Interview with eScan Antivirus!

August 25, 2011 in How-to with 0 Comments

System-log has for the last year made quite a few articles about staying safe on the internet, and how to stay safe while using your computer in general. In january I tested **eScan Internet Security and Antivirus** and was impressed with the package. My final conclusion was :

> *All in all I have no problems recommending this antivirus solution to my readers. If you are using your computer online with browsing, email, messaging, twitting, facebooking or whatever; a stable internet security solution is vital!*

I have kept in touch with eScan since my article, and I recently got the chance to interview them regarding their work and a bit about their history. I am above average interrested in computers and software – and one of my first computer related dreams was to work for the good side and save the world from the Virus threat! I never got around to program my own antivirus solution – I didn't even get around to save the world – but i'm glad someone is doing their share of work to create a safe software package for the computer – **eScan**.

The interview!

Q.
Where is eScan located and how many employees are working to make the computer a safer place?

Incorporated in New Jersey, USA, eScan has its offices in India, Malaysia, Germany and South Africa. Internationally, it is represented by a widespread network of partners, in more than 90 countries. eScan team collectively consists of 170 employees, contributing in different ways with their excellence, making computer a safer place.

The CEO and Managing Director, **Mr. Govind Rammurthy**

Mr. Govind Rammurthy graduated from VJTI Institute of Engineering with a degree in Computer Science. After graduation, he had a brief stint with TELCO, one of the fortune 100 companies in India, where he

was involved with the core team in managing the complete networking project of Telco. Govind founded MicroWorld in 1993, and within a short span, he has transformed MicroWorld into a global company with a large partner network spread across the world. Today, Govind is one of the most well-known and respected figures in India's Information Technology sector.

Q.
How does a company like eScan actually work? Waiting for the next virus to appear, or do you stay one step ahead the enemies – working on ways to prevent viruses from appearing in the first place?

eScan is developed as a next generation protection that actively contributes in combating complex and ever evolving IT threats such as Viruses, Spyware, Spam, Phishing, Hacking, Data Theft and Zero day threats. Practically, it is not possible to prevent the development and release of a Virus. However, as eScan is powered by innovative technologies, it provides futuristic security intelligence to computers, which not only helps in securing your PC from next generation threats but also provides Zero day protection.

Q.
With threats like malware, phishing, etc in addition to the well known virus – what products would you recommend using (both types of software + products as
an example from eScan).

eScan range of products includes the entire spectrum of Information security, making it a one-stop shop for protecting all Information Security assets. These products are segregated for Enterprise, SMB, as well as Home User segment which basically includes a standalone Anti-Virus and Internet Security Suite. eScan Internet Security Suite provides protection against ever evolving threats such as malware and other Internet borne threats which include, such as Viruses, Spyware, Adware, Keyloggers, Rootkits, Botnets, Hackers, Spam, and range of Information Security threats. It includes a Malware URL filter that protects endpoints against Drive-by downloads as socially engineered Malware attacks pose as one of the largest risks to individuals and organizations. Also, it blocks access to malicious websites/ URLs, providing ZERO Day protection to computers. Apart from this eScan also includes a set of predefined access control rules that you can customize as per your requirements. The Firewall has been enhanced for seamless integration with your operating system, including the Network Traffic Monitor that monitors incoming and outgoing network traffic. It also allows users to block execution of network-based executable files, thus preventing network based viruses from spreading.

eScan effectively performs Real-time scans on files, e-mails, e-mail attachments with its advanced and innovative technologies. It keeps the computer safe from infections with the help of its enhanced Self Protection Technology that prevents new generation malware from either disabling eScan or deleting its critical files. It also scans content for confidential data, prohibited information, offensive, and obscene language.

Q.
When surfing the web and using its services – what advises would you give the average user to stay safe?

No doubt, internet is a great medium through which people communicate, share files, etc. , though a dangerous to use, full of hackers, and identity thieves. Hence, user should be cautious while using its services. There are certain things that one should keep in mind while using such services;

- Always use Anti-Virus software that compromises of a web protection module to a standalone Anti-Virus to protect computer from viruses that destroy information, crash systems, and decrease performance.
- Scan your computer on regular basis and make sure your Anti-Virus is updated regularly.
- Make sure that the firewall is turned 'on'. This will filter internet traffic, insure harmful programs and prevent hackers accessing your system.
- Be it emails, texts, and pop-ups that request personal information to update your accounts, use only phone numbers tied to your financial statements or bills when conducting business.
- Make sure to secure your browser via the Internet option or tools menu by increasing your security settings.
- Keep your passwords on a drive which is only accessible to you and make sure it is in the encrypted form. This prevents its access from thieves and hackers.
- Never open an email attachment sent by a stranger as this is the most common way of getting your pc infected.
- While receiving attachments from someone you know, make sure to scan all attachments as this will prevent.
- In case a program application download does not come from a trusted site, then don't download it as such programs majorly, along with programs from game sites and unsolicited pop-ups contain Spyware, Malware, or viruses.

Q.
What problems are most common by your customers today? What products are most wanted?

These days, the common threats that an average computer user faces every day are Viruses, Worms, Trojans, Spyware, Adware, Phishing scams. Also, network security issues such as scans, social engineering, computer theft that causes identity theft and other content security issues, network outbreaks, firewall traffic control, etc. are increasing. According to a new report from Cisco, the current trend of mass attacks have given way to targeted attacks with unique forms of malware, and this trend is accelerating. SQL Injection has topped other lists for IT security. There is an increase in the issues such as Mobile security at data layer, Compliance auditing, Identity management, Patch/update management, Application defense as well as Intrusion detection.

Our wide range of products provide a comprehensive proactive protection from evolving threats to all the segment of users including the SOHO, SM, Enterprise as well as Corporate users.

Q.
Historically – what virus was the worst eScan has dealt with, and how did you solve the situation?

It is very difficult to categorize the virus with regard to the harm it will cause. Viruses can attach themselves to just about any type of file and are spread as infected files. Some viruses are relatively harmless, while others are very devastating. They can destroy files, software, program applications, and cause the loss of data. In recent times, the worst malicious program that we dealt with was the Conficker worm. The worm basically propagated through the network exploiting vulnerability in a network service found within Windows OS. After analyzing the effects of the worm on an infected system, we at eScan modified our scan engine as well as our real time monitor to counter attack the changes made by the worm. After analyzing the effects of the worm, updates were immediately released to curb
the growing threat. What made it really difficult was the fact that the malicious code writers kept on releasing new variants of the worm. Once the computer was infected; in addition to transferring the worm to other computers in the network the infected system was
also converted into a Botnet. Security patches were released by Microsoft to prevent the worm from spreading. However, computers keep getting infected since most users disable the automatic download /install of Microsoft security patches. Hence, to
counter this problem, eScan implemented its users with a new feature wherein some important Microsoft security patches necessary for the operating system are downloaded and installed on the system. This took care of the propagation of the worm due to the vulnerability of the operating system.

To help thwart malware from spreading at a rapid rate, eScan comes with innovative technologies that help protect PC users from existing as well as Zero Day threats. In addition, its enhanced self protection feature keeps the PC safe from a wide range of security threats.

Q.
If you could see into the future – what is tomorrow's threat on the computer – and what must the user do to be prepared?

With the ongoing change in malware trends, security issues such as Data Loss Prevention (DLP), wireless security and managed security services continue to grow at a rapid rate. Moreover, the rise in Internet activity has created new ways for Internet borne threats to spread. Furthermore, social networking has become a major target for scammers and cyber criminals as there has been a significant increase in the number of users for networking sites such as Facebook, Twitter and Google+. These sites have become a haven for malicious hackers, crackers and jackers as they have made it easier to launch attacks with hundreds of millions of people engaging in these online communities. Also, users are more likely to click on links and download content they believe were sent by people they know and
trust. The rapidly growing mobile device audience is unfortunately a new frontier for fraud, irresistible to criminals.

Data loss/breaches and internal threats top the charts as security issues along with the venerable Malware threats. Malware, in fact covers a whole lot of nasty territory that includes viruses, info-stealing keyloggers, fast flux Botnets, Trojans, Zero-day exploits. Having said that, last years (2010) breach in security, which involved the disruption of Iran's nuclear power plant goes on to show the rate at which threats are evolving. However, the discovery of Stuxnet and the TDL4 virus will help security experts and IT administrators get a better outlook on their existing security. at said unknown T and end users. and

enhanced functionality makes it the most prefered These new breed of exploits prove tricky as they constantly change form, launch multiple and different attacks, and more recently, the Stuxnet Trojan/virus and Conficker worm offers insight into global threats and trends, shaping the outlook for IT security.

With their ever increasing skills, cyber criminals are beginning to stay one step ahead of security professionals by combining old-school methods that exploit Windows vulnerabilities with new complex approaches, resulting in increased difficulty in detecting attacks and negligence on the part of IT security operations to protect corporate assets.

Though exciting, but with its growing popularity, cloud computing and virtualization also leads to the next possible target of cyber criminals. Recently, cyber criminals steered the registration process to get access to Amazon's S3 accounts by registering their AWS account using stolen credit cards and personal information. According to the researchers, a number of domains on Amazon's cloud platform that were being used to install malware as part of spam and phishing campaigns were designed to steal banking credentials and other sensitive data. Not only these, but the endpoints of networks have widened with the use of portable computing and storage devices like Smartphones, Netbooks, iPods etc. Hence the risk of data leakage has also increased.

To be on the safer side, computer users should make sure to use a multi-layered Anti-Virus solution that comes with an intrusion detection & protection system (IDS/IPS), firewall protection, end point security management, Zero-day protection, etc.

Q.
Why should people buy eScan Internet Security – instead of other "similar" products on the marked?

There are many reasons as to why one would prefer eScan amongst the other security products available in the market. eScan is equipped with the revolutionary **MicroWorld Winsock Layer (MWL) Technology** that detects information security threats at the Windows
socket layer itself, before it reaches the Application Layer to prevent the applications from getting infected.

eScan has one of the fastest automatic updating system against new and emerging threats while it counters unknown threats using advanced **Behavioral Analysis** to provide protection from Zero Day threats.

eScan also provides options for system administrators to remotely administer a vast network using the newly implemented **eScan Management Console (WMC)**. WMC also allows administrators to remotely install eScan, deploy upgrades, updates and enforce Integrated Security Policies for the entire Enterprise network.

eScan also facilitates endpoint Security with **Device Management** (USBs and CD/DVD ROMs), network outbreak prevention, live alerts and reports to the administrator. It also reports about the outbreaks on the networks and helps administrators manage Critical Hotfixes released by eScan and Microsoft to ensure that all the clients in the network are updated with the latest patches.

eScan's **enhanced Firewall**, on both Server and Client, monitors and logs all incoming and outgoing traffic according to the policy defined by the administrator. In addition, eScan provides sophisticated file blocking & folder protection along with an enhanced on-demand scanner.

eScan effectively prevents data theft and Virus infections via USB and Fire wire-based devices. It includes **Application Control Module**, which allows you to block or permit applications from running on networks and stand-alone computers.

eScan's exclusive and advanced **Anti-Virus Toolkit (MWAV)** is a FREE, intelligent and powerful Anti-Virus utility that enables fast and hassle-free scanning of computers without the need to install and can be run directly from anywhere, on your computer, USB Drive or from a CD ROM. This makes eScan, the most preferred software amongst IT users.

Taking the above mentioned aspects into consideration, our products not only help in securing your digital identity, but also prevent known and unknown malware from infecting systems. With that said, its overall ease of use and enhanced functionality makes it the most preferred software amongst IT and end users.

eScan Internet Security in use :

If you wish to buy 'e Scan antivirus/internet security, please click this link :

www.escanav.com