#1 Choice of DIGITAL WORLD

eScan™ Enterprise Security

RANSOMWARE

eScan debuts new Technology for Detection and Mitigation

An ISO 27001 Certified Company

www.escanav.com

We started our tryst with Ransomware when it started gaining prominence way back in 2012, however Ransomware has been around for almost a decade.

During the initial stages, Ransomware created the effect of awe and shock, unlike Trojans or Malwares or APTs, Ransomware made its presence known. The only differentiating factor was that the message was Loud and Clear – You have been Infected.

For all these years, we have been observing the covert methods of a virus while it was silently infecting the system, staying resident and infecting other systems, moreover, many of these viruses started implementing the logic of Command and Control, wherein, vital information was being discreetly leaked or stolen. The level of expertise required for writing a virus was tremendous as the author had to always find ways to stay a step or two ahead of the detection mechanisms and at the same time, the criminals had to invest into infrastructure which would handle the stolen information.

These criminals also rented out these very infected systems, commonly known as Zombie Computers, to other criminals , who would then carry out their nefarious activities viz. Sending Spam, Initiating DDOS attacks , Bitcoin-mining etc.

However, when we speak about Ransomware, during the initial days, they were thought of as a highly sophisticated piece of code, since encryption was involved. However, Ransomware creators also evolved their tactics and started identifying the important files which would be attacked. There are numerous encryption libraries available which can be used by not just the advanced programmers but also by the script kiddies. It wasn't imperative for the programmer to be an expert in encryption, since all the information was readily available and the points of interest from the ransomware author's perspective were -

1. Ability to sneak into the system.

2. Encrypt the files based on their extensions.

3. Transfer the encryption keys back to the CNC server.

Ransomware infection routines came in various forms, started off as a compressed binary, and when the various vendors started blocking such files from gaining a foothold, we started finding Ransomware being delivered as embedded macros in Doc or Docx files. Very recently, they started using javascripts, VB Scripts and Powershell based scripting to create Ransomware.

In order to combat these, vendors started blocking scripting engines, however, for how long is this game of cat and mouse going to continue? Researchers have been finding it increasingly difficult to find the elixir which will stop Ransomware in its tracks.

Detection of Ransomware is not just the only solution, sink-holing of the DGA based CNC will simply setback the criminal by 3-4 weeks, there can be instances when a Ransomware sneaks into the well protected environment consisting not just the End-Point Security Solutions but also bypassing the perimeter / gateway security appliances and encrypts the local as well as network files.

Conventional backup systems relied on the fact that there are certain folders which are considered important and initiated the backup of the pre-configured folders. However, Ransomware is file-centric, in some instances it will encrypt all the picture files and will leave the thumb-nails file just to make you realize as to what could be lost if ransom is not paid.

We at eScan, have been actively pursuing Ransomware at all levels, analyzing them, studying their behavior and finding out different ways to detect and mitigate this threat, moreover provide a mechanism for eScan users to be resilient.

eScan, now debuts a **Proactive Behavioral Analysis Engine** (PBAE) that monitors the activity of all the processes on the Local Machine and whenever PBAE encounters an activity or behavior which is reminiscent of a Ransomware, a red flag is raised and the process is rendered inactive from conducting any further damage. However, Ransomware is also known to encrypt files residing on the network share, in such cases, when an infected non-protected system is accessing the Network Share of a protected system and tries to modify the files residing over there, PBAE, will immediately invalidate the network session.

In our fight against Ransomware we were working on an Intelligent Shadow Backup mechanism which can be triggered during such eventualities, enabling the users to quickly overcome the aftershocks of Ransomware.

Ransomware to the likes of Locky, Zepto, Crysis, Crypto to name a few, along with their variants are being tackled with relative ease by **eScan's Proactive Behavioral Analysis Engine** (PBAE). Moreover, we have been studying the events from our cloud server and have been successful in detecting and mitigating thousands of Ransomware attacks since the rollout of **Proactive Behavioral Analysis Engine.**