Repulsa IP Reputation Service

CautelaLabs®

Over half of all Web users are not human users at all; they're bots. A bot is an automated or semi-automated tool that carries out tasks requested by shady sources. Often some of these bots – like search engine crawlers – are harmless; others are more dangerous, probing sites, scraping Web content, posting spam messages, or attacking Websites. Besides stopping dangerous bots, organizations must protect their applications from hackers, who often use anonymous proxies and or networks to cloak their identity.

Modern threats can come from anywhere, anytime. As the internet evolves hackers have begun using orchestrated attacks on organizations' infrastructure. Attackers now use a wealth of methods to infect innocent hosts, and control these infections through organized botnets in order to launch automated phishing, spamming, and DDoS attacks on critical business applications and services.

The key difference with modern threats is that they can strike quickly and disappear, only to re-appear in another form in rapid fashion. It is important to have a dynamic solution that can address these evasion techniques. If a malicious actor's machine attacks a target in one location, the rest of the global network needs to learn and update quickly in order to pre-empt the next wave of attacks.

The Cautela Labs'® ***Repulsa*** real-time IP Reputation Service aggregates data from locations and sources around the world that collaborate to provide up to date information about threatening sources. Repulsa is Latin for denial, rejection or refusal and it's what the Cautela Lab's® service actually does to those bad sources or blacklisted IP's. The ***Repulsa*** service automatically delivers the blacklisted IPs directly to your firewalls which can be enforced for inbound and outbound traffic. ***Repulsa*** is a cloud based service that protects your environment from malware such as botnets, Trojans, worms, honeypots, etc.

Overview

Every packet on the internet has a source and a destination IP address. Disabling communication to/from malicious IPs is effective, but difficult without comprehensive intelligence. The Cautela Labs® ***Repulsa*** Service provides up-to-the minute IP intelligence, enabling partners to better protect our customers' networks.

Today, cybercriminals have an immense number of exploits and attack vectors available to them, and they use numerous techniques to hide their identities and activities, such as encrypted communications, DNS cache poisoning, URL redirection, hyperlink obfuscation, etc. However, every packet on the internet has a source IP address and a destination IP address, so disabling inbound and outbound communications to and from IPs known to be malicious is highly effective. But how does one know which IPs to block? How can administrators differentiate between an employee chatting online with a colleague in another part of the organization or the world, or an attack on the corporate network?

The ***Repulsa*** Service helps network and security vendors augment their customers' security by adding a dynamic IP reputation service to their defenses. Repulsa provides its customers with a continuously updated feed of known malicious IP addresses directly to the customer's firewalls.

Prevention, not just detection

Repulsa capitalizes on the value of utilizing the latest up to the minute threat intelligence to identify and protect against security threats. The blocking of traffic is customized according to each client's network environment, data security standards, configuration policy and current security posture. Protection policies can be configured to monitor only, manually block, or automatically block based on certain pre-defined criteria. Each client's blocking policy is designed to maximize threat protection independent of any other countermeasures that are deployed whether independently managed or as part of a managed subscription agreement.

Technology

Repulsa utilizes proprietary data feeds from as many as 30+ unique data sources that include both public and private sources of attacker intelligence. In addition, information gathered through our own network of sensors and client information sources is also used to further identify attack trends, newly released threats, and network reconnaissance.

Our information sources are varied and include specialized as well as broadly recognized attack sources and data feeds. Specialized data intelligence sources include information on botnets, attacks launched from illegal (private) address space, and traffic that originates from countries and sources that may be associated with criminal networks.

Utilizing Repulsa' s Cloud based event correlation technology, IP reputation and Firewall Log information is used to continually monitor both inbound and outbound connections for threats such as:

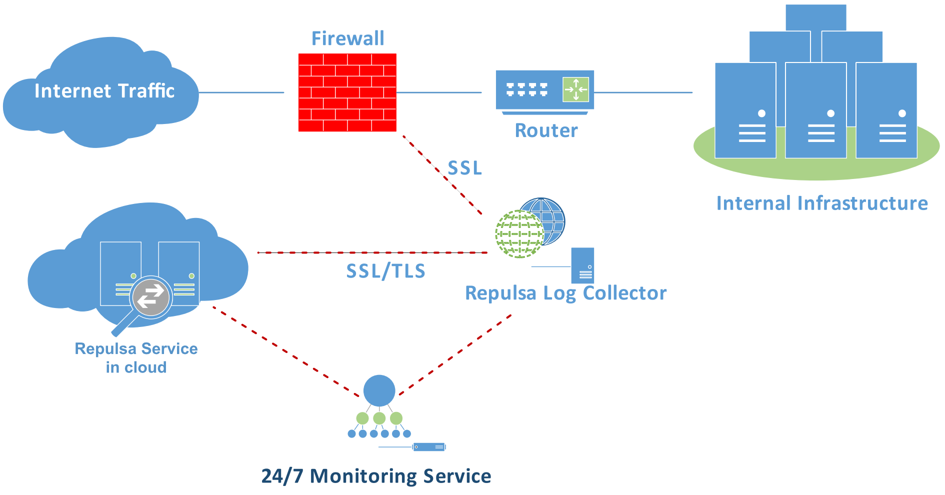
- Infection from botnets & remotely controlled hosts
- Keyloggers
- Trojans, viruses, worms
- Malware/spyware
- Encrypted tunnels
- Phishing sources
- Zero day threats

Repulsa works alongside and enhances IP Reputation based services that may already be employed for use with for URL Web and content filtering and e-mail anti-spam services and is not designed as a replacement for those systems but more targeted towards your firewall so the threat is stopped at the entry and exit point. By further integrating with correlation of firewall logs a continuous close loop environment is setup such that even if there is bypass of the IPs addresses those incidents will be escalated to help take appropriate actions.

Repulsa can integrate with virtually any firewall device. In addition we have developed specific integrations for use with IPS, WAF, and NAC with leading security vendors in each area.

Closed Loop Approach

Utilizing ***Repulsa*** in a cloud-based environment means that your organization does not have to worry about custom integration, long deployment cycles or procuring and owning additional hardware and software licenses. The ***Repulsa*** IP Reputation service is fully integrated into our SIM/SEIM environment which is used to monitor, triage, and block threats as they are identified and remediated in real-time within our Security Operations Center (SOC).



Repulsa is an IP Reputation Service that identifies and prevents internet based security threats based on compiled intelligence regarding their historical interaction on the internet and whether a source is known or suspected to have been involved in committing fraud, computer attacks, or criminal enterprise.

Figure 1: Repulsa IP Reputation Service