CEDACRI GROUP

DNS Exfiltration

14 Novembre 2019

GRUPPO CEDACRI: IL PRINCIPALE OPERATORE ITALIANO NEL MERCATO DELL'OUTSOURCING DI SERVIZI PER LE ISTITUZIONI FINANZIARIE

CEDACRI GROUP

CEDACRI	Oasi	SiGRADE	C-GLOBAL	Docugest	CEDACRI INTERNATIONAL
GESTIONE COMPLETA DEI SISTEMI IT (Full outsourcing, Facility Management, Applicazioni SW)	SOLUZIONI E SERVIZI PER ANTIRICICLAGGIO E SEGNALAZIONI DI VIGILANZA	SOLUZIONI SOFTWARE E SYSTEM INTEGRATION	SERVIZI DI BUSINESS PROCESS OUTSOURCING	STAMPA E POSTALIZZAZIONE	SOFTWARE FACTORY E SERVIZI DI BPO

GRUPPO CEDACRI: DATI CHIAVE

Più di 150 Clienti, tra cui banche, istituzioni finanziarie, aziende industriali e di servizi

Più di **€ 330 mln.** di **fatturato** di **gruppo** nel **2018***

EBITDA: 20% Nel 2018

15 Azionisti

Oltre 1600 professionisti a **supporto** dei **nostri Clienti**

2.700 filiali gestite

30.000 risorse utilizzatrici

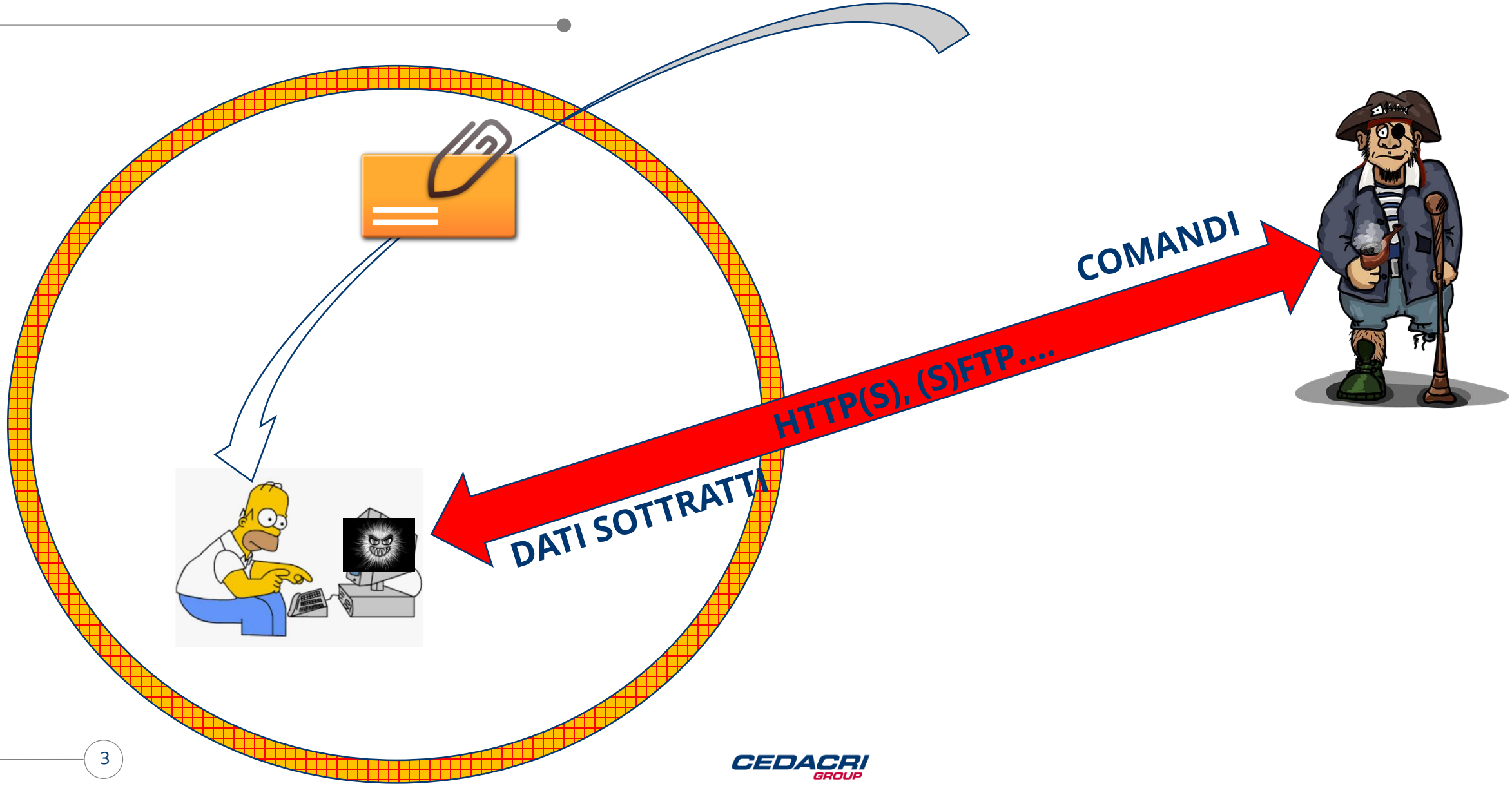
50 mln. transazioni gestite **quotidianamente**

46.000 MIPS di Potenza Computazionale di Mainframe

7.500 server

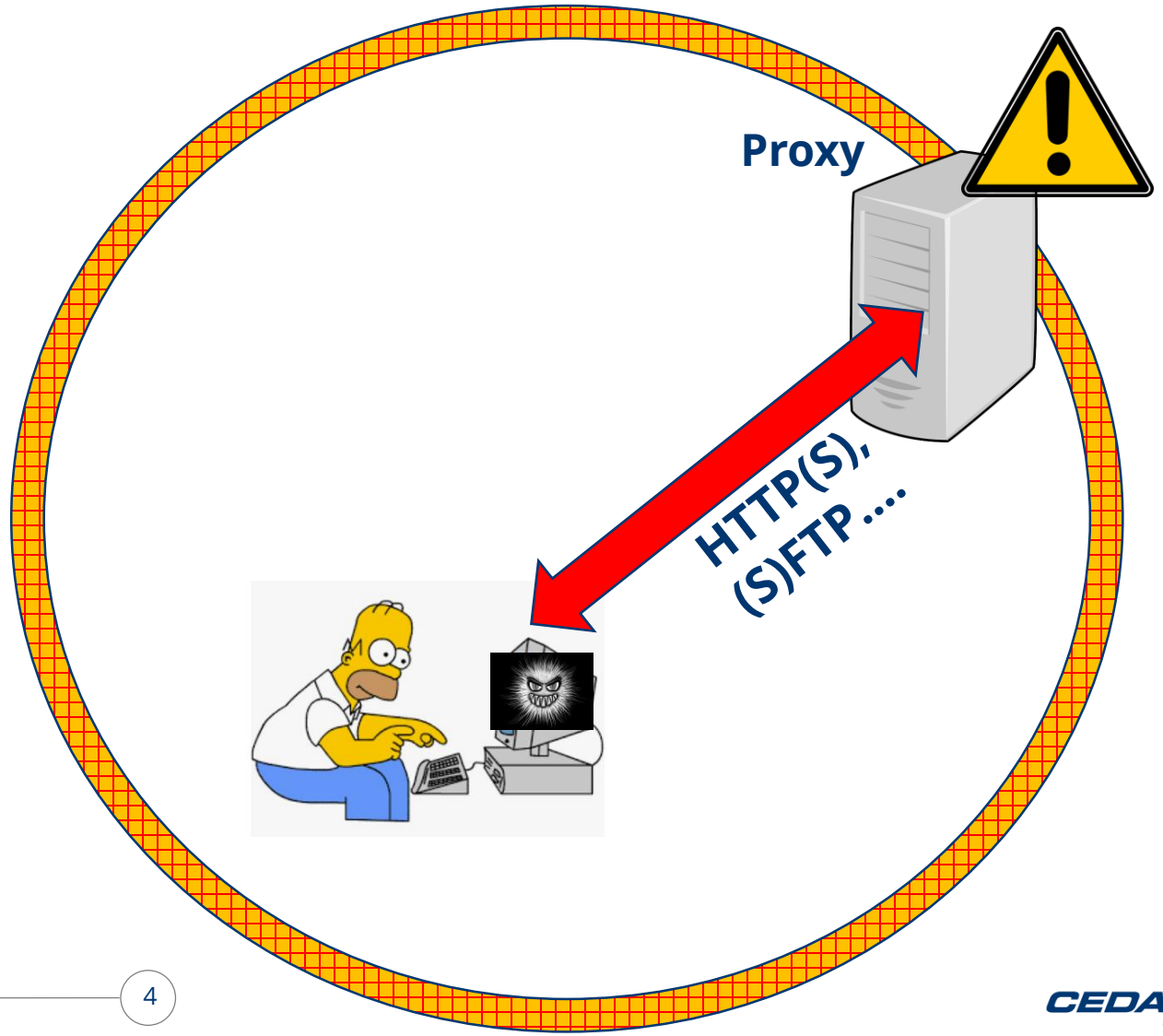
*dati IFRS, proforma incluso OASI

Il problema del tunneling e della data exfiltration



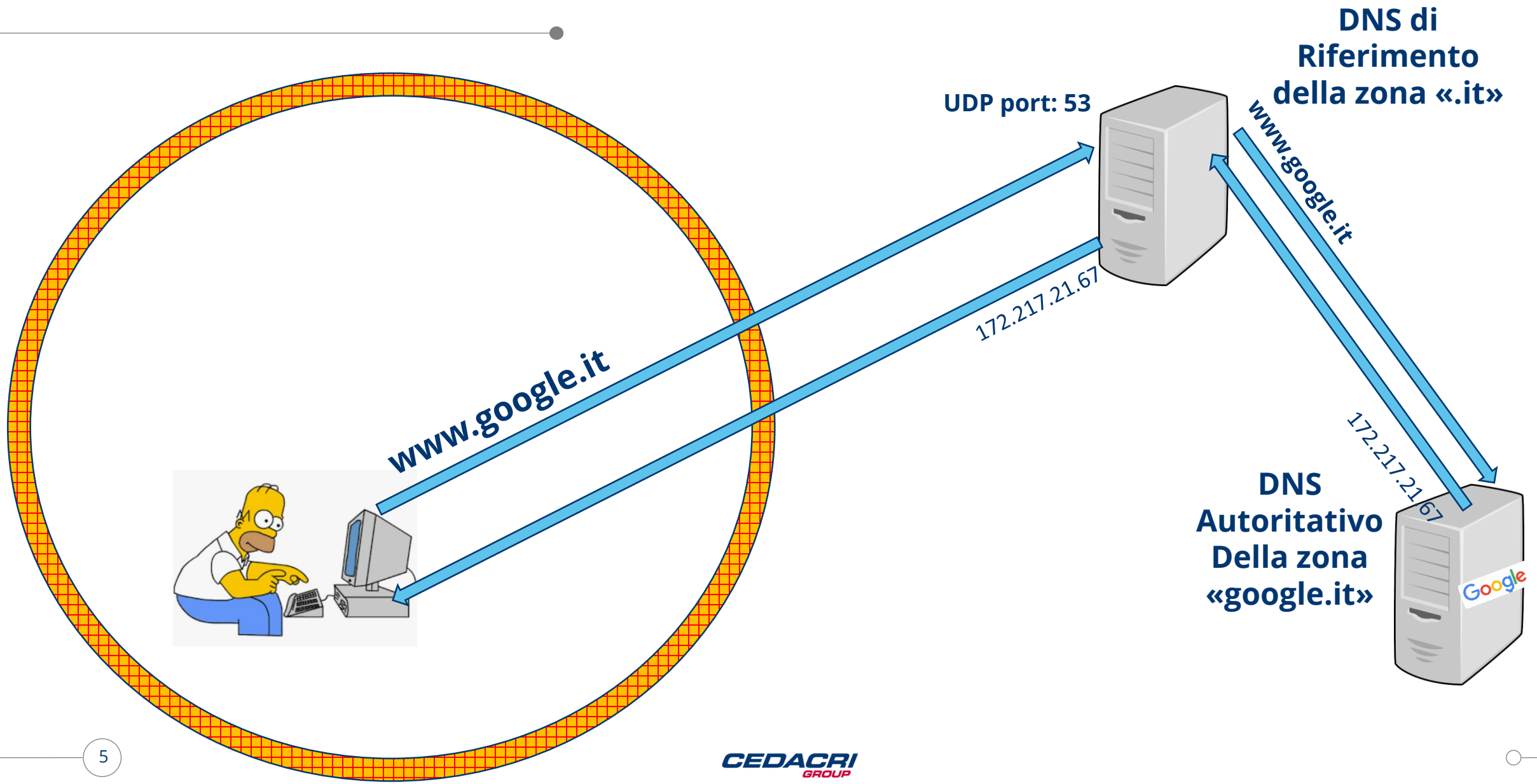
CEDACRI GROUP

Il problema del tunneling e della data exfiltration



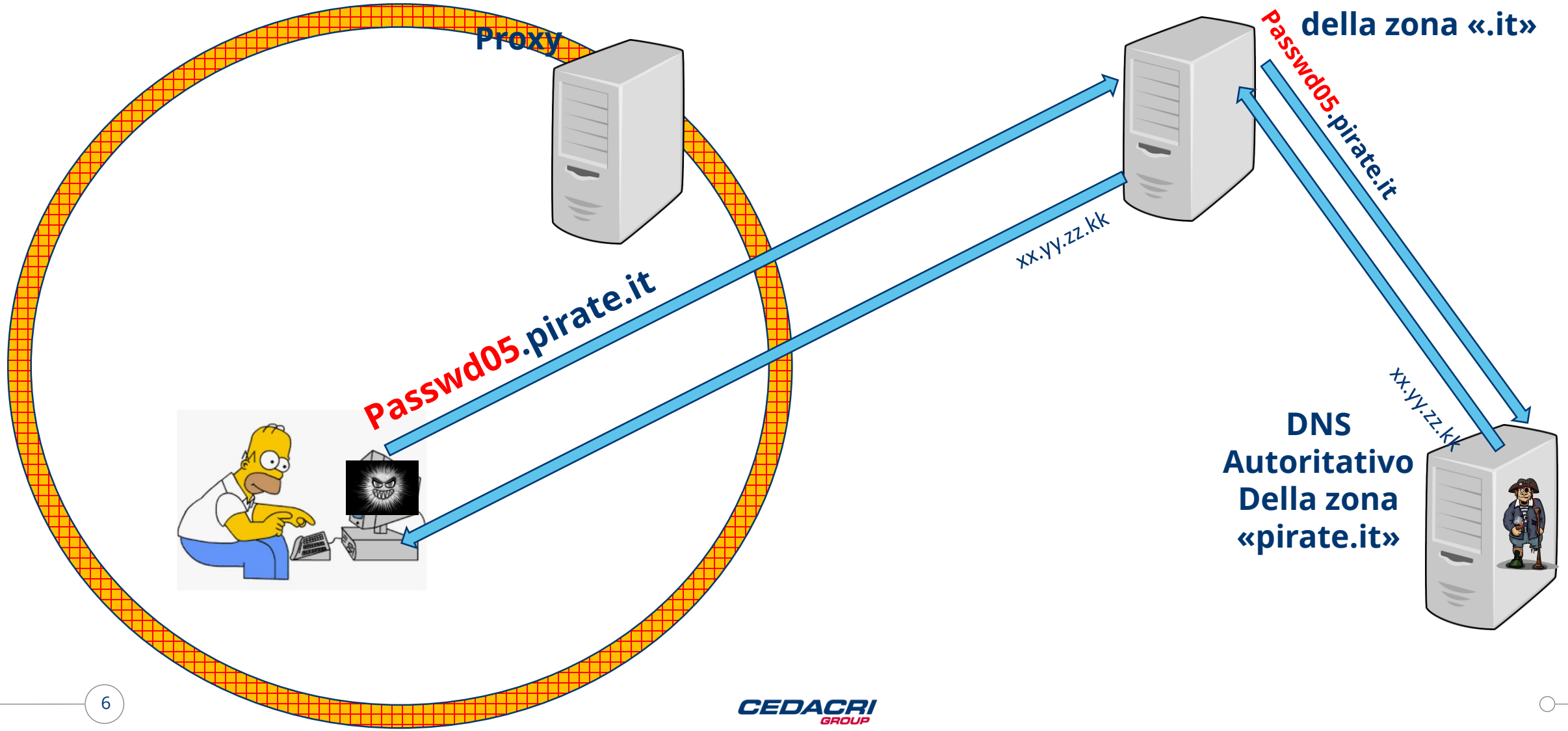
CEDACRI GROUP

Funzionamento logico del Protocollo DNS



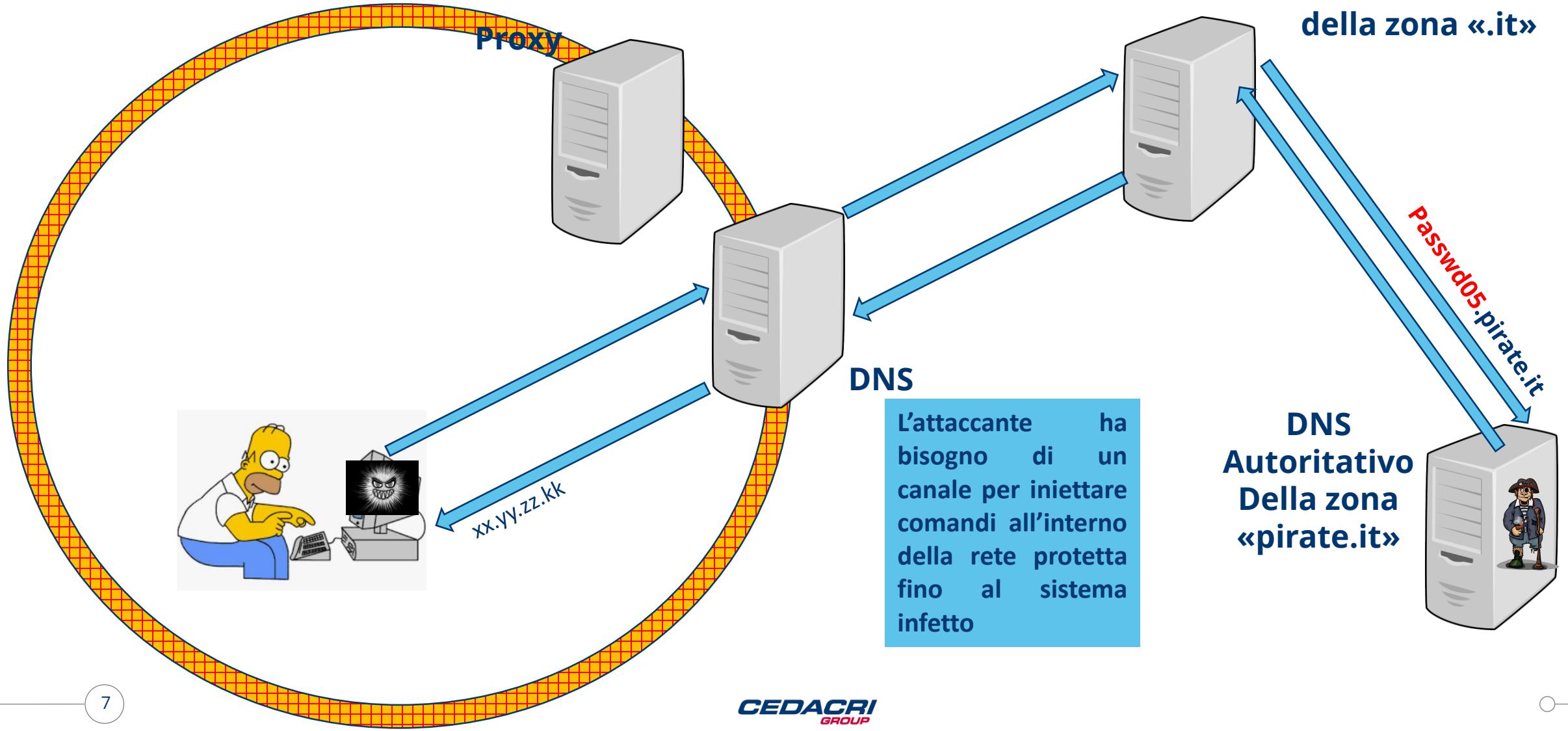
CEDACRI GROUP

DNS Exfiltration



CEDACRI GROUP

DNS Exfiltration



L'attaccante ha bisogno di un canale per iniettare comandi all'interno della rete protetta fino al sistema infetto

DNS Resource Record Types

Il protocollo DNS è uno dei primi creati agli albori della Internet e come era tradizione è estremamente aperto alla sperimentazione

Ci sono 34 tipi «ufficiali» di query DNS, 12 non ben definiti e 4 sperimentali.

il più noto è il type **A** che richiede in risposta l'indirizzo IPv4 della risorsa.

Il type **AAAA** richiede in risposta l'indirizzo IPv6 della risorsa

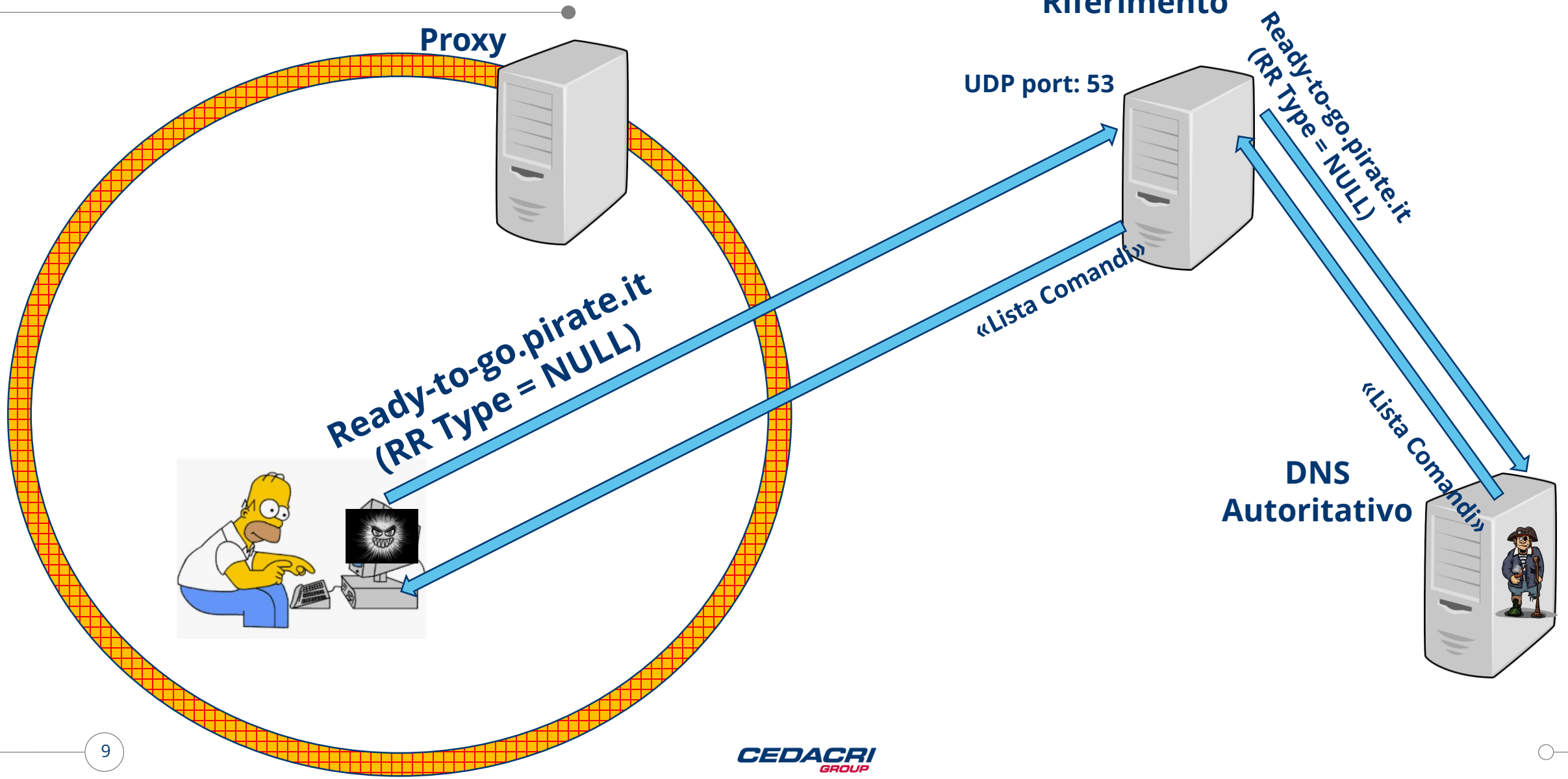
Il type **CNAME**: Permette di collegare un nome DNS ad un altro. La risoluzione continuerà con il nuovo nome indicato dal record CNAME. Questa funzione è molto utile quando, ad esempio, sullo stesso server sono disponibili più servizi come FTP, HTTP, ecc. operanti su porte differenti. Ciascun servizio potrà avere il suo riferimento DNS (ad esempio ftp.example.com. e www.example.com.).

Il type **TXT**: Era stato pensato per aggiungere commenti leggibili ad un record DNS. Dall'inizio degli anni novanta, invece, è utilizzato per trasferire informazioni di sicurezza in accordo alla RFC 1464, opportunistic encryption, Sender Policy Framework e DomainKeys. Il sistema di DNS dinamico del server DHCP ISC utilizza campi di testo nelle zone dinamiche per identificare i record modificati dal server DHCP.

Il type **NULL** ha la seguente definizione da RFC: «Anything at all may be in the RDATA field so long as it is 65535 octets or less. NULL records cause no additional section processing. NULL RRs are not allowed in master files. NULLs are used as placeholders in some experimental extensions of the DNS.»

Questi ultimi 3 tipi sono perfetti per l'invio di comandi da parte degli attaccanti

DNS Tunneling



CEDACRI GROUP

Vantaggi e Svantaggi del DNS per la creazione di tunnel


Il DNS molto spesso non è controllato ne proxato


Il DNS è leggero e quindi generalmente non è soggetto a limitazioni di carico, in più il meccanismo dei DNS autoritativi permette di suddividere i messaggi su più dominii e quindi su più server degli attaccanti


Il DNS è basato su UDP e quindi non è intrinsecamente affidabile

Soluzione: costruzione di un protocollo di controllo TCP like sui payload scambiati


Il DNS è in chiaro

Soluzione: cifratura dei payload scambiati

Contromisure

Seppure le singole chiamate DNS utilizzate per il tunneling sono difficilmente identificabili, Il traffico generale del tunneling è strutturalmente molto diverso dal normale traffico DNS, in particolare si possono identificare:

- Dominii molto più cercati della media
- Presenza massiva di query type normalmente poco frequenti come TXT e NULL
- Contenuti anomali nelle risposte a tali query

Esistono sistemi appositi che su base di considerazioni statistiche e sulla base della reputation dei dominii cercati rilevano queste anomalie e allertano sulla presenza del rischio di exfiltration (efficacia prevista circa il 95% mediante l'utilizzo di sistemi di reti neurali).