KASPERSKY lab

THE POWER
OF PROTECTION

FUTURE RISKS: BE PREPARED

Special Report on Mitigation Strategies for Advanced Threats

kaspersky.com

CONTENTS

ADVANCED PERSISTENT THREATS AND THE THREAT LANDSCAPE

Cybersecurity is anything but a numbers game. When it only takes a single breach to inflict serious damage on your business, defending against the majority of attacks isn't enough.

That's why it's best to focus our attention on the most dangerous threats we face, rather than those we face most often.

The "ecosystem" of malware breaks down into **known** threats (70%), **unknown** threats (29%) and **advanced** threats (1%).

Known threats, accounting for about 70% of malware, are relatively easy to defend against. As long as we recognize the malicious code we can block it: traditional signature-based methods typically cope with this.

A further 29% of malware comes under the banner of 'unknown threats'. Fighting these requires more sophisticated tools. Methods that go beyond standard antivirus software – such as heuristics and dynamic whitelisting – can combat these, too.

Then there's the remaining 1%. Advanced threats are multi-faceted, continuous and targeted attacks. Designed to penetrate a network, lurk unseen and collect sensitive data, once in place, they can remain undetected for years.

An Advanced Persistant Threat (APT) known as "Darkhotel" used the WiFi in luxury hotels to steal data from guests for seven years before being discovered. This was a particularly interesting APT as it was highly targeted (focusing on senior executives and CEOs) and vividly illustrated the IT security challenge presented when endpoints (company laptops and tablets) leave the security of the company network.

An APT known as "Darkhotel" used the WiFi in luxury hotels to steal data from guests for seven years before being discovered.

Though some extremely high-profile organzations have fallen victim to APTs, you don't need to be in the public eye to be in the sights of cybercriminals. Enterprises must be able to mitigate the risk posed by APTs and the consequences that could ensue from an attack – whether that's data loss, extensive downtime or serious reputational damage. And with APTs typically operating silently and stealthily, prevention is far less costly than remediation after an attack (as the attack could have happened some time ago and done untold damage over months or even years).

There is no one solution to this problem. Though useful, the technologies we use to fight known and unknown threats aren't adequate to fight APTs on their own. An increasingly sophisticated and complex threat landscape calls for a multi-layered security approach, in which a combination of integrated technologies provides comprehensive detection and protection against known, unknown and advanced malware and other threats.

This report is designed to help you to be better prepared to fight APTs.

The average cost of a malware incident is $56,000 for a small to mid-sized business and $649,000 a large enterprise organization.[1]

APTs can have huge consequences. During 2014, Kaspersky Lab helped uncover the workings of Carbanak. This complex attack allowed an international group of criminals to steal $1B from a range of financial institutions. Having infected a bank's network, the group was able to record everything that happened on the screens of employees and learn how to transfer money without being detected.

[1] The high cost of a security breach, Kaspersky Lab.

ENTERPRISE IS A TARGET – 5 KEY POINTS

As a large enterprise, you're aware of the IT security threats you face. These threats are only getting more targeted and more sophisticated.

1 The first step to creating an appropriate strategy for dealing with APTs is to understand that you're a potential target. The truth is – whether it's intellectual property, contact details or financial information – your organization holds information that criminals could profit from. Even if it's not your data that they're after, they can use your network as a way to get to your partners or customers (as was the case with Darkhotel).

2 Secondly, we need to develop greater vulnerability awareness. In organizations where large numbers of employees are working across a number of devices, applications and platforms, it can be difficult to stay on top of all the risks and potential attack vectors that exist for cybercriminals to exploit. APTs target vulnerabilities, human or technical – so the larger and more complex an organization, the more potential entry points exist.

3 The rise of Bring Your Own Device (BYOD) policies and remote employees only adds to the challenge. As well as being vulnerable in their own right, phones and tablets are often used to connect to unsecure networks. To make matters worse it's often harder – especially with operating systems such as Apple's iOS – to tell if a device is infected. A mobile workforce is like a moving target; devices operating outside the safety of your perimeter are harder to police, making effective endpoint security a significant component of your security strategy.

4 This wide variety of endpoints, coupled with the number of methods cybercriminals can use to infect a network means that singular security measures simply aren't enough. Instead, robust mitigation measures need to combine threat intelligence, security policies and specialized technology that won't just block recognized incoming threats, but also spot new ones – while using measures such as whitelisting to prevent the execution of threats still considered unknown.

5 Mitigation needs a renewed focus on the endpoint. Cybercriminals exploit vulnerabilities – and the enterprise is often at its weakest at the endpoint: where security is often compromised not just by the device itself, but by the lax behavior of the employee, or the unsecure surroundings on which it is being used. If your endpoints don't have multi-layered protection, then the entire organization can be left at risk.

WHY MITIGATION IS SO IMPORTANT

Mitigation is where enterprises need to start because prevention is significantly more effective and more cost-efficient than remediation after an attack.

The threat actors that develop APTs are highly skilled, determined and well-resourced. However, like all cybercriminals – with certain notable exceptions aside – they still find the path of least resistance attractive. So, while you can't guarantee immunity from APTs, there are measures you can put in place that will make it harder for an attack to succeed.

Just as APTs are often multi-layered threats themselves, an effective APT response needs to be multi-layered. Simple security tools are simply not enough.

So what does this approach look like? The Australian Signals Directorate has developed what Kaspersky Lab sees as an extended and thorough list of strategies to mitigate advanced threats. We believe that these strategies are just as applicable to enterprise, as well, and are a good place to start.

These strategies break down into four main categories:

1 SECURITY POLICIES AND EDUCATION

IT security is not just about IT. Human error is a big help to cybercriminals. By offering comprehensive and regular education on security issues, encouraging the right behaviors and implementing relevant and realistic policies, you can reduce the chance of employees bringing cyberthreats into your organization.

2 NETWORK SECURITY

The structure of your network can greatly help to reduce the potential impact of an infection. There are various network security strategies that can reduce risk and mitigate threats, for example, segregating certain sections of the network means you can reduce the number of endpoints that can access sensitive data, exponentially decreasing your level of risk.

3 SYSTEM ADMINISTRATION

Controlling and indeed restricting user administration privileges through security policies can significantly reduce the number of vulnerabilities you have to deal with. On top of this, capitalizing on the security features built into the programs you use makes a huge difference. Turning off unneeded features means you can make the most of software while shutting down avenues that could potentially be exploited.

Turning off Java® code execution in your browser is a great example of how you can eliminate vulnerabilities from the resources your employees use.

4 SPECIALIZED SECURITY SOLUTIONS

In addition to these steps, specific features of specialized software can add invaluable layers of protection. However, getting solutions to integrate doesn't have to involve huge levels of investment or significant staff resources. In fact, the three specialized security solutions below, together with restricting administration rights (see the System Administration strategy above), actually mitigate 85% of security threats. The three key specialized security solutions are:

- Using application control, whitelisting and default deny mode
- Patching the most commonly attacked applications
- Patching vulnerabilities within your operating systems

KEY MITIGATION STRATEGIES

There are a number of key mitigation strategies that any enterprise should already be doing or at least considering.

APPLICATION CONTROL AND WHITELISTING

Whitelisting is a powerful tool that can significantly mitigate against APTs and other attacks. Instead of asking whether an application might be harmful, whitelisting asks if we're certain it's legitimate. This puts control into the administrator's hands, regardless of users' behavior. A whitelist is created of known and trusted applications – and only applications within this list are allowed. Malware often manifests itself as an executable file of some type – which will be blocked and prevented using this approach. This is the opposite approach of traditional antivirus 'blacklists' which only prevent an application from launching if it appears on a list of "known offenders."

Taken to its most secure extreme, administrators can set up a "default deny" scenario, where only applications that are pre-approved by administrators will run: which massively limits exposure. Though this is an effective way to keep malware out of your network, you need to ensure you aren't blocking tools that your colleagues genuinely need to use to work more effectively. Using more granular application control, with dynamic whitelisting, gives you more control tools at your disposal. You can block or control usage of applications by software category, business unit, individual user and other factors.

Of course, before you can use whitelisting effectively, you need to know what applications are already running on your machines. Therefore taking an inventory is vital. After all, you can't monitor something if you don't know it's there.

KASPERSKY LAB FEATURE: APPLICATION CONTROL WITH DYNAMIC WHITELISTING

Kaspersky Lab's dynamic whitelisting database of legitimate applications is well over 1 billion strong, including 97.5% of all software related to the corporate sector. Our ongoing threat intelligence means this is constantly updated by our Kaspersky Security Network via the cloud.

Our application control goes beyond just "stop/start" functionality. When an application does need to be blocked, we allow all unmodified components of the operating system to run as normal. This means you can stop attacks without disrupting your users' activities. Kaspersky Lab also makes it much easier to implement a default deny mode as we provide a test mode to help you see in advance if there will be complications when it "goes live."

KASPERSKY LAB FEATURES: VULNERABILITY ASSESSMENT AND PATCH MANAGEMENT

The database our technology uses to scan for vulnerabilities is extensive: Kaspersky Endpoint Protection for Business will automatically find and install Microsoft updates, as well as updates (renewals) for non-Microsoft applications. This means you can keep all your applications and operating systems updated, without dedicating valuable staff resources to the task.

"In default deny mode, only trusted programs are allowed to run on your computer and I can tell you, the vast majority of malware used in APT attacks comes in from untrusted or unpatched applications."

Costin Raiu, Director of Global Research and Analysis Team, Kaspersky Lab.

PATCHING APPLICATION AND OS VULNERABILITIES

Both applications and operating systems contain vulnerabilities that can be exploited by criminals. It's important to stay on top of these security gaps and close them before malicious code can be introduced. And it's the popular applications that often contain vulnerabilities when left unpatched.

Patch management tools are critical for multi-layered IT security, as they can automate the task of keeping applications updated across many endpoints. As a result, you can make sure that potential points of entry for an attack are closed as quickly as possible.

Again it should be stressed that there is no fool-proof way to protect you from APTs.

But, correctly implemented, a combination of all four of these strategies (administration privileges, application control, patch management and OS management) can protect against 85% of targeted attack-related incidents. Together, they make it more difficult for malicious code to execute or run undetected. That's because they enable multiple lines of defense.

In 2014, vulnerabilities in Oracle Java, popular browsers and Adobe Reader® accounted for 92% of malware exploits.[2]

[2] Kaspersky Security Bulletin 2014, Kaspersky Lab

OTHER HIGHLY EFFECTIVE STRATEGIES

As we stated at the start of this document, cybersecurity is not a numbers game. Though you can protect against the majority of intrusions using the top mitigation strategies we've already explored, you still need to go further.

Here are a few additional techniques you can use to add extra layers of defense:

OPERATING SYSTEM EXPLOIT MITIGATION

Though native technologies can do a lot to mitigate generic exploits in operating systems, specialized solutions can help you take things further. And there's very good reason to do so. For instance, even if you're constantly patching your applications and operating systems, you're still potentially susceptible to an attack that uses a zero-day vulnerability.

That's why it's important to have a solution that identifies and neutralizes known threats, but also detects anomalies and suspicious behavior – thereby protecting you against unknown threats. This way you can even defend against attacks that have never been seen before.

HOST-BASED INTRUSION PREVENTION

As has been proven, APTs are stealthy malware and can stay hidden for months if not years. So just having a perimeter defense is not enough – what if malicious code is already lurking inside your organization? What's needed is technology that recognizes and prevents program activities that are "too risky", even if they're not definitely malicious. Host-based Intrusion Prevention systems (HIPS) restrict application activities within the system according to their trust level. HIPS spots "execution anomalies" – applications performing functions or activities that are out of context and also suggest risk. This is best done immediately after applications are installed (i.e. before they have any chance to be corrupted by a stealthy malware attack).

KASPERSKY LAB FEATURE: AUTOMATIC EXPLOIT PREVENTION (AEP)

Paying particular attention to commonly targeted programs such as Internet Explorer®, Microsoft Office® and Adobe Reader®, AEP carries out a series of security checks. Continuously monitoring processes in memory, it is able to discern suspicious behavior patterns characteristic to exploits, which are much more limited in their numbers than exploits themselves. This approach allows Kaspersky Lab's AEP to stop even zero-day exploits.[3]

[3] According to MRG Effitas independent test, AEP was able to protect test endpoints against exploit-based attacks in 95% of tests with all other defensive mechanisms switched off'

KASPERSKY LAB FEATURE: SYSTEMS WATCHER AND APPLICATION PRIVILEGE CONTROL

Between these two features, events happening within your computer systems can be monitored and recorded, ensuring that applications don't attempt to carry out malicious actions. System Watcher and its rollback subsystem is able to undo undesired changes, and Privilege Control prevents such changes from happening if they're initiated by applications having a low-trust level.

DYNAMIC ANALYSIS OF EMAIL AND WEB CONTENT

Just as a signature-based approach can't combat zero-day attacks, using traditional "static analysis" to compare the content of emails and web pages to a database of known malware can't secure you against new threats.

That's why dynamic analysis is so important. You need a solution that can look for suspicious characteristics encoded in web pages and emails – such as trying to find and modify executable programmes – and block them before they're opened.

A 'zero-day' attack is one which targets a previously unrecognized vulnerability in an operating system or application, before a patch can be made available.

KASPERSKY LAB FEATURES: WEB CONTROL AND WEB ANTIVIRUS

Our Web Control technology allows you to decide whether to allow users to access sites, both on an individual basis, and by classification of website type (e.g., a gambling site). By monitoring HTTP(S) traffic, you can make sure the web resources accessed on endpoints match your whitelist.

Meanwhile, our web antivirus uses dynamic analysis to spot malicious code delivered by HTTP(S) and FTP protocols, protecting against APTs that use downloads

KASPERSKY LAB FEATURES: MAIL ANTIVIRUS AND SECURITY FOR MAIL SERVER

Using a combination of static and dynamic analysis and heuristics, Kaspersky Endpoint Security for Business helps to block threats transmitted via email. By emulating how attachments might behave, our technology can detect file-based exploits in email attachments.

Kaspersky Security for Mail Server, with its Data Loss Prevention (DLP) option, can also stop employees from sharing important information. By rendering files "un-sharable," you can ensure they don't leave your company via email attachments.

THE KASPERSKY LAB APPROACH: MULTI-LAYERED PROTECTION

The security threat landscape is a complex and fast-evolving one. At Kaspersky Lab, we work with large organizations on a multi-layered strategy – from mitigation to threat intelligence services.

As a technology-driven company, we've developed the tools you need to build a well-rounded mitigation strategy. And because they're all built from the same code base, they integrate seamlessly, allowing you to formulate a comprehensive security strategy without leaving unnecessary gaps in your armor.

At the core of our approach is our award-winning anti-malware technology and endpoint firewall. Together these block the 70% of known threats. With more advanced tools such as behavioral analysis, heuristics, application control with dynamic whitelisting and web control, we protect against the unknown threats. And for the advanced threats we add another layer of protection to help, using advanced tools such as Kaspersky Automatic Exploit Prevention and Systems Watcher.

INTELLIGENCE AND DETECTION – TO RAPIDLY IDENTIFY LIVE ATTACKS

Although a thorough approach to mitigation is vital, your counter-APT strategy should also include measures that ensure you can detect a "live" attack – without causing any time-consuming false alarms. In addition, your strategy should include technologies that can rapidly block an attack and minimize the damage caused to your business.

Our recommended approach includes endpoint-level detection, network-level detection, intelligent sandboxing and a comprehensive events database.

Recently, network-level detection has captured the imagination of several IT vendors – and many vendors have introduced dedicated appliances for network detection. However, we believe an alternative solution – one that uses a distributed sensor architecture – can offer significant advantages. By placing sensors at key points in the network – all feeding data into a central point – it can help to improve detection. In addition, it can allow greater scalability and helps to reduce costs when complex, enterprise-level networks need to be protected.

BEYOND THE TECHNOLOGY: THREAT INTELLIGENCE SERVICES

Even though mitigation will greatly reduce the risks for any organization, it's not possible for any security solution to guarantee 100% protection.

If an attack is successful, your business will need to determine:

- Exactly what data has been stolen – so you can take action to limit the damage caused by the loss
- How the attack was enabled – so you can address any specific vulnerabilities and security gaps

That's why it's important to have the best in forensic analysis at your disposal – ready to provide you with rapid access to the necessary security expertise.

Kaspersky Lab offers a range of intelligence services – and you can choose the level of service that's right for your business:

- Malware analysis – for customers that have their own in-house forensics team
- Digital forensics services – including malware analysis
- Full incident response services – including forensics

WHY KASPERSKY LAB

Kaspersky Lab is one of the organizations at the very forefront of the fight against APTs. Our GReAT (Global Research and Analysis Team) experts have been involved in the discovery of many of the world's most dangerous and complex threats, from Red October to the recently uncovered The Equation Group of cyberespionage tools.

Unfortunately for cybercriminals, scale isn't much of an issue. Once advanced cyberweapons are developed, it doesn't take much for groups to repurpose them for business targets. That means even weapons that may have been covertly developed at huge expense by nation states can end up in the hands of criminal gangs.

We recognize this. That's why we're moving to level the playing field. We use the intelligence gathered from investigating APTs to advise governments on how to defend against cyberattacks. But we don't stop there. We use everything we learn from this work to build solutions that will be both effective and practical at the enterprise level.

To this end we combine our unparalleled security intelligence with technological innovation. We have a significantly higher proportion of our people working in research and development than any of our competitors.

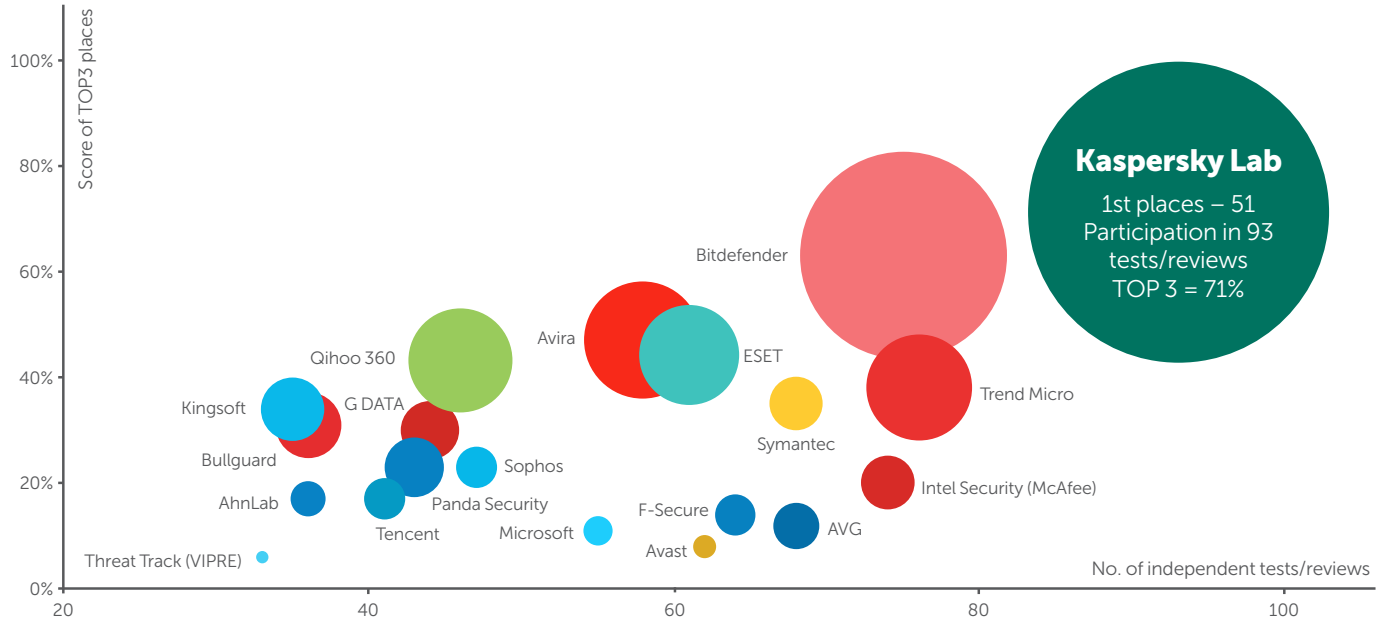
The result is a multi-layered approach to enterprise security, which can help form the mainstay for any enterprise looking to build a counter-APT mitigation strategy.

Our confidence in our solutions has led us to enter more independent tests than any other vendor. We've achieved malware detection rates of over 99% and, of the 93 independent tests we entered in 2014, we finished in the top three in 66, and first in 51[4] – results that none of our competitors come close to. Kaspersky Lab technology is also used and trusted by over 130 OEM partners – so you could already be using Kaspersky Lab today.

[4] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

KASPERSKY LAB: BEST IN THE INDUSTRY PROTECTION*

In 2014, Kaspersky Lab products participated in 93 independent tests and reviews. Our products were awarded 51 firsts and received 66 top-three finishes.



* Notes:
According to summary results of independent tests in 2014 for corporate, consumer and mobile products.

Summary includes tests conducted by the following independent test labs and magazines: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. The size of the bubble reflects the number of 1st places achieved.

PROTECTING TODAY, SECURING THE FUTURE

An increasingly sophisticated and complex threat landscape calls for a multi-layered security platform that defends against known, unknown and advanced threats.

Visit **kaspersky.com/business-security** to find out more about Kaspersky Lab's unique expertise.

GET A FREE TRIAL

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

Review our blog

Join us on Threatpost

View us on Securelist

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.