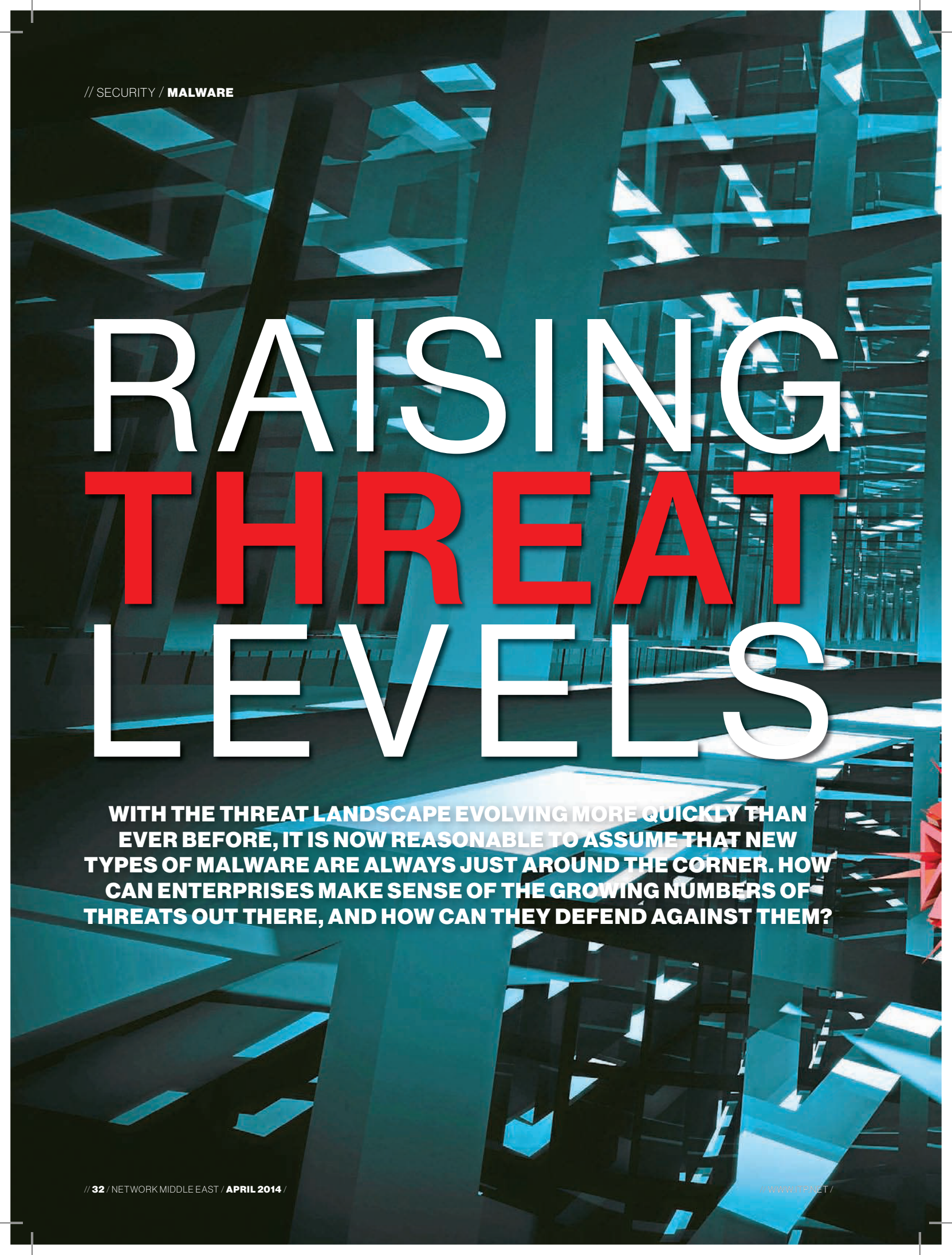
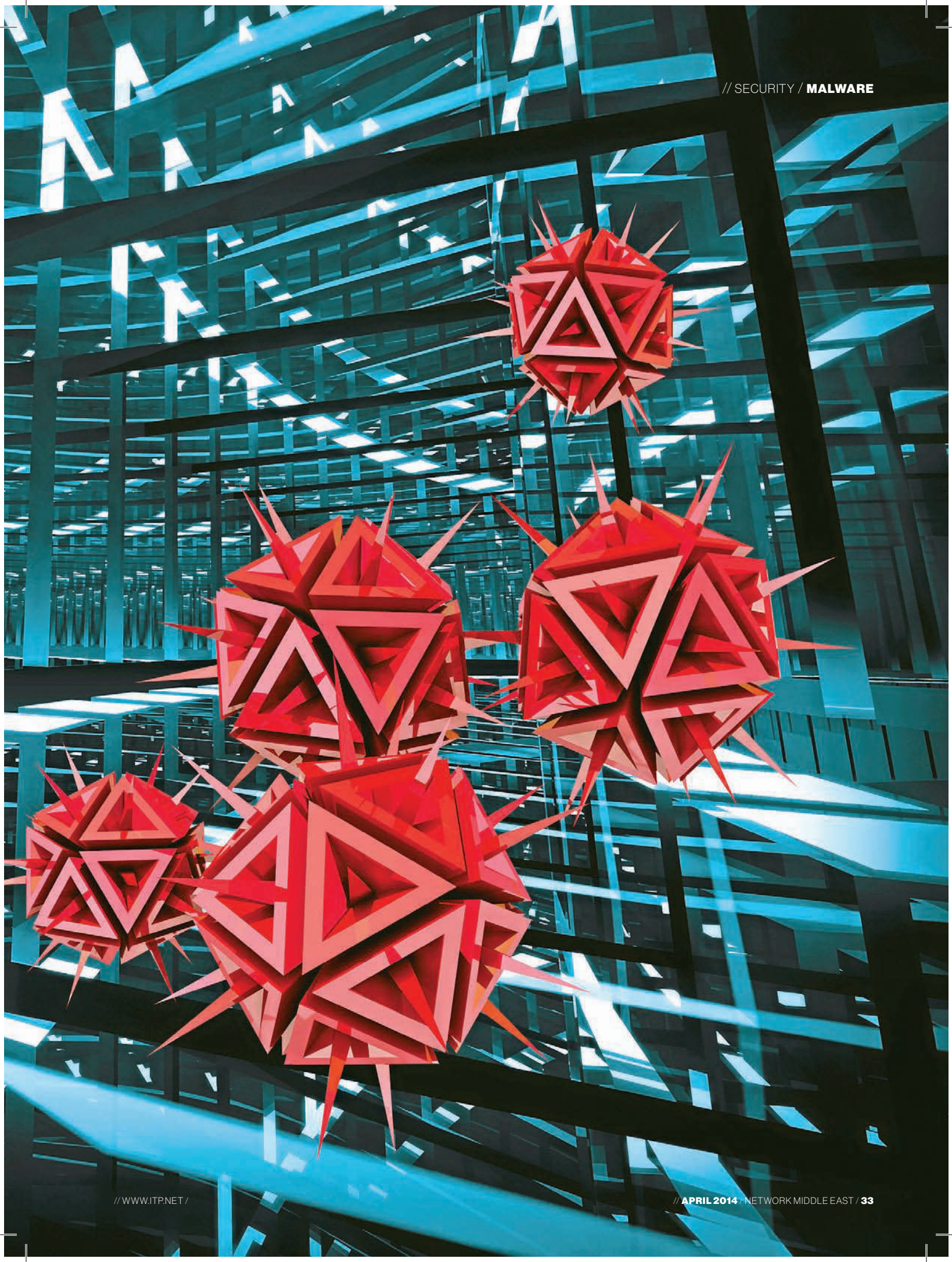


RAISING THREAT LEVELS

WITH THE THREAT LANDSCAPE EVOLVING MORE QUICKLY THAN EVER BEFORE, IT IS NOW REASONABLE TO ASSUME THAT NEW TYPES OF MALWARE ARE ALWAYS JUST AROUND THE CORNER. HOW CAN ENTERPRISES MAKE SENSE OF THE GROWING NUMBERS OF THREATS OUT THERE, AND HOW CAN THEY DEFEND AGAINST THEM?



In March this year, researchers from ESET, CERT-Bund, the Swedish National Infrastructure for Computing, and a number of other agencies, uncovered a widespread cyber-criminal campaign that had seized control of over 25,000 Unix servers worldwide. The attack, dubbed Operation Windigo, resulted in infected servers sending out millions of spam emails, which would then infect computers and then steal information from them.

The Windigo campaign had been running for over two years, totally undetected. And its discovery provided the most recent evidence that, despite the industry's best efforts, we are largely in the dark as to what tricks cyber-criminals are going to pull next. Big discoveries like the Windigo one come along regularly, of course, but if each campaign manages to run for such a long time undetected, it stands to reason that the cyber-criminal underworld has much more up its sleeve.

And this is particularly true when it comes to malware. The big security vendors play a vital role in hiring researchers to scope out the security landscape. But it takes these people time to find new strings of malware, which are created on a daily basis, meaning that the next new piece of dangerous software is always just around the corner.

"Malware families tend to peak, or see maximum infection rates, for short periods of time, during which security solution vendors play catch-up," says Manish Bhardwaj, marketing manager at Aruba Networks.

According to the McAfee Labs Q4 2013 Report, there were over 2.3 million new malicious signed applications during the fourth quarter of 2013 — a 52% increase from the previous quarter. During the year, McAfee Labs found 200 new malware samples every minute, or more than three new threats every second. With statistics such as these as your backing, it is fair to say that cyber-criminals are endeavouring to stay one step ahead.

"Given that polymorphism — i.e. the ability of malware to dynamically create different forms of itself — is a popular tactic used by malware writers to help circumvent security signatures, even traditional forms of malware can periodically slip through undetected and then pose a challenge to enterprise security," says Bhardwaj.

But this does not mean that attempting to understand the threat landscape is futile. Indeed, security experts advise obtaining as much knowledge as possible about the evolving nature of various types of malware, as this knowledge can go a long way in not only setting up good defences, but also in working out what cyber-criminals might come up with next. And some believe that IT professionals in the Middle East should pay particular attention to the threat landscape.

"The MENA region is a major target for malware and cyber-threats. The region suffers all the normal malware infections — Trojans, worms, botnets, and viruses — that affect the rest of the world, but also seems to suffer a higher infection rate than other regions. For instance, according to the latest regional statistics from Microsoft, Middle East countries outpace other countries for the highest percentage of infected machines, and Egypt seems to lead the region in infected machines. A growing economy combined with less cyber-regulation and adoption of cyber-security technologies probably contributes to the increased infection rate in MENA," says Surender Bishnoi, WatchGuard's regional manager for the MEA region.

"Besides suffering from normal cyber-threats, the MENA region also is the target of higher-than-average amounts of industrial and government cyber-espionage. MENA has been the victim of many advanced persistent threat (APT) campaigns that seem to originate from other nation states, such as Duqu, Flame, Gauss, Mahdi, and the infamous Stuxnet. Some of the most advanced cyber-attacks seen in history are targeting organisations in MENA."

ADVANCING THE ART

Indeed, the state-sponsored malware argument is hammered home by a number of other experts. Ali Joseph, general manager of RadarServices Middle East, says that nation states in the region aim to steal valuable information for companies in their home country. What's more, he warns, state-sponsored organisations have the resources and know-how to develop very sophisticated malware.

Even in the cyber-criminal underworld, sophistication is the order of the day. According to Ray Kafity, FireEye's regional director for the Middle East, threat agents have increased the sophistication of both their attacks and their tools.

"Upgraded and more sophisticated versions of traditional malware have certainly given us enough to worry about in 2013 and have caused harmful financial losses. Hackers are being inspired by older malware and are developing new versions in order to create more sophisticated attacks that are hard to fight," he says.

"The region suffers all the normal malware infections — Trojans, worms, botnets, and viruses — that affect the rest of the world, but also seems to suffer a higher infection rate than other regions."

Aruba's Bhardwaj: Malware families tend to peak for short periods of time, during which security solution vendors play catch-up.

As well as creating more robust and complex pieces of malware, with added capabilities, cyber-criminals are also looking to become stealthier with their creations. While not a new term, the advanced persistent threat (APT) made big headlines during 2013, thanks largely to security researchers discovering more variants that actively work to evade detection.

"Even after successfully accomplishing the mission, the APT continues to live on to gather additional information. Defending against the stealthy and persistent nature of APTs is a complex undertaking, and requires a coordinated approach on the systems as well as the network level," says Kafity.

Perhaps the biggest advancement on the malware scene over the past 12 months was the CryptoLocker ransomware, which locks users out of certain files and folders and demands a ransom be paid to unlock it. Experts have branded it as one of the most threatening pieces of malware of 2013.

OLD SOFTWARE, NEW TRICKS

Malware such as Trojans and viruses these days make up just a fraction of a cyber-criminal's inventory. Indeed, many seek to get into corporate networks through vulnerabilities in popular software, such as Java or Adobe PDF Viewer. And though these vulnerabilities are regularly found and patched, the majority of businesses are running on outdated software that could potentially expose them to risk.

"As part of Trend Micro's yearly predictions report, we have outlined few of the major possible threat vectors, such as widely used systems and software in organisations [that have gone] out of support — such as Windows XP and Java 6," says Tony Zabaneh, a senior sales engineer at Trend Micro Middle East.

Indeed, the so-called 'zero-day' attack grabbed headlines across the world last year, with researchers discovering that cyber-criminals had been exploiting vulnerabilities in soft-

Expert advice

"Malicious software such as viruses, worms, Trojans, spyware and adware still play havoc and can have a profound negative impact on any IT environment. Increasingly, this type of intrusion is becoming harder to detect if you don't have the right tools and expertise to design an antimalware solution that will most effectively protect your IT environment."
— Anas Ali Al Naqbi, senior security consultant, eHosting DataFort

"In this Generation Y era, where social media is so important and most employers daren't stop their employees from accessing it during the working day – we have seen the attackers take advantage of this and use these sites as command and control channels for their new breed of malware, or to use them as mechanisms to silently extract the information that is the focus of their attack."
— Sean Newman, field product manager, SourceFire

"Clearly cybercriminals are putting a substantial amount of effort into churning out hundreds of thousands of new malware variants daily in the hopes that some of them will be successfully implanted on a target devices. 2013 was a bumper crop for malware targeting mobile devices."
— Guillaume Lovet, senior manager of Fortinet's EMEA threat response team

"All too often, organisations are not even aware that they have suffered an APT attack in the first place. This is because they lack the proper monitoring systems and security mechanisms to detect these attacks. It is also good for organisations to know that the number one infection vector for APTs is through spear-phishing emails."
— Pradeesh VS, general manager, ESET Middle East

> "Hackers are being inspired by older malware and are developing new versions in order to create more sophisticated attacks that are hard to fight."

WatchGuard's Surender Bishnoi believes that, due to the high infection rate in the Middle East, enterprises here are at greater risk than in other parts of the world.

Ray Kafity, FireEye, says that defending against advanced persistent threats has become a complex undertaking.

ware before any problems had been found by software creators. According to Florian Malecki, EMEA product and solutions director at Dell SonicWall, a number of notable zero-day attacks affected users around the world during 2013.

"In 2013 there were 14 reported zero-day vulnerabilities. Browser-based attacks lead the list with Java being the number-one targeted application, followed closely by Internet Explorer, and Adobe Flash Player. Other notable zero-days targeted Adobe Reader and the Windows operating system," he says.

And with Microsoft discontinuing support for Windows XP this month, security researchers predict that zero-day attacks are only set to increase. Some experts believe that cybercriminals are even stockpiling their vulnerability exploits for use after the support cut-off date of April 8. After all, with the venerable operating system still commanding a worldwide market share of 29.53%, according to netmarketshare.com, there will soon be a healthy chunk of vulnerable computers open to hackers once Microsoft stops providing support.

HOW TO TACKLE THE THREATS

As companies move towards third-platform computing that incorporates elements of cloud and mobility, experts warn that IT managers have forgotten about the basics of security. To combat the ever-growing threat landscape, then, it is advisable to re-visit some of those basics.

"In the late 1990s and early 2000s, we all accepted we needed anti-virus and content filtering. However, in the mid-2000s, the cloud exploded and the way we interact and access data changed. Now, most companies are accessing data from different places and mediums with no anti-virus, control and detection mechanisms. So, from a hacker's point of view, it's easy pickings. They are doing the same old attacks, but in a different way and with slightly different tools," says Sebastien Pavie, SafeNet's regional sales director for the MEA region.

"Another security mistake companies are making is failing to encrypt their data. We have heard countless stories over the past year of devastating attacks and data breaches, yet if this data had been encrypted in the first place then all hackers would have found is scrambled information, rendering the theft pointless. The problem is that too many companies shy away from encryption due to fear that it will be either too expensive or complicated, however the reality is that it doesn't have to be either."

> "Besides suffering from normal cyber-threats, the MENA region is also the target of higher-than-average amounts of industrial and government cyber-espionage."