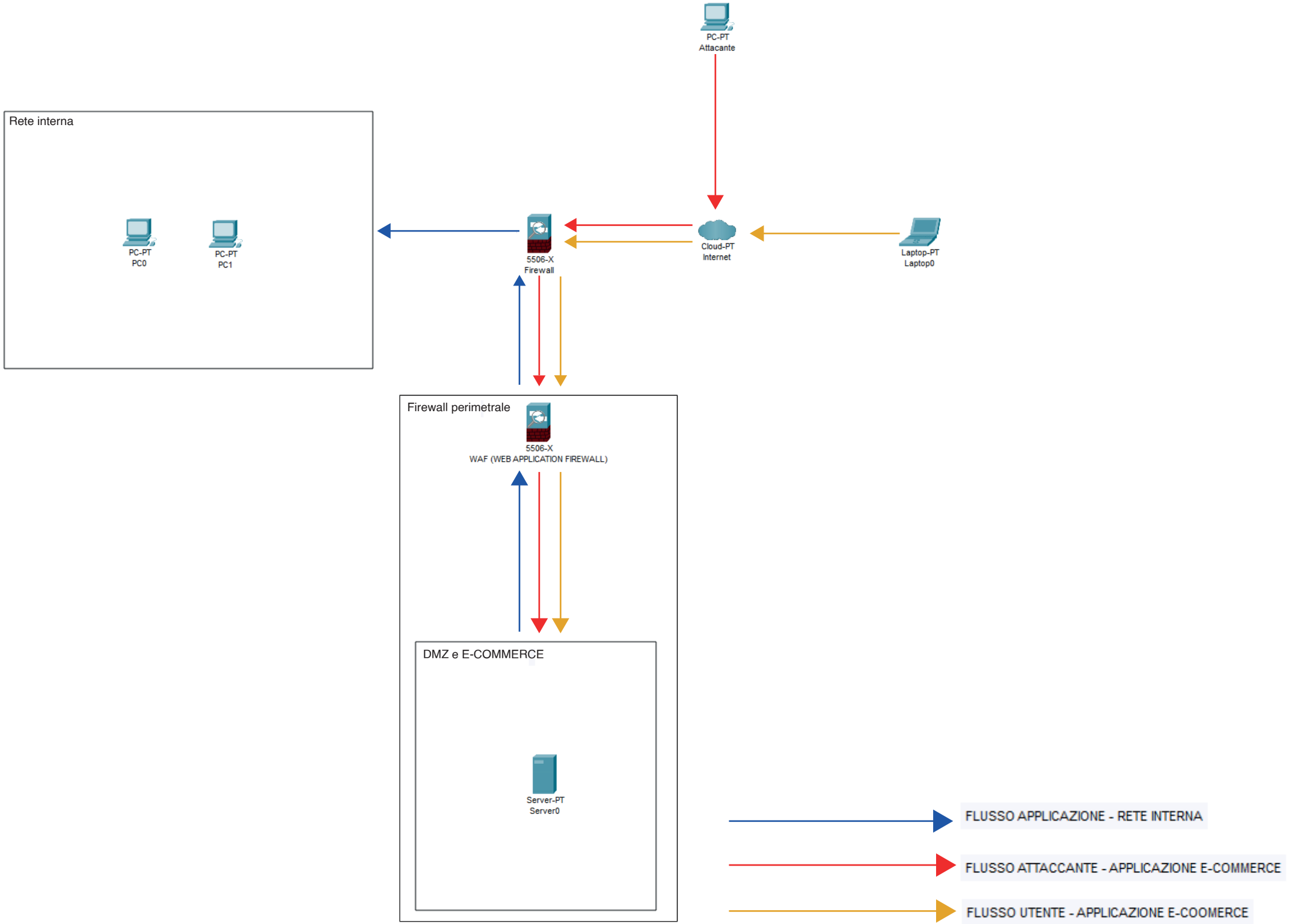

PC-PT
Attacante
Rete interna
PC-PT
PC0
PC-PT
PC1
5506-X
Firewall
Cloud-PT
Internet
Laptop-PT
Laptop0
Firewall perimetrale
5506-X
WAF (WEB APPLICATION FIREWALL)
DMZ e E-COMMERCE
Server-PT
Server0
FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COOMERCE

Per calcolare l'impatto finanziario dell'attacco DDoS sulla piattaforma di e-commerce, possiamo utilizzare la seguente formula:

Impatto Finanziario = (Perdita di guadagno al minuto)
x
(Durata dell'indisponibilità in minuti)

Dato che ogni minuto gli utenti spendono in media 1.500 € sulla piattaforma di e-commerce, la perdita di guadagno al minuto è di 1.500 €.

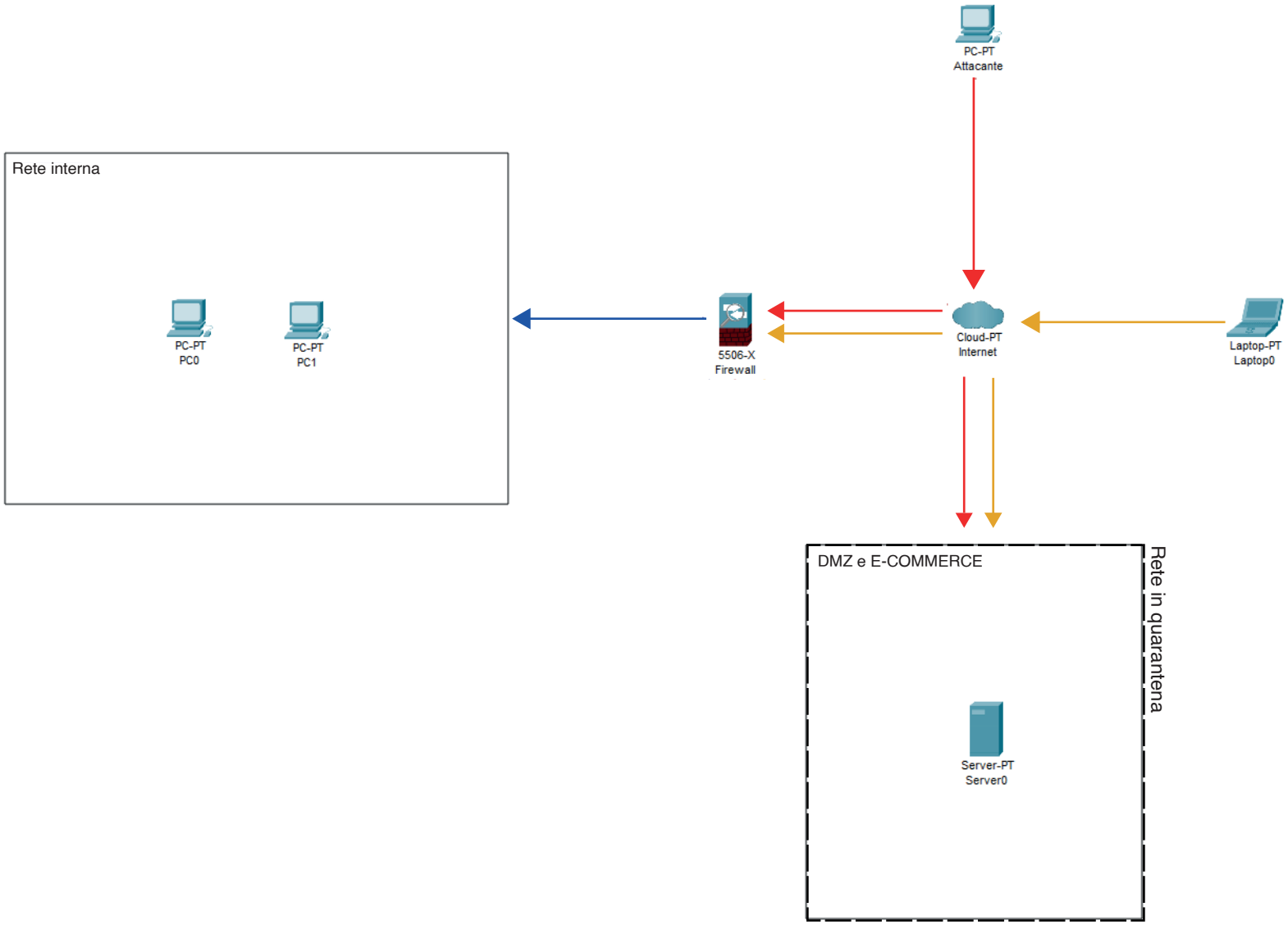
Se l'applicazione è stata resa indisponibile per 10 minuti a causa dell'attacco DDoS, l'impatto finanziario può essere calcolato come:

Impatto Finanziario = 1.500 €/minuto
x
10 minuti
=
15.000 €

Quindi, l'attacco DDoS ha causato un'impatto finanziario di 15.000 € sulla piattaforma di e-commerce.

Per prevenire o mitigare gli attacchi DDoS e ridurre l'impatto finanziario causato dalla non raggiungibilità del servizio, si possono considerare le seguenti azioni preventive:

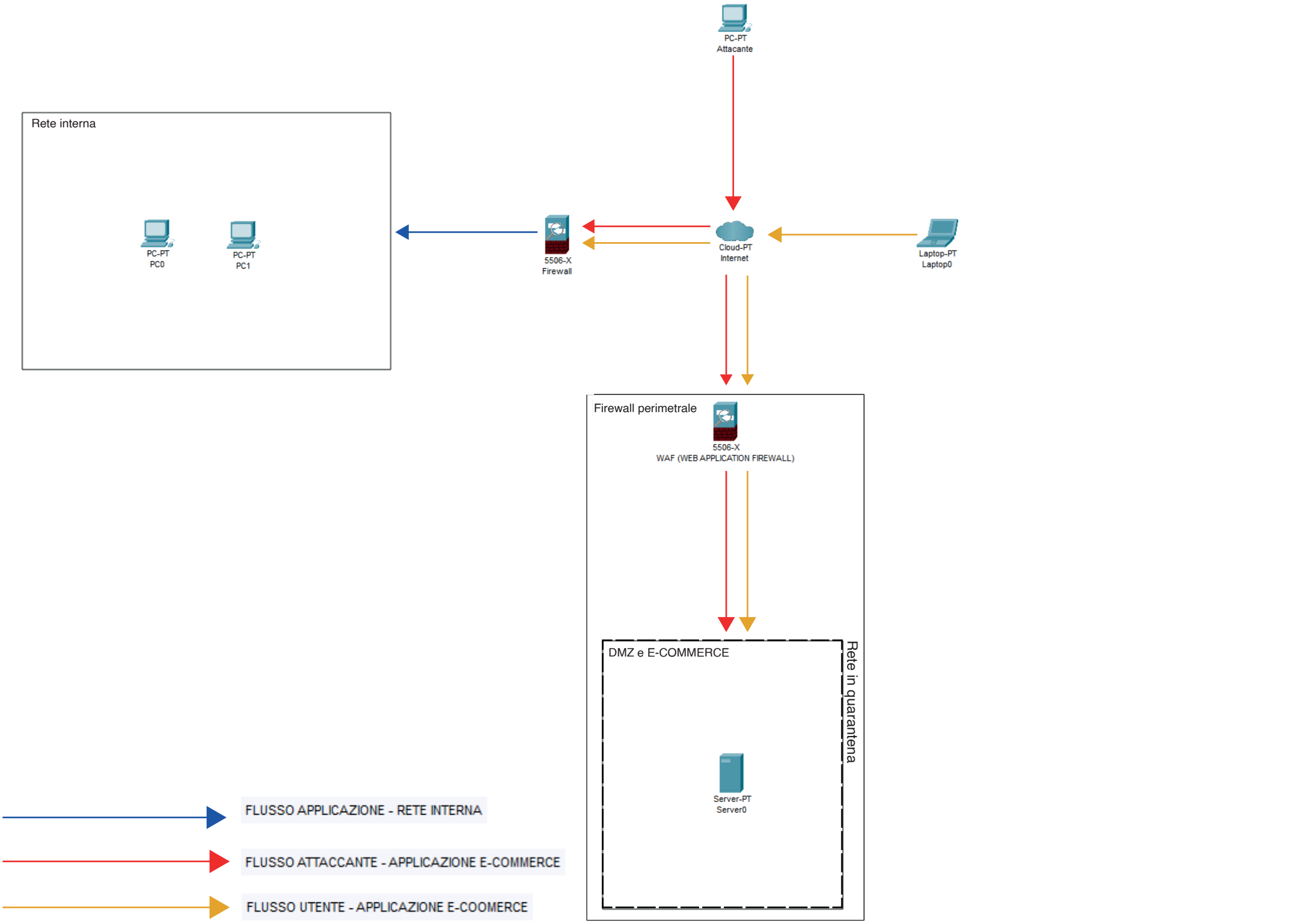
1) Implementazione di un servizio anti-DDoS:
Utilizzare un servizio di mitigazione DDoS fornito da provider di sicurezza specializzati.
Questi servizi possono identificare e filtrare il traffico malevolo prima che raggiunga l'infrastruttura dell'applicazione.
2) Configurazione di limiti di richieste:
Impostare limiti sul numero di richieste che un singolo indirizzo IP può inviare nell'unità di tempo.
Questo può aiutare a mitigare gli attacchi DDoS distribuiti che coinvolgono un gran numero di indirizzi IP.
3) Utilizzo di un CDN:
Utilizzare un Content Delivery Network (CDN) per distribuire il carico di traffico su più server geograficamente distribuiti.
Questo può aiutare a distribuire il traffico DDoS in modo più efficiente e a mitigarne gli effetti.
4) Monitoraggio del traffico e del comportamento degli utenti:
Implementare sistemi di monitoraggio del traffico e del comportamento degli utenti per rilevare pattern anomali che potrebbero indicare un attacco DDoS in corso. In base a questi pattern, possono essere attivati automaticamente meccanismi di mitigazione.
5) Pianificazione di risposta agli incidenti:
Avere un piano di risposta agli incidenti ben definito per gestire rapidamente gli attacchi DDoS quando si verificano.
Questo può includere procedure per scalare risorse aggiuntive, contattare il provider di servizi anti-DDoS e informare gli utenti dell'indisponibilità temporanea del servizio. (WAF)
6) Aggiornamenti di sicurezza regolari:
Mantenere aggiornato il software dell'applicazione e l'infrastruttura di rete per correggere eventuali vulnerabilità che potrebbero essere sfruttate per lanciare attacchi DDoS.

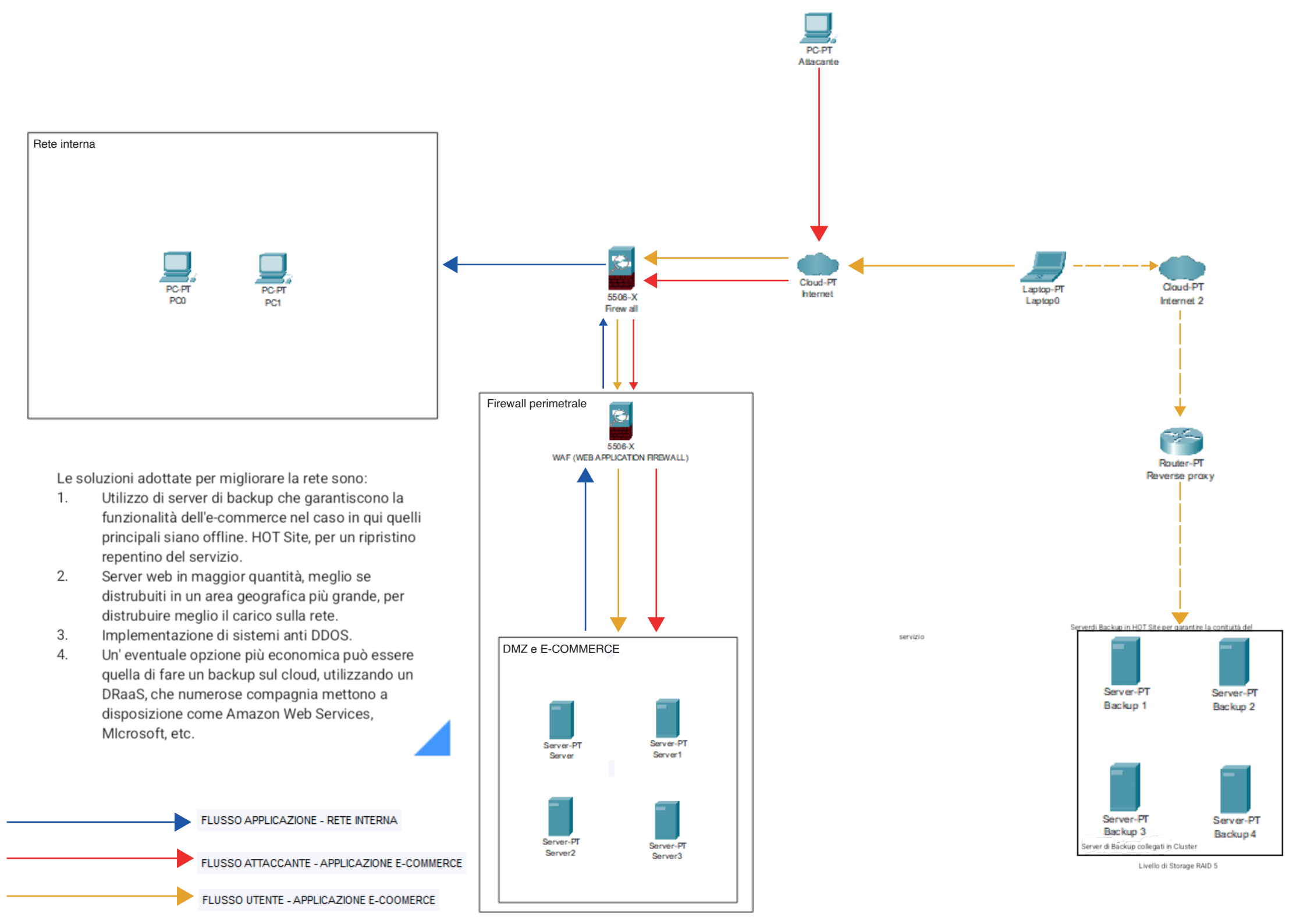


FLUSSO APPLICAZIONE - RETE INTERNA

FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE

FLUSSO UTENTE - APPLICAZIONE E-COOMERCE


PC-PT
Attacante
Rete interna
PC-PT
PC0
PC-PT
PC1
5506-X
Firewall
Cloud-PT
Internet
Laptop-PT
Laptop0
Firewall perimetrale
5506-X
WAF (WEB APPLICATION FIREWALL)
DMZ e E-COMMERCE
Rete in quarantena
Server-PT
Server0
FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COOMERCE



Le soluzioni adottate per migliorare la rete sono:

1. Utilizzo di server di backup che garantiscono la funzionalità dell'e-commerce nel caso in qui quelli principali siano offline. HOT Site, per un ripristino repentino del servizio.
2. Server web in maggior quantità, meglio se distrubuiti in un area geografica più grande, per distrubuire meglio il carico sulla rete.
3. Implementazione di sistemi anti DDOS.
4. Un' eventuale opzione più economica può essere quella di fare un backup sul cloud, utilizzando un DRaaS, che numerose compagnia mettono a disposizione come Amazon Web Services, MIcrosoft, etc.

FLUSSO APPLICAZIONE - RETE INTERNA

FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE

FLUSSO UTENTE - APPLICAZIONE E-COOMERCE

Traccia Bonus
Dalle verifiche effettuate, abbiamo riscontarto che entrambi i malware appartengono alla famiglia degli spyware, in quanto raccolgono molteplici informazioni del computer attaccato.

1. https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

   Il primo malware raccoglie informazioni di sistema e crea una copia che viene passata come backup, modifica le policy di esecuzione della PowerShell, esegue una scansione dei software installati e modifica le autorizzazioni di alcuni file o directory.

2. https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

   Il secondo malware si presenta come un normale download del browser Edge, ma proviene da una sorgente sospetta, un drive, anziché da una fonte ufficiale Microsoft. Oltre a leggere le specifiche del browser, il malware droppa eseguibili Windows legittimi, sostituendoli, e disabilita il SEHOP, una tecnica di protezione per prevenire attacchi che sfruttano lo Structured Exception Handler Overwrite. Per evitare tali situazioni spiacevoli, è consigliabile scaricare solo prodotti verificati da fonti affidabili, e mantenere un antivirus aggiornato insieme a un firewall funzionante per contrastare questi attacchi.