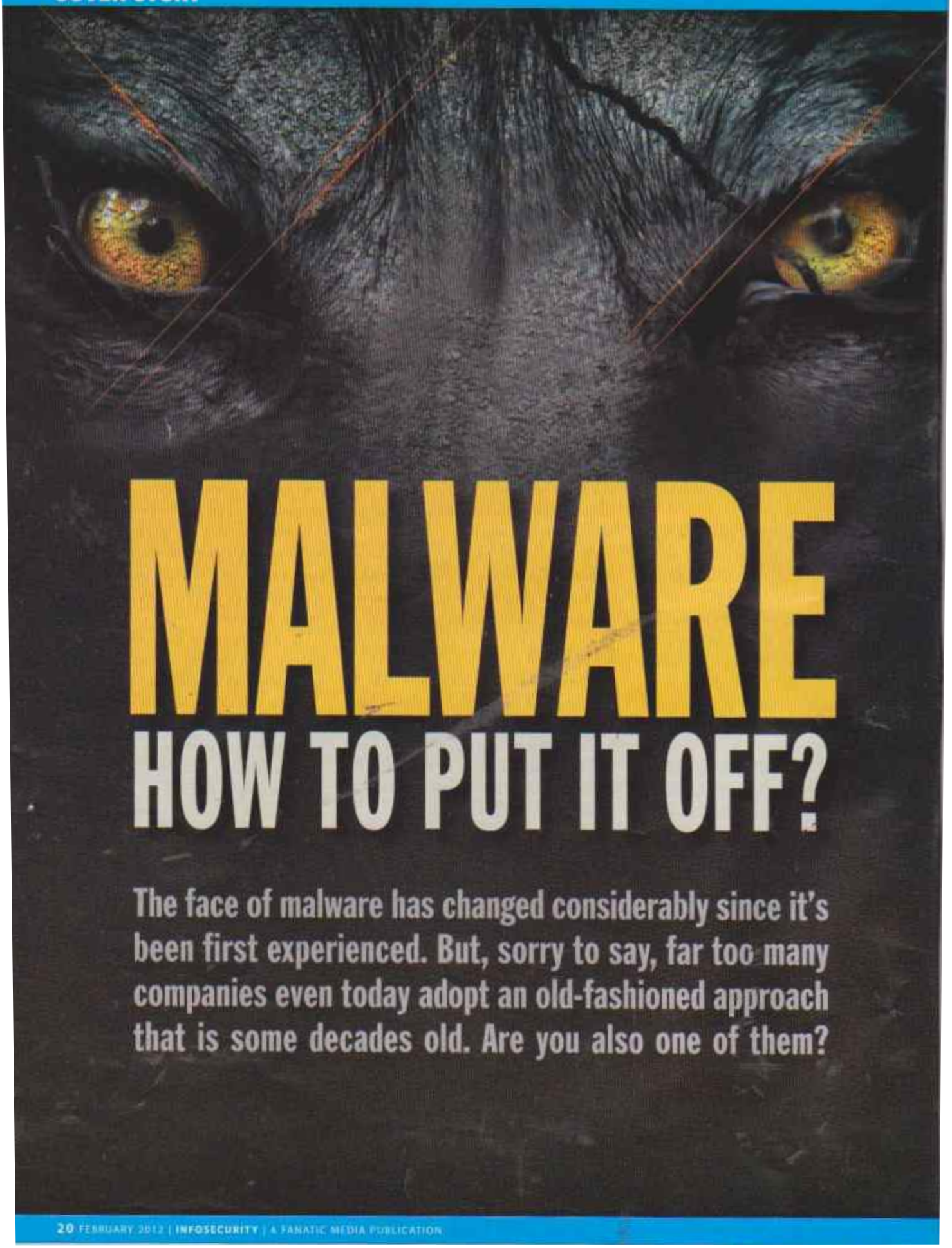


MALWARE
HOW TO PUT IT OFF?

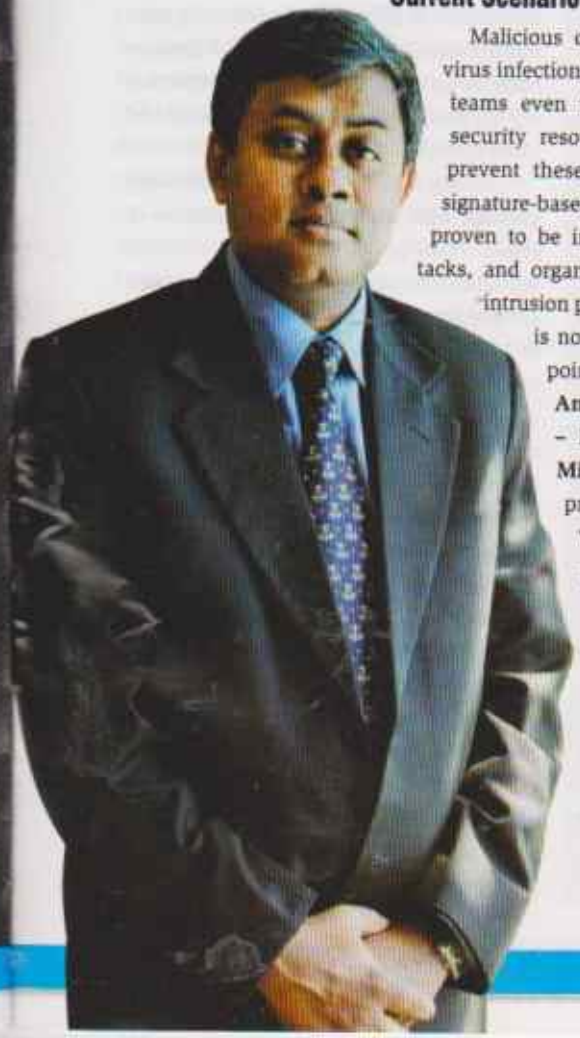
The face of malware has changed considerably since it's been first experienced. But, sorry to say, far too many companies even today adopt an old-fashioned approach that is some decades old. Are you also one of them?

The countenance of malware has come a long way, particularly in the last decade. It has evolved tremendously from the time when the early computer viruses were first brought in. At the moment, it advances so fast that a lot of users, who come across it, nearly find it hard to keep up with the latest threat. Security experts have already warned that in excess of 280 million viruses were hurled, only during the previous year.

If the sudden increase in malware variants wasn't sufficient, sophisticated Advanced Persistent Threats (APTs) catch victims in ways that are completely beyond conventional security traps. A recent research suggests that in so far as 75 per cent of new malware is noticed on a particular endpoint and barely about 40 per cent of today's innovative malware gets perceived at all.

It's not an issue of whether your network will be hit by an advanced malware or not, but the greater issue is how you will respond to any such attack. Advanced malware is somehow showing the way how security should be managed.

Current Scenario



Malicious code infections, malware and virus infections continue to frustrate security teams even though significant enterprise security resources have been devoted to prevent these very infections. Traditional signature-based anti-virus approaches have proven to be ineffective against modern attacks, and organisations that have tried host intrusion prevention find that technology is not an effective part of the endpoint security solution, anymore. **Amit Nath Country Manager – India and SAARC at Trend Micro** rightly comments on the present-day problem, by saying, "Protection is needed not only against known attacks but also against new and unexpected threats."

On a similar line, **Altaf Halde, Managing Director at Kaspersky Lab – South Asia** expects to see threats like, "mobile malware and mobile espionage" eating up the greater part of a security budget and brains of the security professionals. He also considers "consumerisation of technology", as a dangerous trend and something rife with risks. He assumes the "number of targeted attacks" to grow significantly in the times to come. The tendency of attackers to "steal others money" would be the main driver for carrying out any attacks. Above and beyond he foresees, "Multiple attacks on various government institutions and businesses will be carried out across the world."

Amit Nath, Country Manager, India and SAARC, Trend Micro

On corporate and government level, specific malware designed to attack specific targets as famous Stuxnet did last year is likely to become more sophisticated. Right now, we're seeing Duqu worm, an offspring of Stuxnet, and **Pankaj Jain, Director of ESET India** believes, "In all probability, we will be seeing more of this kind of threat in the years to follow."

Talking of the latest Win32/Ramnit.A virus, he expresses concern for a lot of people, "who are disposed to using pirated software on their systems, downloading cracks and key-gens from untrustworthy Web-sites, are most vulnerable for it." It is a virus spread through the Internet and via removable drives. It infects .dll and .exe files and also searches .html files and opens a back door that compromises a computer. Using the backdoor, a remote attacker can access and instruct the infected computer to download and execute more malicious files. In this context, he informs, "For last several month this virus was on the top of cyber threats in India, according to ESET ThreatSense.Net, a cloud-based reputation technology." Another most common malware in India, he quotes was, "INF/Autorun (uses autorun.inf file as a way to compromise a computer) and Win32/Sality.NBA (a virus which infects executable files)".

More than 40% of all infected systems in India are affected by worms and Trojans. Potentially unwanted applications (PUA) are also a big challenge for Indian users. At the same time a dangerous worm, he informs, "Win32/Conficker is elsewhere predominant, but surprisingly ESET researchers didn't see this worm being that active in India."

Other than malware, users have to be responsive of scams and other social engineering tricks on social networks and in spam E-mails. "Social engineering and search poisoning are very successful in India, due to the lack of cyber security awareness, I guess," says Jain.

India has been named as top-spam-sending country. Jain says, "In 2011 India continued to be on the top of the rank as about 15-17% of world's spam was coming

from India, while Brazil, China, Vietnam followed." He adds, "In 2010 more than 700,000 IP addresses globally were infected with Rustock bot-net and the majority of them in India. The bot-net was believed to send out as many as 40 billion spam E-mails per day." He presents logic, by saying, "Even after cleaning most of infected machines the amount of spam did not become less," and expects to see more bot-nets in and from India, in coming years.

Considering that many computers, especially in India, are not protected with any anti-virus software, they become an easy target for the bad guys. Penetrating into the system, they can easily make it a part of bot-net consisting of thousands or even millions of other compromised computers, controlled from the bot-net's command and control centre. Bot-nets are used to steal bank data, E-mails and perform such cyber attacks as spam, DDOS, phishing, click fraud, adware and malicious programs' distribution. All these are the source of hackers' income.

This year we expect to see more arrests of cyber criminals globally in conjunction with the takedown of bot-nets, but the number of bot-nets being created will not drop. Some of these bot-nets will be used for political purposes and some will be based on mobile devices.

Another emerging trend is mobile malware. "Today, there are five billion mobile devices in the world, one out of four of which is a smart-phone with the ability to connect to the Internet and access E-mails (personal or corporate), social networks, e-Commerce Web-sites, Home Banking, etc.", articulates Jain.

Android OS with its 43% market share has been the focus of attention from malware developers for mobile devices for some time. "In 2011 ESET researchers identified 41 major malicious codes (and variations) for Android platform, starting with the emergence of FakePlayer, the first Trojan for Android. Our findings of this analysis indicate that 30% of threats in 2011 were made available for download in the Android Market, 37% of those are SMS Trojans and 60% of the malicious codes have some botnet characteristic," speaks Jain.

In 2011, we've seen SMS Trojans and other malware that allowed the attacker to gain remote access to and control of the device, which, once infected, becomes a zombie. For example 'Zeus', first appeared in 2007 for desktop computers and now is available for all four OS for mobile devices. The malicious programs of the rogue type, that is, fake security software, have also appeared for Android platform. Another mobile malware appeared in 2011 is DroidDrea which had main objective of stealing info mation that allows an attacker to identify t infected device and install other maliciou code. "More than 2.5 lacs downloads of th threat from Android Market were reporte in 2011," tells Jain. This attack had such a impact that Google decided to uninstall th application remotely from all the infecte systems and the users who were infecte were notified by E-mails.

Altaf Halde, MD, Kaspersky Lab – South Asia

Cyber-criminals diversified their target to include new platforms, as business us of mobile devices accelerated. And we sa a number of politically motivated "hack tivist" groups take the media spotlight even as the more common threats to ou cyber security grew. "Cyber-criminals ar becoming more professionalised throug the availability of commercial crime-war kits like the increasingly popular Black-hol kit," adds **Pratapaditya Mondal, Regional Manager at Satcom Infotech.** The resul is mass generation of new malicious code and exploits, and a significant increase in the volume of malware. In the coming year businesses will be challenged to manage these threats alongside new ways of access ing applications and data, like mobile and cloud services.

Taking a stride forward **Govind Rammurthy, CEO and Managing Director of eScan** sums it up and says, "Currently virtualisation and cloud-based platform are the top most concerns." The increase in consumerisation and mobility has led to increasing complex and mobile security threats. Network up-time and data protection are currently major issues faced by all the segments. Advanced persistent threats (APTs) and automated 'drive-by' attacks against high-profile companies and government agencies have become more predominant increasing data theft and financial loss. Threats, like Stuxnet and Duqu, which are specifically designed for data extrusion are an alarming danger to businesses. In addition, enterprises are having hard time dealing with insider threats and the risks associated with insider breaches. Apart from this, entirely new series of cyber attacks have been introduced for emerging social

media applications. In addition, smartphones that contain huge amount of data and are constantly connected to the Internet, are luring cyber-criminals.

Quest for Comprehensive Security

Consideration of comprehensive security schemes involves multiple capabilities. The basic capabilities are protection, detection and response. Anti-virus products are often overlooked, considered to be commodities and automatically renewed annually. This results in the quality of detection and response capabilities also being overlooked. These are imperative elements in the security strategy.

The focus of many organisations is shifting to newer security technologies, such as DLP, Encryption Technologies, etc. Halde maintains, "While these newer technologies are helpful, yet the overall number of malware incidents and infections continues to grow." An IDC survey found that 46 percent of organisations experienced an increase in malware incidents, while only 16 percent experienced a decrease. The SMB environment had the most dramatic differentiation, with 44 percent seeing an increase in malware and only 7 percent seeing a decrease. That means malware is still slipping through these enhanced prevention measures, demonstrating that increased emphasis must be paid to detection and response capabilities. Halde locates, "IT departments have invested in protection mechanisms at the gateway, yet open up wide doors for employees to surf the Web without the proper detection mechanisms in place to ensure that cyber-criminals are detected and effectively blocked." Because cyber-criminals today target the endpoint, robust detection and response technology needs to be deployed at the endpoint to protect it from malware designed by cyber-criminals to steal data, credentials and revenues.

Even so, quite evident that it takes more than just an anti-virus to keep today's advanced threats off. Protecting corporate assets requires a complete security solution that includes anti-malware, host-based intrusion prevention system (HIPS), Web protection, patch assessment, application and device control, network access control, data loss prevention, firewall and other capabilities. In addition to complete protection you need a solution that's easy to install and manage, and that can grow with your needs—saving you time and ensuring comprehensive protection for years to come. Mondal summerises by saying, "In short, you need an advanced endpoint protection solution." More advanced endpoint solutions, according to him should "also include cloud-based protection, device and application control, patch assessment, Web productivity filtering, network access control, data loss prevention and full-disk encryption." Even if you don't expressly need these advanced capabilities today, he takes his point ahead and says, "your organisation

Pankaj Jain, Director, ESET India

PandaLabs' Annual Security Report 2011

Panda Security's antimalware laboratory (PandaLab) has recently released its Annual Security Report 2011, which declared the year 2011 as a year, which had witnessed ample of data thievery, hits on social networks and intense cyber warfare. According to the report, malware creation went to a new high during the year with twenty six million new species were recorded in circulation, nearly 30 per cent of all malware that has ever existed and been noticed by the company.

The statistics exemplifies the sheer capacity of cyber-criminals to mechanise the formation of new variants of malware, further corroborated by the average number of new threats created and released every day increasing from 63,000 by 16 per cent, in the year. The company employs Collective Intelligence, a cloud-based system, to detect, analyse and classify most of the malware received, leaving only half a per cent of them to be dealt with manually. In November 2011, the company announced that Collective Intelligence had processed more than 200 million files. So, they analyse a huge number of files, to start with.

In 2011, Trojans subjugated the threat view above all. Whereas in 2010 Trojans made up 56 per cent of all malware, the percentage jumped up by 25 per cent. Thailand, China and Taiwan were found to be the top three countries that generated infectious traffic.

In the year only, Sony suffered a substantial data breach that exposed data belonging to a hundred million users. This is supposed to be the biggest security ever estimated and recorded. In this year only, the Steam video game service, being brought into play by around 35 million people, was also compromised by hackers.

Social networking sites also become a lowly hanging bunch of flowers to pluck, for money-hungry cyber-criminals. Even though more than 25 million users registered on Google+, only in a matter of first few weeks, it is still far away from its direct competitor, Facebook and Twitter, which makes it less of a target for cyber-crooks.

Cyber-war also stole headlines in the year, 2011. The total number of cyber-attacks burgeoned world-wide, bothering governments all over.

will likely need them tomorrow, given the increasing complexity of security threats."

Therefore, for a comprehensive security, one should opt for an all in one security application to protect from all the known and unknown sophisticated attacks. According to Nath, "The key features one should look for in an anti-malware software are anti-virus, anti-spyware, Web threat protection, data theft prevention, system tuner, social networking security, parental controls, smart-phone protection and secure erase." While Rammurthy prescribes, "An ideal anti-malware should have capabilities like, proactive / heuristic detection and mitigation of malicious scripts, flash files scanning and purification, iframe injection detection, URL / Domain reputation tracking and anti-phishing feature."

Pratapaditya Mondal, Regional Manager, Satcom Infotech

Bringing the Indian perspective in, Jain says, "I understand how difficult it is for Indian users, both home users and corporate, to choose an anti-malware vendor." Understanding which features are really going to help in protecting your system and which of them sound more "marketing-oriented" than technically helpful is a difficult task. Jain adds, "From my point of view, users have to pay attention to the scanning and malware removal technology, ability to scan and manage removable media, the availability of firewall and spam filters, if the user depends on Internet surfing and emailing. Such features as Parental Control, Gamer mode or special social media features are useful and nice, but always additional."

Protecting the system by comparing incoming code to a list of "known bad code" (your updated signature database) is the basic strategy of almost every antivirus product. He goes further by saying, "While the alternative one, which is used by ESET, is heuristic detection, that is, identifying code as potentially malicious based on everything that malware experts know about current and future malware." The fact though holds water that well-written heuristic detection systems have a good track record of preventing infections by previously unknown malware, even malware that seeks to exploit zero-day vulnerabilities.

Set of Propositions

Today, cyber-criminals act with even more persistency and sophistication, as the world shifts from the desktop computers towards mobile and cloud computing devices. Nath puts it this way, "The need of the hour is a next generation content security infrastructure that will deliver smarter security to in-the-cloud applications, data-centres, delivery systems and endpoints."

Halde belives, "These days, clients are spending disproportionate time and money reinforcing the datacentre perimetre with technologies such as authentication, access management, firewalls, network intrusion prevention, etc. We are not saying any of these technologies aren't important. They definitely are. But, we need to concentra on where our data currently resides; o on the endpoint. The endpoint represen a more immediate threat to data loss." H refers current "IDC data" in this contex which "shows mobility is the number o factor driving new security spending" Th data suggests that more organisations a taking heed and beefing up security mea ures beyond their datacentre perimetres.

Employees are equipped with the devic of their choice instead of a device that optimised for managed anti-malware, an theft and privacy technologies. The result an expanding variety of devices, operatin systems, carriers, security profiles, and othe technologies within the business networ Consumerisation is well there, unstoppab and increasingly demanding on the securi front. Yet, IT departments treat a laptop a a glass bottle of Coke. When a device is lo or stolen, the insurance claim only conside the value of the empty bottle, ignoring a the valuable data that was contained with the device. Because of that, the protectio schemes on mobile devices usually addres the value of the device, instead of considerin the value of the data. The fact is that mo often the value of the data on the devic exceeds the value of the devices itself, ofte hundreds of times over. Use of managed ant malware, anti-theft and privacy technologie for mobile device is a good start to addres protecting mobile data.

Let's talk about Social Networks now This is the new "must have" technolog that segments of business are demandin for growth. When properly used, it can hel tremendously. A formal policy to control th access and management of social media i essential. For example, if a company protect its perimeter against malware attacks bu lacks adequate control for social network ac cess, one employee's carelessness could lea to malware infecting the company networ and causing significant economic losses either directly or indirectly. Social network are also a possible means for informatio leaks by employees who voluntarily shar information with third parties.

Talking of the latest offering of Kasper sky Lab Halde says, "Kaspersky Endpoin

Security 8 for Windows is designed to provide organisations with deeper protection and more flexible and comprehensive controls, whether it is application, device or Web control capabilities." This is of course a topping over their traditional offerings.

Rammurthy submits his proposal by saying, "eScan range of products are powered by futuristic and innovative technologies as well as sophisticated Anti-Virus Heuristics Algorithms. It provides Zero-Day Protection against malware, hacking, phishing and spam to both servers and endpoints." Mondal promotes Sophos products by saying, "To counter the malware threat, Sophos uses proactive detection technologies." Explaining, he says, "In the last six months of 2011, 80 per cent of the unique malware seen by our customers (over 5.5 million different files) was detected by just 93 proactive detections." Truly, ideal proactive detections are designed to detect not just the millions of existing malware, but future malware before it is even been created. It is always better to be proactive than reactive, responding to threats individually as they emerge.

ESET, according to Jain, targets both enterprise and home consumer segments, offering a diverse product line of security solutions. He talks of NOD32, anti-virus and anti-spyware for protection online and offline, Smart Security, an advanced product with integrated anti-malware and spyware scanner, a two-way firewall and intelligent anti-spam to eliminate all types of security threats. He proposes of Cybersecurity for MAC OS X users, which shuts down all attack vectors, neutralising threats designed to attack Windows or Linux systems, along with emerging exploits against the Mac platform – to keep the sensitive data and identity protected around the clock. He also informs about ESET Mobile Security, which is as the name suggests specially designed for Windows Mobile, Symbian and Android smartphones and tablets. The solution detects the most sophisticated mobile malware. He claims that the solution protects the smart-phones against multiple types of junk SMS, Trojan installers, a host of viruses, spyware, adware, rootkit infections, worms and other unidentified malicious mobile software. All information coming via Wi-Fi, Bluetooth or Infrared is scanned to protect user's phone from emerging exploits, data loss, and SMS spam. For SMB segment he proposes Business Security Packs for 5, 10 or 25 users. "This suite provide comprehensive round-the clock protection of small companies' endpoints, file and mail servers and mobile devices as well," claims Jain. Talking of their enterprise-class products, he says, "Apart from end-point security offered by us, we offer Remote Administrator to simplify management of computers in the network, File security, Mail security, Gateway security for Microsoft Exchange Server, Linux / BSD / Solaris and Kerio."

Tall Claims

Performance measures how a security solution impacts user experience and the number of help desk calls. Ideally, users won't experience slowdown when a security solution is scanning their system; during scheduled scans, at boot up or when opening a file. This should still be the case on a loaded or low-memory system. Strong security performance can improve IT efficiency and end-user productivity. Mondal claims, "Several independent tests found Sophos had high scan speeds for both on-access and on-demand scans, did well in low-memory situations." He adds, "We give customers everything they need to stop malware and protect data in one console and agent. Get fast, effective and complete security for users, wherever they are. It's easy-to-install, manage and use—saving time and money. And, it is all one license along with unlimited 24/7 support, free security updates, software upgrades, home use and more without stretching our customer's budget." When asked about real-time response for online protection, he said that Sophos End Point Security Solution uses live, cloud-based protection to check suspicious files against their database, stopping malware before it run.

Adding, he says, "Also we put web malware scanning and inappropriate site filtering in our end point agent." This is with the intention to give Web protection anywhere, while keeping a check over Web gateway costs. Making a special mention of their Data Protection Module, he says, "It is one of the most effective features in our endpoint solution, which helps our customers to control critical data flow in and out of their IT Infrastructure comprising managed and sometimes unmanaged endpoints."

Halde makes a claim like, "At Kaspersky Lab, we have earned quite a reputation for rapid and comprehensive malware detection, as well as small, frequent signature updates. Traditionally, we have small disk and memory usage, and we have further improved on this feature in our new offering." In the same context, he tells about an option named, "don't run full scan on battery power." He adds, "Kaspersky has tightly-integrated code architecture. We haven't acquired other technologies and forced

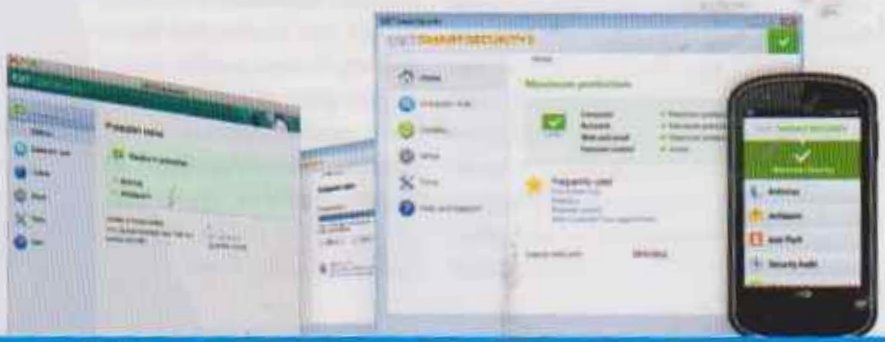
Govind Rammurthy, CEO and MD, eScan

them into our solutions but built them from scratch, making our solutions light-weight, agile, easy to deploy and ahead of new threats." Talking of endpoint platforms that their products support, he names, "Windows Server 2008, Windows 7 Workstations, Citrix, Linux, Novell NetWare, Microsoft Exchange, LotusNotes/Domino, Windows Mobile, BlackBerry, Android, and Symbian, as well as MicrosoftForefront Threat Management Gateway and EMC Celerra."

As per him, "The cloud-based Kaspersky Security Network (KSN) is always alert to malicious programs and behaviours, constantly watching over users protected by our technology. Because of its advanced threat detection capabilities, KSN immediately knows if any attempt is made to infect any computer. In less than 40 seconds, millions of KSN participants are alerted to the new threat and get protected." Mentioning some of the striking features in their products, he says, "Our solution provides effective tools to control compliance with policies on application, device and Web usage level. Application Startup Control, Administrator-based Whitelisting, Application Privilege Control, Vulnerability Scanning, Device Control are Web Control and Content Filtering are just a few to name, in this context."

Talking of speed versus performance aspect, Nath says, "Our anti-malware security includes parental controls, a system tuner, data theft prevention, automatic updates, a government-level file shredder, and 2 GB of online storage boosting the speed and performance aspects." Adding on, he says, "It also consist a highly effective detection system which further moves detection to the cloud making it run with less interference in the system." Talking about Smart Protection Network infrastructure, he says, "Our cloud-computing security technology, products and services stop threats where they emerge, on the Internet and are supported by 1,000+ threat intelligence experts around the globe." To tackle online threats they have cloud-based services to offer. On the same line, he carries on to say, "We use real-time threat data to block advanced persistent threats, targeted attacks, malicious links, and compromised Web-sites, before they reach the Web, E-mail, IM, collaboration systems, and network perimetre. Protection for the outbound data at vulnerable points throughout the network is facilitated with messaging security content filtering and E-mail encryption solutions." He adds, "Our InterScan Web security solution offers Web gateway protection which defends against advanced Internet threats, while application visibility helps manage the risks inherent in cloud-based consumer applications being accessed in the workplace. Its instant visibility provides on-the-spot risk management." Confronting a query about phishing protection software, he says, "We offer a comprehensive approach to stop identity theft and protect confidential corporate information, by filtering messaging traffic, stopping fraudulent, phishing-related E-mails at the messaging gateway and mail servers. Credit card and bank account numbers, user names, and passwords are also included in our security protection domain."

Similarly, Jain also claims, "ESET is known for being very light on system" and cites a few independent tests where their solutions performed competitively. He explains, "The latest ESET products, ESET Smart Security 5 and ESET NOD32 Antivirus 5, offer various new and improved features including ESET Live Grid (former ThreatSense.Net), cloud-based reputation and protection technology, New Removable Media Control, aimed to secure users from viruses and malware that spread though removable media affecting computers without the need for internet access. This tool automatically prompts the user to scan the content of all flash drives (USB, SD), firewire, CDs and DVDs, so that specific threats can be blocked from trying to get into the system through the media devices. Parental Control (in ESET Smart Security 5 only) allows blocking Websites with potentially offensive material. Advanced Host Intrusion Prevention System (HIPS) implemented in 5th generation of ESET products allows tech savvy users to customise the behavior of the whole system and its each part. User can define rules for system registry, processes, applications and files. The tool can be used to block unauthorised changes to programs. Gamer Mode that switches to silent mode and disables pop ups to conserve system resources and enhance the gaming experience." Talking about the real-time detection and removal of malware, he says, "ESET products focus on real-time detection of malware utilising advanced heuristics to help protect the users from different kinds of malware." Being based on ThreatSense.NET technology these solutions automatically collect data from worldwide user base of the company and immediately sends feedback on new threats trapped by the heuristics to their Threat Lab. This information is immediately incorporated into new updates, as the company finds it necessary to do. This also helps reducing false positives, tremendously, as per his claims. He adds, "Apart from signature updates, ESET uses heuristic detection, i.e., identifies code as potentially malicious based on everything that malware experts know about current and future malware." Their Heuristics Engine enables detection of malware not even specified in the signature database. The primary advantage of the heuristic-based model is not only its ability to detect variants or modified forms of existing malicious programs, but also new previously-unknown malicious programs. Jain highlights the feature called "Remote Administrator," which comes free of cost with the Business Edition of Smart Security and NOD32 and says, "It is an application which allows you to manage our products in a networked environment. It



is a solution which allows you to administer these products – including workstations and servers – from one central location. The built-in task management system enables timely responses to malware incidents. Update signature databases, run reports, and enforce consistent security policies with ease across your entire network."

Facing the question of speed versus performance Rammurthy responds, "eScan's Whitelisting Technology facilitates the system administrator to allow users to only have access to certain listed applications." When this feature is enabled, all other applications other than the ones mentioned in the list will be blocked. Hence, known good applications can be whitelisted by mentioning their paths. He explains, "This will not only reduce unnecessary bandwidth usage within the network, but also result in faster scans without affecting the systems performance. eScan also has one of the lowest memory-footprints, hence does not affect the performance of the system."

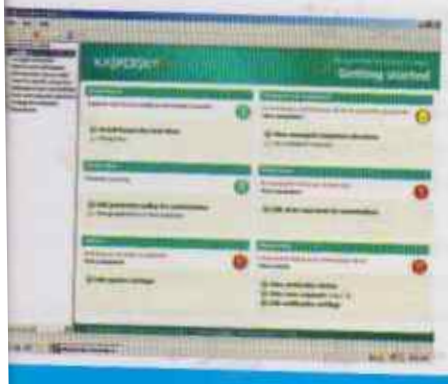
"We provides Multi-level protection against the ever growing information security threats, claims Rammurthy. It is equipped with MicroWorld Winsock Layer (MWL) Technology that detects information security threats at the Windows socket layer itself, before it reaches Application Layer to prevent applications from being infected. He adds, "We have one of the fastest automatic updating systems against new and emerging threats, while it counters unknown threats using advanced Behavioral Analysis to provide protection from zero day threats. It also facilitates system administrators to remotely administer a vast network using the management console (WMC) that also allows remotely installing our software, deploying upgrades; updates and enforce integrated security policies for the entire enterprise network." The two-way Firewall with predefined rule sets at the client monitors and logs all incoming and outgoing traffic according to the policy defined for the client. Rammurthy says, "Our Secure Web Interface encrypts all communications between the server and the clients effectively preventing man in the middle attacks." "In addition," he says, "our solution automatically prevents spreading of malware infection on networks and can sending alerts to the administrator about the outbreaks on the networks. It can also instantaneously display live alerts about applications, USB / flash devices and site browsing information of the clients."

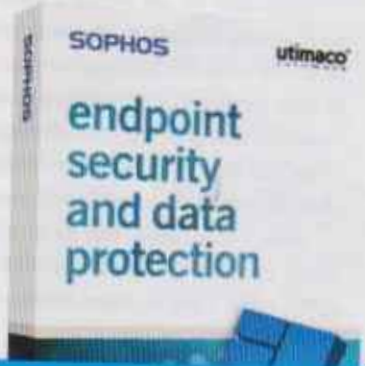
"We provide real-time automatic updates every 2 hours," informs Rammurthy. This keeps the anti-virus software updated to deal with the new malware that are continuously released. This also helps in proactively protecting against zero-day threats. He adds, "Our Self Protection Technology prevents new generation malware from either disabling eScan or deleting its critical files. With such instant detection of viruses, eScan assures that the system is constantly monitored for malware and experiences the highest level of protection." In addition, it also scans content for confidential data, prohibited information, offensive, and obscene language. He further stresses on the fact, "The features of our solution include anti-phishing, anti-spyware and anti-rootkit." It facilitates USB Control, Application Control, User-based Parental Control, Folder and File Security along with Web Protection that includes Virtual Keyboard. He adds, "Our Web Phishing Filter warns the users of phishing web-sites. Our Anti-Spam and Content Scanning modules prevent infected E-mails and attachments from reaching your inbox" This helps protect a computer from malicious programs that propagate through E-mails. It enables you to create and configure filters that filter spam based on keywords and phrases that appear within E-mails. He goes on and says, "Our Auto Back-up and Restore utility takes back-up of all the frequently used files (PE files) and stores it in an encrypted form. If an infection is detected, Auto Back-up and Restore utility restores all the clean files in real-time without the need to format the system. The solution also includes a Malware URL filter that protects endpoints against drive-by malware downloads as socially engineered malware attacks pose one of the largest risks to individuals and organisations."

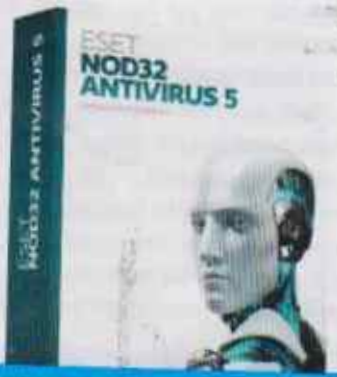
Killer Features

Nowadays, as company's sensitive data are more on fly due to the business needs and consumerisation of technology, so corporate IT is always under pressure to secure their critical data from getting leaked and compromised from the endpoints either knowingly or unknowingly. Mondal says, "Here Sophos' unique and simple approach to data loss prevention integrates the scanning for sensitive information into the antivirus engine on the endpoint, lets you watch for the transfer of sensitive data, such as personally identifiable information (PII) or company confidential documents." By that you can reduce the risks of data accidentally saved to a removable storage device or sent out of the organisation, without keeping your employees from going about their daily tasks.

Nath speaking about their latest offering Titanium says, "It utilises less than half the disk space and memory as it moves detec-







tion to the cloud which supports up to 2GB of online storing." According to him, "It is simple, easy to use software to protect data from outside threats."

One of the newest features in ESET 5th version products says Jain is, "Host Intrusion Prevention System (HIPS)". With this feature user can customise the behavior of the system in greater detail: specify rules for the system registry, active processes and programs, set permissions for applications and fine-tune your security posture. User can lock any application from accessing the core system files such as the registry and other system processes so that unwanted applications cannot access sensitive files without the administrator's consent. User can also allow applications to delete a file or even modify the system startup settings. So in short, HIPS protects the system from malware or any unwanted activity attempting to negatively affect the security of the computer. It utilises advanced behavioral analysis coupled with the detection capabilities of network filter to monitor running processes, files and registry keys, actively blocking and preventing any such attempts.

With the increasing cyber crime, malware writers are continuously releasing new malware. Hence, every computer user demands a comprehensive security solution that prevents confidential data as well as excellent system performance. Home users today face a threat landscape that involves stealthy, targeted, and financially motivated. USB / flash drive is one of the most successful computer interfaces in the history of the personal computer. All desktop or notebook computers manufactured today support this feature which replaced the parallel and serial ports. These devices can be easily brought in and out of office areas, and they can be "silently" inserted into, receive data from and then removed from a workstation with absolutely no record of the actions taken. "With eScan Endpoint Security, data theft and virus infections via USB or Firewire-based portable storage devices can be effectively prevented," says Rammurthy. It prevents data theft by blocking all but your trusted USB storage devices and stops your files from walking away on thumb drives, iPod, mp3 players and portable USB hard drives.

Halde says, "We rely on providing deeper protection through one of the best anti-malware solutions, by maximising usage of security cloud with Kaspersky Security Network, improving manageability and providing flexibility into application, device and Web control."

Try it to Taste it!

"Trial versions are available for all the four products under Kaspersky Open Space Security, that is, Work Space Security, Business Space Security, Enterprise Space Security and Total Space Security," tells Halde. He adds, "Similarly trials are also available under Targeted Security for Anti-spam, Security for Mail Servers, and Security for Internet Gateway and Anti-virus for Storage (EMC Celerra). He also provides the link, where these trial versions could be found—http://www.kaspersky.com/downloads/trials/#tab=tab-3.

Nath soliciting sales queries at toll free number 1800-103-6778 reveals the link—http://www.trendmicro.co.in/in/homeandhomeoffice/index.html, where a 30-day-trial of Trend Micro Titanium Maximum Security 2012 could be found.

Mondal says that Satcom Infotech is National Master Distributor of Sophos (http://www.sophos.com/en-us/products/endpoint/endpoint-protection.aspx) in India and divulges their contact details, as info@satcominfotech.com and +91-22-67911040.

Jain puts it simply by revealing just the link where all ESET trial versions are available—http://esetindia.com/download/antivirus. Similarly, Rammurthy tells the link upfront—http://escanav.com/english/content/products/MWAV/escan_download.asp.

Making a Choice

With time we are seeing a surge in the sheer volume of data a typical security vendor must deal with. Not only has the total volume of data increased with times, but also the volume of malicious data. Security experts estimate that more than 280 million viruses were released, during the previous year alone.

Even worse, these threats of today are highly momentary. As a matter of fact, just about three forth of these threats have a lifetime as short as null, which means that they are seen the very first as well as the last time on an endpoint, simultaneously. The amount of data under threat during any of the occurred incidences of theft is inflating enormously, with no signs of abating in the foreseeable future.

Collaboration is the key and an anti-malware built on this principle would prevail henceforth. Advanced threats require a more collaborative approach to deal with them. Rather than operating autonomously, different protection technologies should form a tightly integrated system and work in tandem. These technologies should amalgamate natively and operate in concert to reach a final disposition of whether a picky file or application presents or represents a threat.

Then it is of value to have a broader view-point. Don't just think of an endpoint, it is in fact a question of all endpoints and thus make it a question for all of them, to carve out the correct answer. Therefore think collectively, while thinking of how to tackle advanced malware.

Then, you should know your threat landscape. Parts that form the threat landscape of an organisation include its size, the value of its information assets, its outline or credit within the industry, and the vulnerabilities lying within its computing system. For example, a tiny business that offers sweets in a particular locality has different information security implications than a multi-national company that fabricates sensitive technologies for a government. So as to battle against advanced malware, you should know where and how your valuable data resides and how to build a castle around it. You should not rely exclusively on your anti-malware vendor to develop protection against new attacks, without having done your home-work.

It's almost firm, as of now, that detection is no longer enough. Today, the best-of-the-breed solutions also include technologies that help you hurriedly counter an almost inevitable outbreak; technologies that can help you answer critical questions like: where did it initiate, how did it multiply, can it be restricted and so on... ●

—By: Manu Priyam, InfoSecurity Bureau.