File Reputation: Effective Proactive Approach

White Paper

Document Version (esnfp 14.0.0.1)

Creation Date: 20th Feb, 2013

File Reputation: Effective Proactive Approach

White Paper

In this paper, we explain information about what makes digital security reputation system effective. What is the use of reputation system? How is it effective from the traditional approach? What are the benefits?
Since the early days of online communities, reputation is the most important factor in doing online business, Wikipedia define reputation as *"Reputation of a social entity (a person a group of people, an organization) is an opinion about that entity, typically a result of social evaluation on a set of criteria. It is important in education, business, and online communities"*.

When we talk about reputation, first we need to understand that reputation is dynamic in nature and temporary, it keeps changing frequently as soon as the content changes. Reputation system is more proactive in comparison to the traditional approach. Reputation is more critical today to cyber security than ever before, as more users are connected to internet to access emails, files and URLs.

Bad guys (cybercriminals or hackers) realize that traditional approach is reactive and cannot keep up with extremely high volume of threats, this opens up the window of opportunity to attack a system and gain access and do whatever they want to, until the virus signatures are downloaded, bad guys have already done the damage. Major drawback of traditional approach is the volume of virus signatures, they are just skyrocketed, enterprises are struggling to find ways to distribute virus signatures more efficiently and quickly, considering large amount of signatures, it is very frustrating and time consuming in bigger environments. The number of threats being released by bad guys is growing at an alarming rate.

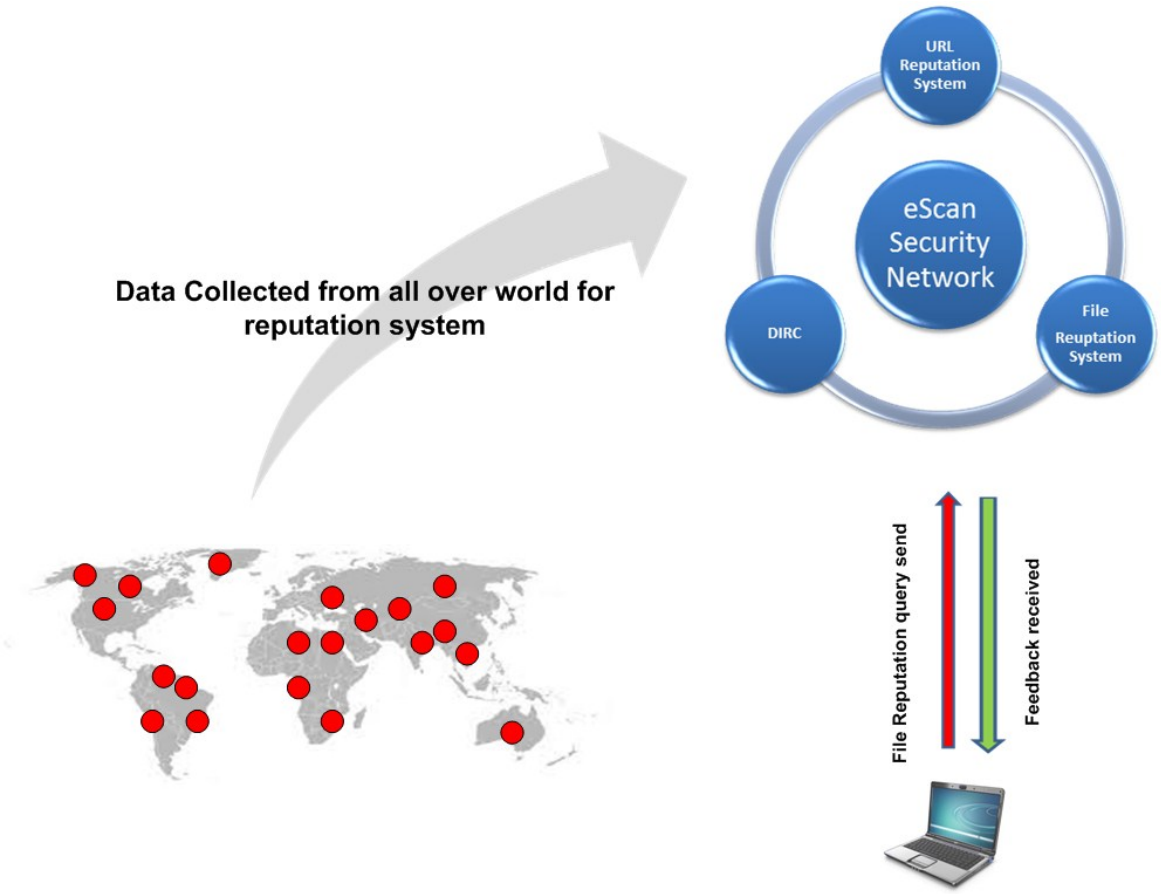
eScan experts have been analyzing and monitoring these threats over the years, and the rate in which the threats are found is eye-opening. If we think 5 years ahead from now, using traditional approach alone will not be enough; you need to have something which should be fast and accurate. When we say fast, it means, it should detect new threats on-the-fly and remediate them immediately. Accuracy will be the important factor in avoiding false positives. Having said that eScan has developed proactive approach over traditional method, this technology is called as File Reputation, Domain Reputation. In this document we will discuss about file reputation approach.

Reputation is just not an important factor of security system, it is essential. If we have to protect our customer as quickly as threats are released, then traditional approach is not enough, so how eScan protects their users from online emerging threats? Answer is simple, eScan uses file reputation system to analyze file reputations online, we check the reputation of the file and identifies whether the file is clean or suspicious. The fact is that reputation is dynamic, so the reputation may change quickly. On the other hand bad guys are targeting to propagate threats to avoid detection, cause minimum damage and achieve a high objective. To combat these kind of threats eScan experts developed a sophisticated technology called as file reputation service, in eScan, it has been referred as **eScan Security Network + Proactive Monitoring Behavior**, it is a combination of two methods which go hand in hand, available within all product ranges from SOHO to Enterprise level. eScan File reputation is a collective intelligence about that object, eScan tag that object as per the online reputation and then decides the appropriate action based on that reputation.

(Please refer to HIPS whitepaper for more information about Proactive Monitoring Behavior)

How this is achieved?

eScan lab receives feedback from all participants worldwide, in which eScan product queries to eScan reputation system on cloud, based on these feedbacks, data is generated on eScan Reputation System and then analyzed, based on the analysis; reputation database is updated on the cloud, which will be available to all the eScan customers.



Queries and their responses are important events into reputation system, robust reputation system, those with millions of eScan products used worldwide, sends request to reputation system, this is how data is collected on the reputation system and will be available to all eScan users within few seconds. This proactive approach is proven approach in finding zero-day threats. An effective reputation system must collect data efficiently, rapidly and should distribute it instantaneously.

eScan Security Network receives millions of file reputation queries on daily basis and eScan responds to those queries based on collective intelligence.

What are the advantages of File reputation system?

1. Increase in Scanning speed
2. Low false positives
3. Higher accuracy
4. Independent of traditional virus signatures
5. Blocking of zero-day threats

6. Low system resource utilization

These are the few benefits of cloud file reputation system. eScan is striving hard to give immediate protection with less complexity.