Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

Strumenti per le strutture

Luca G. Carbone
Mini WS CCR sulla Sicurezza Informatica
13-15/2/2023 –Padova

DNSRPZ/DNS firewall

What is it?

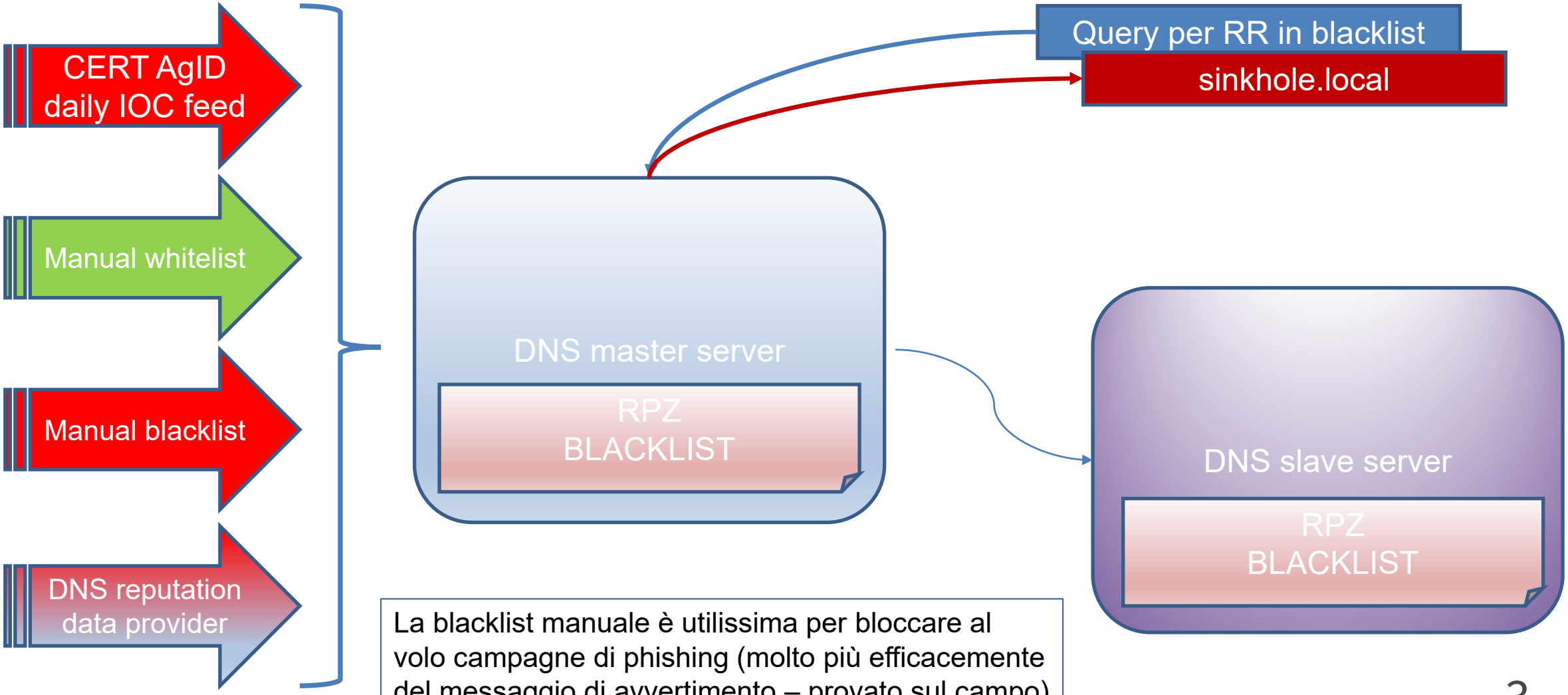
Domain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones (**DNS RPZ**) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide alternate responses to queries. It is currently implemented in the ISC BIND nameserver (9.8 or later). Another generic name for the DNS RPZ functionality is "DNS firewall".

Why IS RPZ useful?

The prime motivation for creating this feature was to protect users from badness on the Internet related to known-malicious global identifiers such as host names, domain names, IP addresses, or nameservers. Criminals tend to keep using the same identifiers until they are taken away from them. Unfortunately, the Internet security industry's ability to take down criminal infrastructure at domain registries, hosting providers or ISPs is not timely enough to be effective. Using RPZ, *a network or DNS administrator can implement their own protection policies base based on reputation feeds from security service providers on a near-real-time basis:* if one knows a bad hostname or domain name, one can block clients from accessing it or redirect them to a walled garden.

From https://dnsrpz.info

DNSRPZ: implementazione



La blacklist manuale è utilissima per bloccare al volo campagne di phishing (molto più efficacemente del messaggio di avvertimento – provato sul campo)

DNSRPZ: possibile attività

- Definire (e migliorare) configurazione: master RPZ centrale vs master RPZ indipendenti in ogni struttura;
- Analisi log per individuazione clienti potenzialmente compromessi;
- Migliorare gestione feed CERT-AgID;
- Testare altri feed e feed diretto da DNS reputation data provider:

Provider	Service
DissectCyber	rpzone.us
FarsightSecurity	Newly Observed Domains and example
InfoBlox	DNS firewall
SpamHaus	Several popular block lists are available via RPZ. Data sheet, Article, Pricing
SURBL	Data Feed
SWITCH	SWITCH DNS Firewall
ThreatStop	DNS firewall and announcement
Malware Patrol	RPZ Package

log traffico di rete/eventi di sicurezza

- Idealmente ogni struttura dovrebbe dotarsi di uno strumento per l'analisi del traffico geografico inbound/outbound:
  - sniffer di rete su porta mirrored del router di frontiera o del backbone collassato: **argus**, **zeek** (ex bro)
  - NIDS/NIPS: **snort**
  - raccolta dati netflow et similia da router di frontiera
  - log da firewall (o da router ove la potenza di calcolo lo consenta)
- i dati raccolti (e possibilmente normalizzati) vanno salvati localmente e inviati al sistema di analisi centralizzato (quantità, qualità e tipologia dei dati da definire)
- anche i log da HIDS (**wazuh**) o **fail2ban** su macchine selezionate (per esempio bastioni) o honeypot sono di un certo interesse e vanno inclusi.

firewall

- Difficilmente ci potremo permettere di finanziare un NGFW (abbonamento annuale alle signature incluso) a ogni struttura, soprattutto con l'avvento delle linee geografiche generaliste a 10G. Possibili soluzioni:
  - verifica prestazioni e potenzialità FW open source (**pfsense**, **opnsense**, **FW ad-hoc**?) su H/W attuali (collaborazione con *netgroup*);
  - FW a protezione di subnet *sensibili* (ove le reti siano ancora piatte vanno opportunamente strutturate);
  - **firewalld** supporta pienamente **ipset**: è possibile superare il modello fail2ban dotando macchine sensibili (bastioni, mail server, …) di configurazioni in grado di bloccare dinamicamente da singole reti a intere nazioni (tra l'altro: l'attività di raccolta delle liste di reti malevole è rimasta al palo, e andrebbe rimessa in cantiere).