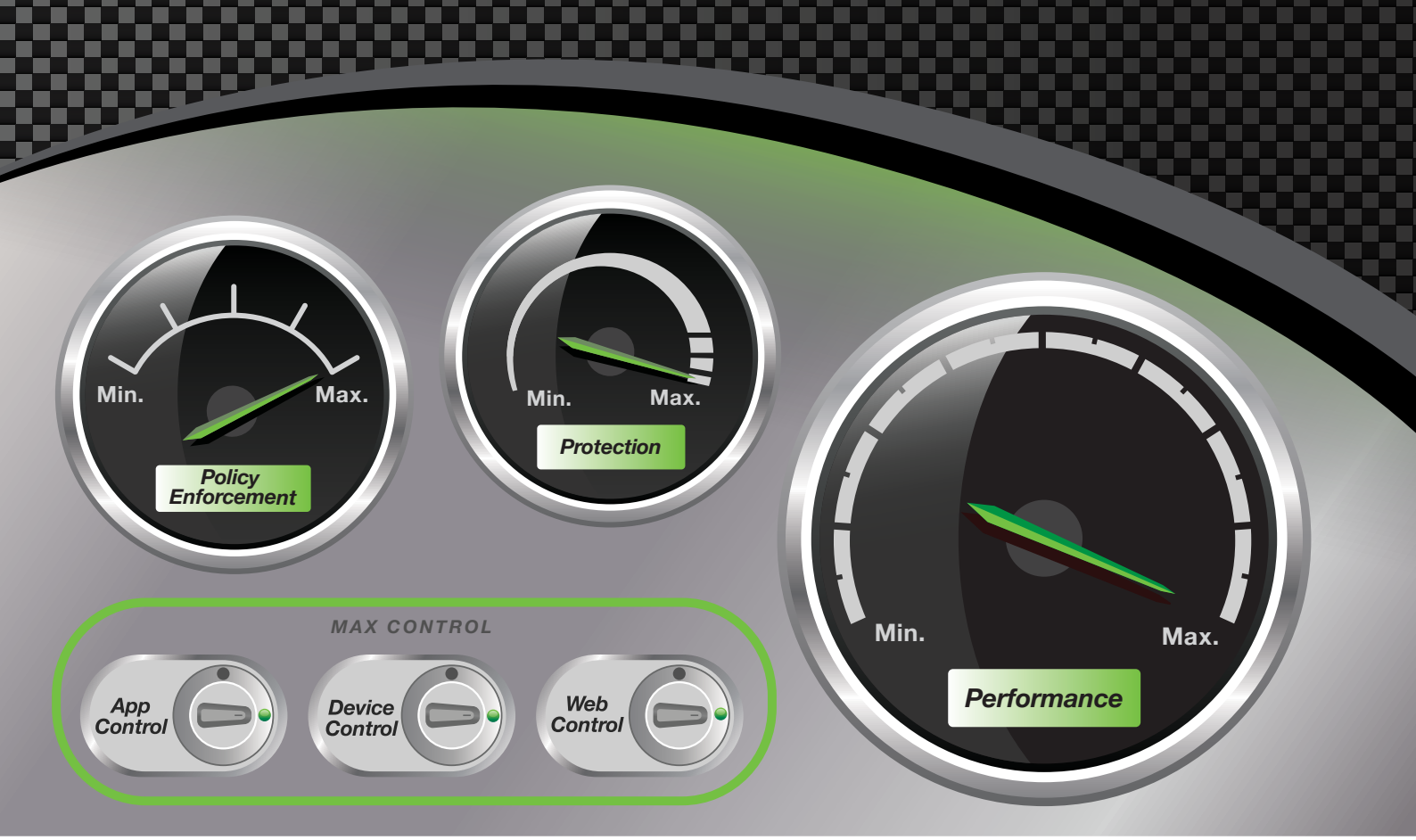

Advanced persistent threats: not your average malware

Your business may not be the target, but you're still at risk

kaspersky.com/beready

KASPERSKY lab

Introduction

1.0

“

ADVANCED PERSISTENT THREATS AND ZERO-DAY ATTACKS ARE PERVASIVE AND UNRELENTING AND THEY ARE FORCING MID-MARKET ORGANISATIONS TO QUESTION THE CURRENT SECURITY PARADIGM.

A truism in information security is that every user and every device face the same malware threats. Over the years, malware has evolved from nuisances that disrupt operations and destroy data to tools of criminal theft, corporate espionage and state-sponsored warfare.

The problem is only getting worse as endpoint devices become increasingly mobile and operate outside the control of corporate security. This risk is paramount, as seen in the evolving class of malware used in connection with ‘advanced persistent threats’ (APTs) that stealthily infiltrate networks, in many cases, by tagging along with endpoints and portable media.

A good example of these emerging threats is ‘Flame’, the weaponised worm that attacked the Iranian energy sector and is now spreading throughout the Middle East. Discovered by Kaspersky Lab, Flame[1] is being called ‘one of the most complex threats ever discovered’. While targeted at Iran’s nuclear efforts, Flame has security experts worried about the virus spreading beyond its intended target and infecting corporate systems around the world.

Before Flame, there was Stuxnet, which was specifically designed to infect and disrupt the SCADA (supervisory control and data acquisition) systems controlling Iran’s uranium enrichment centrifuges. The malware proved exceedingly successful at causing the machinery to operate uncontrollably and head towards self-destruction. Unfortunately, Stuxnet migrated beyond the Iranian targets and started infecting SCADA systems in Germany and, ultimately, other parts of the world.

Both Flame and Stuxnet are APTs, weapons of a new generation of warfare powered by governments, terrorists and well-funded cybercrime syndicates. Equipped with a host of stealth capabilities, they are programmed to focus on intellectual property, military blueprints and other valuable corporate assets. However, the casualties of this war will likely be mid-market and small enterprises, which will be caught in the cross-fire if they don’t develop a comprehensive security infrastructure to lock down their endpoints.

The days when mid-market and enterprise companies could enjoy a relatively anonymous status, or skimp a little on their security posture, have come to an end. APTs and zero-day attacks are pervasive and unrelenting and they are forcing mid-market organisations to question the current security paradigm and change their approach to network and data defences. Network security is important, but the humble endpoint cannot be overlooked.

Enterprises have a plethora of security options, such as Kaspersky Lab’s full pallet of anti-virus and endpoint security solutions, which can comprehensively prepare them for today’s most malicious threats, as well as the looming and increasing dangerous attacks of an uncertain future.

In this whitepaper, we will review the growing number of APTs and zero-day threats against endpoints; the security options available to mid-market and enterprise users; and how Kaspersky Endpoint Security 8 provides superior protection against routine and advanced malware threats.

[1] Securelist, May 2012

APTs: Not Your Average Malware

2.0

CYBERCRIMINALS EMPLOY MALWARE TO HUNT AND PHISH FOR HIGHLY PERSONALISED INFORMATION THAT TARGETS INDIVIDUALS, WHICH IS THEN USED AS PART OF A SECOND-STAGE ATTACK.

Once, security threats were delivered in bulk, typically via email. The victim would be enticed with a phishing message purporting to be from an overseas financier or a long lost relative. While potentially harmful, these threats were indiscriminant, fairly easy to detect and preventable with a basic security infrastructure.

These kinds of attacks are still prevalent, but lately, threats have been elevated to the status of APTs and zero-day attacks, and are now terms used to create fear, sensation and drama.

In the last few years, the list of the most notorious APT attacks has defied the imaginations of even the most creative scriptwriters:

- **Google's Operation Aurora:** In 2009, this attack, traced to China, exploited Windows' Internet Explorer vulnerabilities to obtain source code and other intellectual property from Google and around 30 other global corporations.
- **RSA:** This attack, which compromised the security company's flagship SecurID tokens, enabled cybercriminals to infiltrate U.S. military contractors Lockheed Martin, Northrop Grumman and L3 Communications in 2011.
- **Oakridge National Laboratories:** The Department of Energy lab was forced to go offline when administrators discovered sensitive data being siphoned off a server via a phishing attack.
- **GhostNet:** This cyber espionage network of 1,295 infected hosts in 103 countries was aimed at a list of Tibetan supporters and other high-value targets, including local ministries, foreign affairs commissions, embassies, international organisations and non-government organisations (NGOs).
- **ShadyRat:** This high-profile hacking campaign included governments, non-profits and global corporations, with 70 victims in 14 countries.

These days, APTs and zero-day exploits go hand-in-hand and enjoy a prolific presence in the media. Yet, what exactly are they, and how do they differ from any other ordinary Trojan or worm?

It's safe to say these are not your average 'teenage-hacker' attacks. Like their name suggests, APTs rely on advanced technology as well as multiple methods and vectors to target specific organisations to obtain sensitive or classified information.

Unlike the 'script-kiddie' launching SQL injection attacks – or your average malware author renting botnets to the highest bidder – APT masterminds tend to be highly organised syndicates with teams of experts and multiple intelligence-gathering techniques at their fingertips. With stealth capabilities and a 'low-and-slow' attack method to stay under the radar, the APT becomes the tool of choice for cyberspies, hostile governments, terrorists and profit-driven cybercrime syndicates.

“

ONCE IN, THE APT EMPLOYS ANY NUMBER OF SOPHISTICATED TROJANS, WORMS AND OTHER MALWARE TO INFECT THE NETWORK.

Here’s how it typically happens:

With an APT, cybercriminals target individuals by employing malware to hunt and phish for highly personalised information, which is then used as part of a second-stage attack. From there, the APT relies on individualised social-engineering techniques to infiltrate an organisation via its ‘Achilles heel’: the end-user.

During this attack phase, the APT targets a handful of key individuals with known access to the targeted accounts, reeling them in with convincing emails that appear to come from HR or a trusted source. With one careless click, the cybercriminals have free access to an organisation’s most precious information without anyone being aware.

Once in, the APT employs any number of sophisticated Trojans, worms and other malware to infect the network and establish multiple backdoors on systems that will likely remain on desktops and servers indefinitely. During that time, the threat moves undetected from one host to the next with protracted stealth that enables it to hunt for its assigned target.

Attack Target: Zero-Day Exploits

3.0

2011 ENDED WITH NO LESS THAN 535 DATA BREACHES INVOLVING THE LOSS OF 30.4 MILLION RECORDS.

The 'tools-of-choice' for APTs are, unfailingly, zero-day exploits. These aptly named threats take advantage of security vulnerabilities in software before the vendor has time to address them or even realise they exist – indicating a window of zero days between the first attack and the fix. The result is tantamount to a cybercrime free-for-all. Without fear of reprisal, cybercriminals reap the benefits of executing an attack for which there is no known cure.

Malware that targets zero-day vulnerabilities can silently wreak havoc on an organisation, homing in on its proprietary information, such as source code, intellectual property, military blueprints, defence data and other government secrets used in espionage activities. As the attack unravels, the fallout is nothing short of a PR nightmare, costing organisations millions in damages related to everything from security infrastructure overhauls to litigation costs and customer attrition – not to mention the untold costs needed to rebuild reputation and regain consumer confidence.

APTs and zero-day exploits are nothing new and were first executed years ago, way before these terms became part of the security vernacular. Many organisations still don't realise they've been hit with a zero-day APT attack until months or years later – according to a Verizon data breach report[2], 44 percent of data breaches involving intellectual property take years or longer to discover.

Case in point: A Christian Science Monitor[3] report detailed that three oil companies – ExxonMobil, Marathon Oil and ConocoPhilips – where victims of targeted APT cyber-attacks that dated back to 2008. During the attacks, which were thought to be sourced from China, cybercriminals funneled critical industry information on the quantity, value, and location of oil discoveries worldwide to a remote server. But these companies only discovered the attacks when the FBI informed them their proprietary information had been stolen.

By 2011, APTs had taken their place as the big new threat in the security food chain. APTs were responsible for some of the biggest losses that year, which included high-profile attacks on Sony, Epsilon, HBGary and DigiNotar, as well as RSA's loss of approximately 40 million one-time password (OTP) token seed files. All told, RSA's[4] breach cost the company an estimated $66 million, while Sony's[5] 100-million-record loss in its first breach cost an estimated $170 million.

2011 ended with no less than 535 data breaches involving the loss of 30.4 million records, many of which were due to some of the year's most sensational attacks, according to the Privacy Rights Clearinghouse[6]. These are only a fraction of the known breaches as there are thousands of security breaches that go unreported or undiscovered each year.

[2] Verizon 2012 Data Breach Investigations Report, March 2012
[3] U.S Oil Industry Hit By Attacks—Was China Involved? - Mark Clayton, Christian Science Monitor, 25th January 2012
[4] RSA SecureID Breach Cost $66 Million - Matthew J. Schwartz, InformationWeek, 28th July 2011
[5] Sony Network Breach to Cost Company $170 million - Adam Rosenberg, Digital Trends, 23rd May 2011
[6] Data Breaches: A Year in Review - Privacy Rights Clearinghouse

Arming the Enterprise against APTs

4.0

“

END-USERS SHOULD BE FAR FROM THE ONLY LINE OF DEFENCE, MAKING THE IMPLEMENTATION OF ROBUST INFORMATION SECURITY INFRASTRUCTURE VITAL TO THE SAFETY OF AN ORGANISATION’S DATA.

But could 2012 be even worse? Research suggests it can…

With last year’s epic breaches setting a strong precedent, future generations must prepare themselves for waves of increasingly malicious threats perpetrated by foreign agencies, hostile governments, political hacktivists and unscrupulous companies illicitly stealing secrets. Global events such as the Olympics Games, continued unrest in the Middle East and economic instability in Europe could set the stage for such attacks.

Depending on who you ask, the rise of state-sponsored hacking is either an imminent threat or a horrifyingly monstrous problem. According to the Asia Times,[7] the Congressional United States-China Economic and Security Review Commission (USCC) recently shared similar concerns when the director of the Cyber-Statecraft Initiative for the Atlantic Council said the Chinese threat was so big our military cyber-defences has called it “the biggest transfer of wealth through theft and piracy in the history of mankind.”

In light of their insidious and ever-expanding global presence, APTs clearly spell trouble. As military contractors and high-profile enterprises continue to gain awareness and bolster defences, mid-sized and small enterprise companies become the next logical step for targeted attacks. Often, these market sectors possess a deadly combination: all the confidential information of large enterprise and government agencies – with the security defences of a SMB.

However, where they differ is with a comparatively reduced IT budget and lack of dedicated IT security staff that could protect them from the increasingly treacherous security landscape. Add to that a lack of security awareness stemming from a misguided perception about their anonymity, and the mid-market is primed as a big APT target. Considering that hackers were able to dig deep into Lockheed Martin’s network before being discovered, the threat against mid-market and relatively smaller enterprises is paramount.

Faced with the daunting – if not downright terrifying – APT threat on the horizon, it may seem that mid-market and small enterprise segments have few weapons in their arsenal. This is far from the truth.

Many mid-market attacks can be mitigated or stopped with regular user education and training. Best security practices such as avoiding clicking on attachments and PDFs from unknown or unsolicited sources, double-checking suspicious emails and regularly changing passwords should be applied frequently. Best of all, the cost of upfront prevention is a fraction of what organisations would have to spend on the backend conducting remediation and damage control after an attack has occurred – an attractive ROI for the budget-conscious mid-market.

That said end-users should be far from the only line of defence, making the implementation of robust information security infrastructure vital to the safety of an organisation’s data.

Security expert Bruce Schneier said it best: In conventional malware attacks, “Security against this sort of attacker is relative; as long as you’re more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it’s an attacker who - for whatever reason - wants to attack you. Against this sort of attacker, the absolute level of your security is what’s important. It doesn’t matter how secure you are compared to your peers; all that matters is whether you’re secure enough to keep him out.” [8]

[7] Washington Sweats At China’s Cyber Threat - Benjamin Shobert, Asia Times, 29th March 2012
[8] Advanced Persistent Threats - Schneier On Security, Bruce Schneier 9th November 2011

First and Best Step: Secure the Endpoint

5.0

FOR THOSE WHO THINK EMAIL IS AN ANTIQUATED VECTOR: THINK AGAIN. MOST APTS INVOLVE SOCIAL ENGINEERING DELIVERED OVER EMAIL OR INSTANT MESSAGING (IM).

The mid-market must improve its defences to mitigate the increasingly menacing APT threat. Standard firewalls and IDS technology are not enough to block evasive and sophisticated targeted attacks.

Complicating matters, many of these technologies are not adequately monitored or updated, lulling end-user organisations into a false sense of security, while giving a free pass to the APT operators. As a bare minimum, mid-market companies need to have a strong endpoint security agent that incorporates anti-virus, application control, device control and web control.

Most APTs rely on little-known, or unknown, zero-day vulnerabilities to gain entry. Enterprises need an endpoint security solution that incorporates reputation-based technology to screen for suspicious behaviours, and detect and eliminate those yet-undetectable threats. These reputation filters will also alert users when they are surfing compromised and suspicious websites that could contaminate them with malware.

Kaspersky Endpoint Security 8 combines all of these features required to block APTs at every turn. The solution combines bleeding-edge **anti-malware** protection with data-centric controls, such as **Application Control, Device Control and Web Filtering** technologies, along with customisable whitelisting / blacklisting capabilities to limit applications. Heuristic technologies alert the user to unknown threats, and, if necessary, can take immediate action to eradicate the attack and restore damaged data.

Meanwhile for those who think email is an antiquated threat vector: Think again. Most APTs involve social engineering delivered over email or instant messaging (IM). Essential in Kaspersky Endpoint Security 8 is its secure electronics feature, which is compatible with the most common email programmes, scanning files and links sent via IM systems. In addition, the solution contains anti-phishing technologies, including a list of phishing URLs updated in real time by the Kaspersky Security Network (KSN).

Additionally fortifying the email gateway is Kaspersky Anti-virus Security for Mail Servers, which protects groupware servers and all popular mail servers – including Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim – from malicious programmes and spam. The solution scans of all incoming and outgoing messages and attachments, filters the messages by attachment type, and sweeps them with anti-virus on Exchange, helping the end-user to ward off APT phishing attacks.

But few, if any, APTs stop at the endpoint – and an organisation's anti-malware solution shouldn't either. Anti-malware should without fail be extended to all components of the network, including file servers, workstations and mobile platforms.

Further safeguarding the mid-market is Kaspersky Security for File Servers, which provides on-access, scheduled and on-demand scanning of all key system components while detecting, removing and blocking malicious software and infected objects.

KASPERSKY ENDPOINT SECURITY 8 PROVIDES THE FUNCTIONALITY, MANAGEABILITY AND SECURITY THAT MEETS ENTERPRISE PROTECTION AND BUDGET NEEDS.

Because APTs can gain entry through any workstation, **Kaspersky Anti-Virus for Workstations** provides protection against all types of cyber threats, including viruses, spyware and hacker attacks on all remote and desktop workstations. Powering the solution is a vulnerability and threat scanner that continuously monitors all incoming and outgoing files and data streams, including email, internet traffic and network communication, for malicious content with real-time, on-access and in-depth scanning.

A few years ago, APTs needed to go no further than the Windows platform to achieve their objectives – but those days are over. The recent outbreak of malware targeting the Mac OS X platform have upended Mac users and left them increasingly susceptible to the same types of APT attacks as their Windows-counterparts. Earlier this year, the Flashback Trojan circulated amongst shocked Mac users, infecting more than 748,000 computers by the end of April 2012.[9]

Kaspersky Endpoint Security for Mac offers all the same protections against threats like Flashback and the imminently rising numbers of Mac malware with a powerful anti-virus engine, heuristic-scanning technology and optimised CPU usage, along with remote deployment, detection management, quarantine and backup storage capabilities. Meanwhile, the anti-virus engine behind Kaspersky Anti-Virus for Workstations is capable of detecting, quarantining and removing malware on most Linux operating systems.

Visibility is key. Technologies that provide complete visibility and reporting capabilities and give administrators the ability to assess the organisation's entire IT environment and security posture, historical data and security events will be crucial in the line of defence. That holistic window needs to extend beyond the endpoint or workstation to servers, virtualization and mobile platforms.

Tying it all together is **Kaspersky Security Center 9**, which provides a comprehensive suite of administration tools that can do just that: manage an array of threat protection applications, set up and schedule policies, integrate with Cisco NAC and Microsoft NAP solutions and regulate mobile devices. Nothing guarantees absolute protection against malware infections, especially as APTs become more powerful and pervasive. The goal of any security program should be the mitigation of security threats with as much ease and as low a cost as possible.

Security suites such as **Kaspersky Endpoint Security 8** and its complementary products provide the functionality, manageability and security that meet enterprise protection and budget needs.

[9] The Anatomy Of Flashflake, Part II, Securelist, Sergey Golovanov, 24th May, 2012

About Kaspersky Lab

With the increase in sophisticated malware, use of potentially malicious applications and employees bringing their own devices to work, it's even harder to manage all the potential IT security threats within your business.

With **Kaspersky Endpoint Security 8**, you set the rules, you control applications, web and device usage. If it's happening in your business, Kaspersky can help you see, manage and protect it.

You're in control. You're in the driver's seat.

Be Ready for What's Next
kaspersky.com/beready