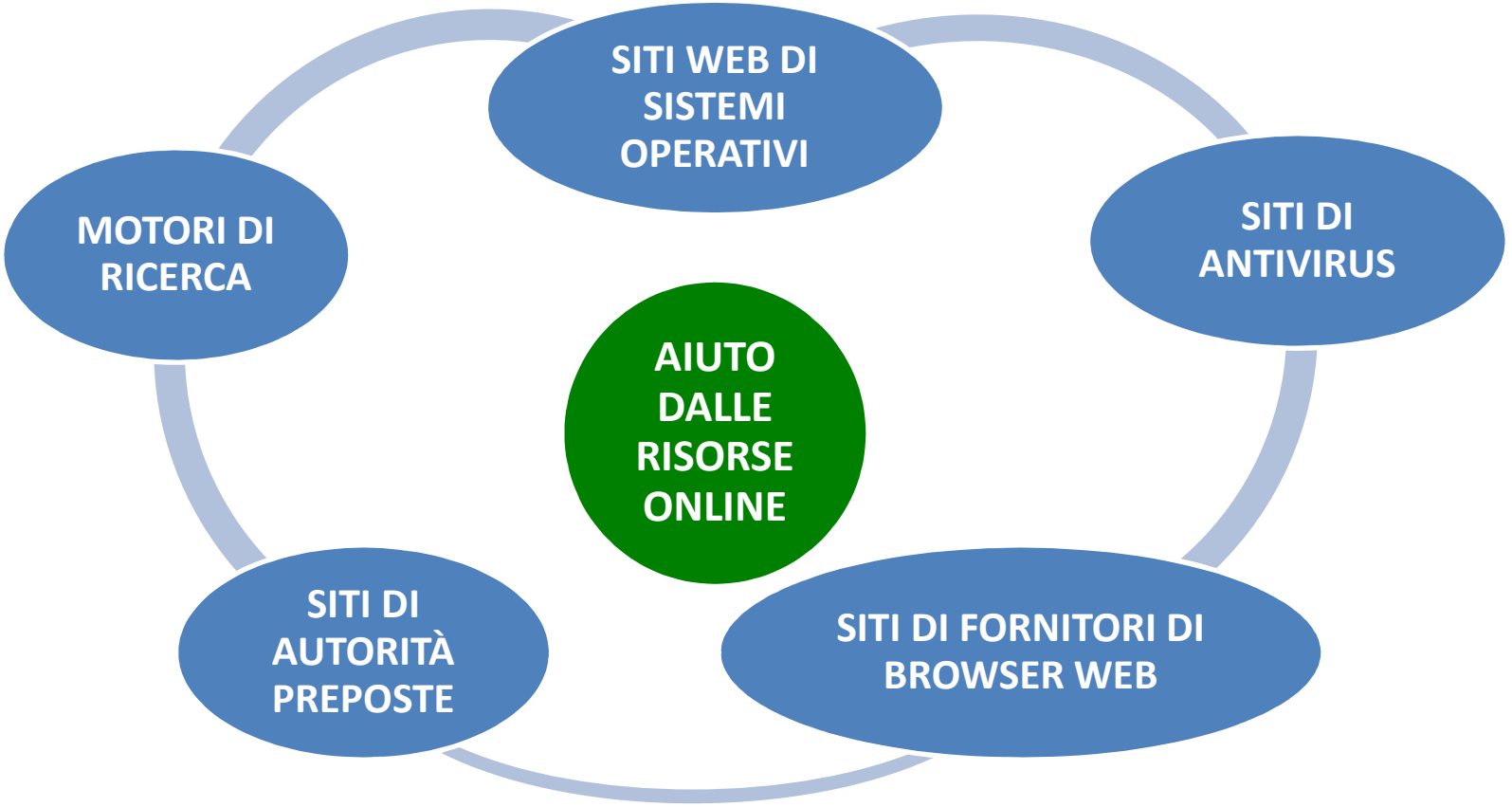


In genere, tramite una finestra di dialogo, l’utente può decidere se eliminare definitivamente il file posto in quarantena o, dopo le opportune verifiche, ripristinarlo.

SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online



SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online

SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online

SEZIONE 2 – MALWARE

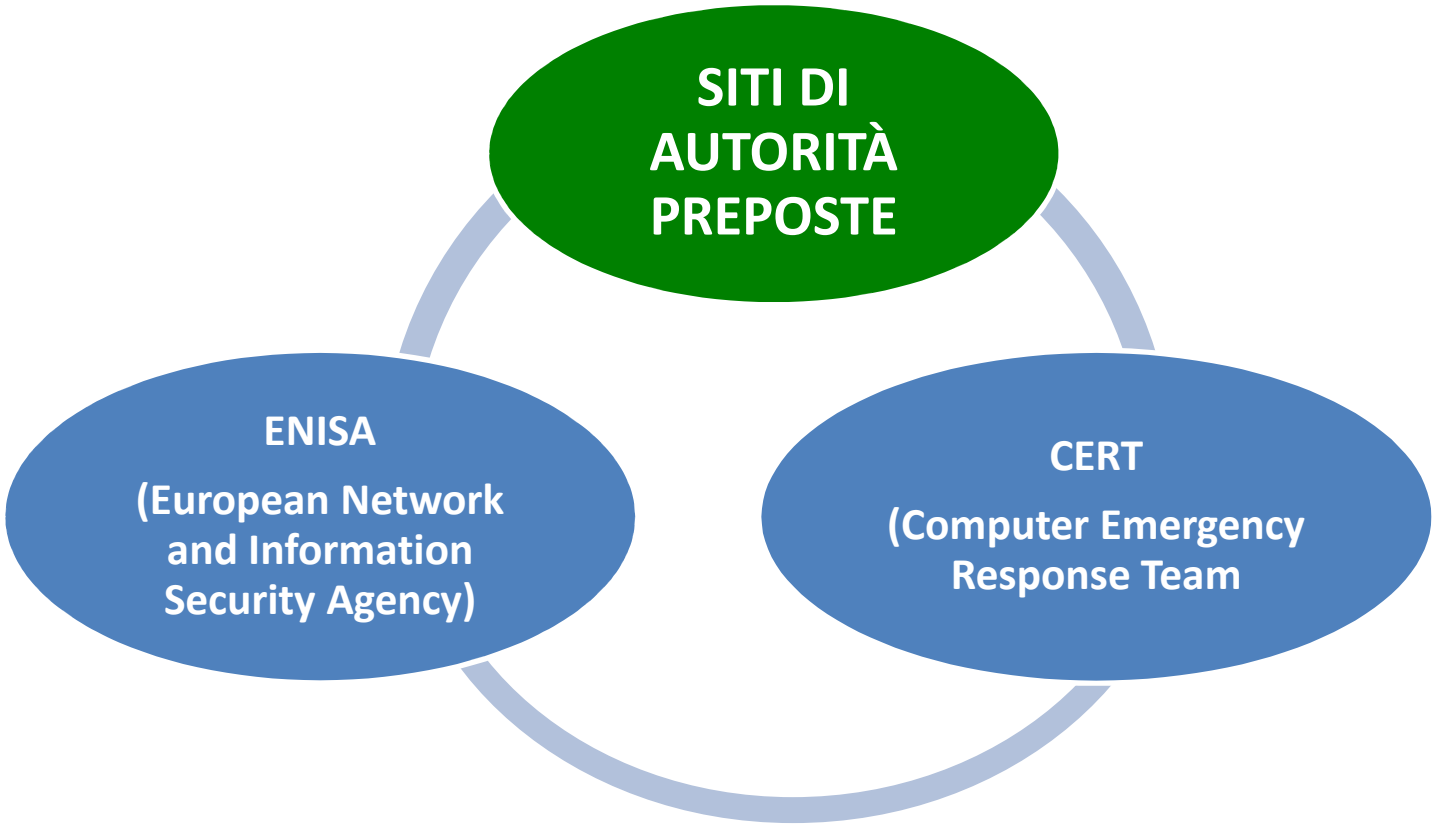
TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online

SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online



SEZIONE 2 – MALWARE

TEMA 2.3 RISOLUZIONE E RIMOZIONE

Argomento 2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online