ADVANCED THREATS: MEET ADVANCED DETECTION TECHNIQUES

www.kaspersky.com

The number of targeted attacks on enterprises is growing and the techniques and skills of the attackers are more sophisticated than ever. Harder to detect and - often - even harder to eliminate, targeted attacks and advanced threats call for a comprehensive, adaptive security strategy. Advanced detection capabilities sit at the core of this approach.

TOO LATE TO VACCINATE?

No organization is immune to cyber-attack. But most are stopped at the perimeter by the company's IT security solution, no harm done. Of the ones that do breach the perimeter, many will still be detected and mitigated. So far, so good.

> *Every business big enough to occupy a significant segment of their market is a potential target. This doesn't mean smaller businesses are immune – in many cases, criminals view them as an easy-to-breach stepping stone from which to reach their bigger target. In the case of market leaders, the odds of attack increase substantially. It's not a case of 'if' but 'when'...*

But there are more advanced, specially targeted threats that can go undetected for weeks, months, or even years while the perpetrators silently gather information and work incrementally to search for and exploit the vulnerabilities in their target's systems.

These advanced, targeted threats are tailored specifically to exploit the unique vulnerabilities of their chosen targets' systems. Unlike regular malware, advanced, targeted threats are actively controlled and managed by the perpetrators. The goal isn't limited to malware delivery – the actors seek persistence inside the enterprise perimeter, from where they slowly and silently steal the information they're looking for. They're the result of patient, often painstaking research by actors who are prepared to wait for their prize. And they're on the increase: 15% of enterprises have experienced a targeted attack, more than 53% losing sensitive data as a result[1].

And they're just the businesses that know they've been hit...

[1] Kaspersky Global IT Security Risks Report 2015

MIND THE GAP

A defining feature of advanced, targeted threats is their stealth. Research shows that financial organizations take an average of 98 days to detect an attack; retailers take up to 197 days[2]. This 'detection deficit' can be costly. By the time the enterprise has noticed they're under attack, the damage is done.

One-in-three companies reporting a data breach event suffered temporary loss of the ability to trade; typical direct costs incurred by a serious event are $38k for a small business and $551k for enterprises.[3] That's before you factor in the less-easily-defined costs associated with legal costs, reputation damage or loss of competitive advantage.

So what can you do about targeted attacks and advanced threats? First, let's take a quick look at how they work...

Who's on the attack?

Cybercriminals – who sell data to the highest bidder or simply steal money. They usually develop their cyber tools themselves or buy them on the black market.

Competitor companies – looking for confidential data or even committing sabotage. Usually 'buy in' the services of cyber-mercenaries.

Cyber-mercenaries – masters of cyber-espionage, they develop their own tools and sell their 'services' to the highest bidder.

Hacktivists – claim to be working for a 'greater good', they're inventive, use complex toolsets and present a serious problem for any business that attracts their attention

Government agencies – they may deny it, but it's generally accepted that governments the world over routinely track individuals, groups and businesses. Their toolsets can be extremely sophisticated, expensive and hard to detect.

IT STARTED WITH A PHISH... FIVE PHASES OF AN ATTACK

Just like a real-world military operation, targeted attacks are campaigns rather than one-off hits. They're made up of several incremental phases of execution: 1. Reconnaissance and testing 2. Penetration 3. Propagation 4. Execution.

At the heart of these phases lies a need to somehow dupe end users into installing the malware needed to do the job. Phase 1 usually provides the insight needed to tailor the best penetration method. Social engineering, water-holing (infecting via web sites that research shows are popular with the criminal's target users), phishing attacks and portable devices are the somewhat low-tech-but-effective techniques used to gain the toehold needed for more sophisticated malware to do its work. For really well-prepared attacks, malware often isn't used initially at all – the attackers can steal administrator credentials or falsify certificates to gain a toehold on company systems without ever triggering security software. Whatever the technique used, reconnaissance is all about finding ways to circumvent existing security measures without alerting anyone. For some cyber criminals, this is where their involvement ends; others fully compromise their targeted systems before going dormant and offering access for sale 'as-a-service'.

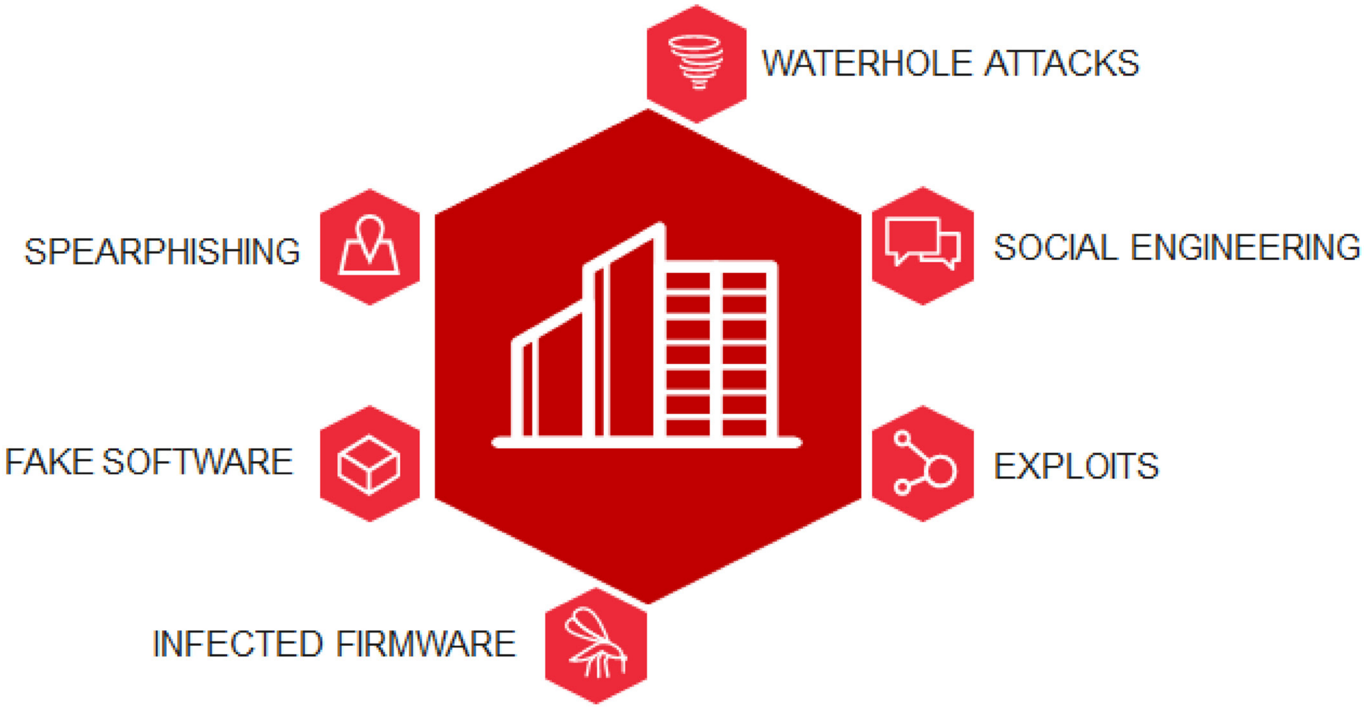
[2] Ponemon Institute, *Advanced Threats in Financial Services – A Study of North America and EMEA*

[3] Kaspersky Global IT Security Risks Report 2015

Reconnaissance also feeds testing – criminals gather as much information as possible on any security software in place, developing their attacks and testing them out against their target's chosen product. It's easy to do: all it takes is a download of a free trial and they can hone their attack against the target's existing defences. In this environment, prevention on its own can never be enough – you've got to go for advanced, multi-factor detection.

The penetration and propagation phases involve the silent installation of malware from within the company's systems. Targeted attacks are shipments of malicious code designed first to obscure itself and secondly to perform what is effectively a high-end, automated heist on targeted systems – information is being gathered and sent back to a remote 'command and control' server; further malware is used to spread out, deeper into the company network in search of the targeted data. And still no one knows this is happening. Undetected, this can go on for months or even years.

At the execution phase, the targeted data is gathered and sent to the command and control servers. At this point, the criminals have complete control over their target system and are able to effect changes in ways that don't attract attention or trigger security software. They can lie dormant between attacks in order not to attract attention by grabbing too much data at one time. They can hide in plain view, using the same ports as regular users use for web surfing to communicate with their remote servers – hitching a ride on normal end user activity is a classic technique targeted attackers use to hide. If sabotage is their aim, attackers can now corrupt systems, wipe critical information or even take control over hardware to effect malicious activity.



Even at this point, a targeted attack can be difficult to detect: remote, often automated managers constantly update the malware, changing the code that drives the attacks and monitoring security software blacklists they use to locate command and control servers. All this makes it harder to track, disrupt or detect in the first place. And when the job is done – or you do detect them…

It's clean-up time. Every trace of the malware is removed or obscured to make forensic analysis or tracing impossible.

Targeted attacks often exploit unpatched or previously unknown zero-day vulnerabilities in widely used business software to gain initial access to their chosen victim. Often, a combination of all these techniques is used.

DETECTION IS DIFFICULT – AND OFTEN TOO LATE

The reality is that malware is responsible for only 40% of breaches – as we've seen, threat actors use a variety of techniques to access company systems. Even when malware is used, 70-90% of it is is unique to the organization it's found in[4]. What this means in real terms is that cybercriminals spend a lot of time tweaking their code and using heavy obfuscation techniques to evade detection - almost as much time as your end users spend clicking on their sophisticated, well-researched phishing emails… A campaign of just 10 emails yields a greater than 90% chance of success[5]. In 60% of cases, attackers can compromise an organization within minutes[6], and at a relatively low cost: Kaspersky Lab research indicates a new trend towards the use of re-purposed, 'cheap and nasty', off-the-shelf malware for these attacks. Apart from being cost-effective, this less sophisticated malware has the added advantage of allowing perpetrators to hide among "mass market" threats, where its true intentions are less easily discerned.[7] And reduced costs usually mean more participants in the 'market'….

Perimeter security techniques like firewalls and anti-malware software can hold their own against some of the more opportunistic attacks. Targeted attacks are a different matter. Some vendors have sought to address this using a variety of standalone, discrete products: sandboxes, network anomaly analysis or even endpoint-focused monitoring. While these can – and do – offer some protection and blocking of the cybercriminal's toolset, individually, they're not enough to uncover

[4] Verizon: Data Breach Investigation Report

[5] According to the Verizon Data Breach Investigation Report 2015, 23% of recipients click on phishing mails and 11% open attachments; almost 50% of users open emails and click on phishing links within an hour of receiving them. In 60% of cases, attackers can compromise an organization within minutes.

[6] Verizon Data Breach Investigation Report 2015.

[7] Kaspersky Security Bulletin 2015: 2016 Predictions: It's the End of the World for APTs as We Know Them.

a targeted, co-ordinated attack. That requires detection of multiple events occurring across all levels of an enterprise infrastructure. This information can be processed using a multi-layered analysis system before interpretation using the latest security intelligence from a trusted source...In other words, a solution that integrates the best of sandboxing with network anomalies analysis and endpoint events analysis.

And that is exactly what Kaspersky Lab's Anti Targeted Attack Platform does. As we've seen, targeted attacks are compound, multi-stage and complex. To be able to connect the dots, enterprises need security based on exceptional insight into how these attacks work, supported by the very best technologies capable of predicting, preventing, detecting and remediating threats of all kinds.

GOOD, BETTER, GREAT

Kaspersky Lab was the first technology company to establish a dedicated advanced threat lab, back in 2008. That's why Kaspersky Lab has uncovered more of these advanced, targeted threats than any other security company, including some of the most notorious. If you read about the latest advanced persistent threat in the news, chances are Kaspersky Lab's elite Global Research and Analysis Team (GReAT) detected it.

This threat intelligence and insight directly informs Kaspersky Lab's product development; while Kaspersky Security Network builds on the real-time intelligence generated by over 60 million nodes worldwide, GReAT contributes a unique set of skills and expertise to our threat detection and research capabilities, developing solutions to detect increasingly complex, sophisticated, advanced threats.

Kaspersky Lab's understanding of the inner workings of some of the world's most sophisticated threats has enabled us to develop a multi-layered, strategic portfolio of technologies and services capable of delivering a fully integrated, adaptive security approach. Our expertise has seen Kaspersky Lab achieve more first place rankings in independent threat detection and mitigation tests than any other IT security company. Now, we're bringing this targeted attack detection expertise into one standalone solution – a combination of a decade's worth of threat research and analysis and mature, proven technologies.

This is the foundation on which Kaspersky Kaspersky Anti Targeted Attack Platform has been built – it's capable of detecting the stealthiest, most advanced threats.

KASPERSKY ANTI TARGETED ATTACK PLATFORM: DETECTION IN DEPTH

Standard threat prevention technologies can't differentiate between regular malware and that used in targeted attacks. The key to detecting targeted attacks lies in any organization's ability to detect the subtle behaviours and changes in systems that are indicative of a breach. Once a threat is detected, mitigation should be complemented by threat analysis, enabling enterprises to continually learn from attacks and strengthen their security strategy.

Kaspersky Anti Targeted Attack Platform is part of our adaptive, integrated approach to enterprise security, built on the pillars of prediction, prevention, detection and response. Real-time network traffic monitoring combines with object sandboxing and endpoint behaviour analysis to deliver maximum oversight into what's happening across the infrastructure.

This monitoring and analysis capability is complemented by the very latest threat intelligence from Kaspersky Security Network (KSN).

REAL-TIME, CLOUD-BASED THREAT INTELLIGENCE

Effectively a global, cloud-based threat laboratory, KSN uses real-time anonymized threat data from over 60 million volunteer endpoint sensors globally to deliver the latest threat intelligence to Kaspersky analysts and customer systems. Every file that passes through Kaspersky Lab protected systems is subject to analysis based on the most relevant threat intelligence. This means organizations always have the most up-to-date threat intelligence against which to analyse or detect suspicious activity on their systems.

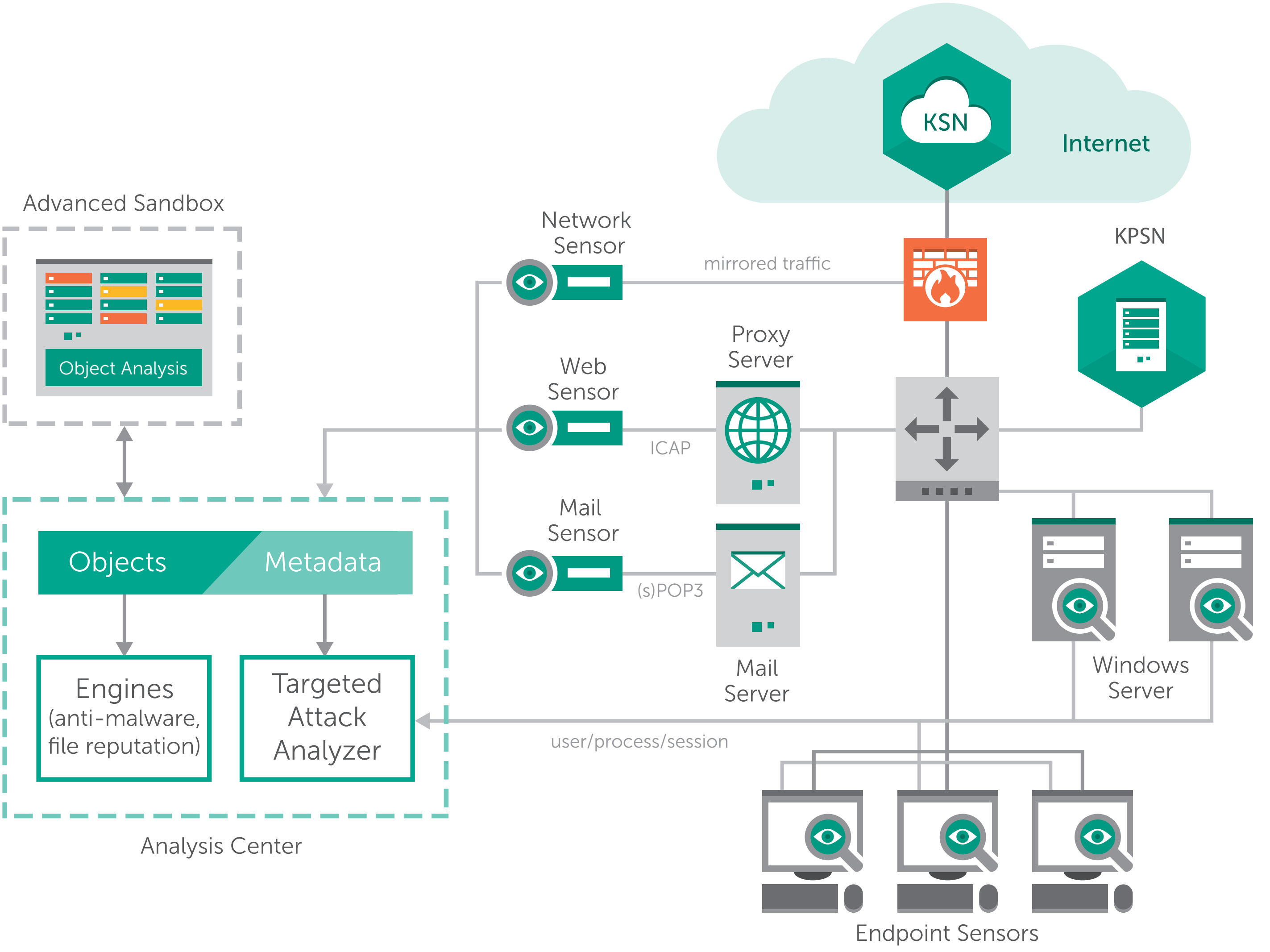
KSN has a high number of participants among consumer users, giving Kaspersky Lab unique insight into the minds of targeted attack actors, who regularly exploit home user behaviors to compromise their targets. Business users often transfer malware from home to the workplace without anyone knowing; Kaspersky Lab's 360-degree insight into both consumer and business-focused threats delivers supplies our Anti Targeted Attack Platform with comprehensive threat intelligence from across all use spectrums.

ALWAYS ON, ADVANCED LAYERS OF DETECTION

While Kaspersky Security Network delivers the latest threat intelligence, our Anti Targeted Attack Platform operates on three key levels: network traffic, distilled objects and endpoint-based activities. Network sensors watch over network traffic providing metadata and objects for study, Web and Mail sensors deliver comprehensive monitoring of emails and distilled traffic objects.

Abnormal **network activity** or suspicious **files are flagged**; advanced **sandbox technology** provides a safe, virtualized environment in which suspicious objects can be allowed to execute, enabling further analysis. **Anti-evasion** technologies mean sandboxes can proactively detect unknown or tailor-made malware that escapes the attention of traditional, file-based anti-virus software. Support for **YARA rules** means security analysts can apply their own rules - or publicly available third-party rules.

Kaspersky Anti Targeted Attack Platform



This advanced detection capability is further enhanced by targeted attack-related host detection, a continuously updated database of active command-and-control servers, toxic web sites and malware distribution points. Data supplied is the very latest intelligence from Kaspersky Lab's GReAT team, enabling detection of even the very latest threats.

Kaspersky Lab's Targeted Attack Analyzer, meanwhile, detects activity abnormalities in near real-time. This component monitors the combined data from both network and endpoint sensors, delivering statistical and reputational analysis; calls to command and control servers (a sure sign of a breach) can also be detected.

What each of these layers working together can do is develop the capacity to match information about ongoing activities and system behaviour patterns that are normal for your specific enterprise. As soon as something out of the ordinary happens, even if it looks legitimate, the Kaspersky Anti Targeted Attack Platform knows to check it out and send an alert to security staff.

AT YOUR SERVICE

As we've seen, successful targeted attacks use multiple techniques and exploit different areas of vulnerability. It makes good strategic sense for any organization to learn as much as possible from an attack; understanding your adversary's tools and techniques is key to strengthening and honing your enterprise security strategy. If you don't understand how to respond to an attack – and adjust your strategy accordingly - detection in and of itself becomes almost pointless, no matter how good the technology you have in place is. Problems persist unless you adjust to deal with them.

Kaspersky Security Intelligence Services, including Incident Investigation, Incident Response and Targeted Attack Discovery Service, complement the cutting-edge detection capabilities of Kaspersky Anti Targeted Attack Platform. Incident investigation and response services deliver tailor-made rapid-response to any incident, minimizing the damage and ensuring that the right kind of evidence is collected to enable a tailor-made forensic analysis to be completed (and learned from). Full malware analysis – everything from how it was installed to related vulnerabilities, means of propagation and functionality, among other things – enables complete understanding of the behaviour and objectives of the attack, along with remediation advice and support.

Targeted Attack Discovery Service delivers 'scene of the crime' analysis – before the crime can take place. Kaspersky Lab experts conduct an on-site assessment of organizational vulnerabilities while searching for any as-yet-undetected attacks that might be underway.

A word on sandboxes

Many 'targeted attack detection solutions' on the market simply comprise of a standalone sandbox. Even vendors with no track record in new, advanced threat discovery claim to offer sandboxes that are often little more than an extension of their anti-malware engines – and have no significant threat intelligence behind them.

Kaspersky Lab's sandbox is just another part of our integrated detection capabilities. Not only that, it's a derivative of our in-house sandbox complex, the technology the company has used for itself for more than a decade. Its capabilities have been honed on the statistics gathered from ten years of threats, making it more mature and more focused on targeted threats than a lot of companies currently selling them as silver bullet solutions.

Networks are checked for Indicators of Compromise (IoC), critical resources assessed for vulnerabilities and any evidence associated with attack – including log files, hard drive images, memory dumps – collected for further analysis. A detailed report with remediation advice is then prepared, further strengthening security strategy.

Kaspersky Lab's vision for the most comprehensive detection strategy available doesn't end here; research and development teams are currently building our Endpoint Detection and Response (EDR) solution, which will deliver a collection of tools that focus completely on detecting, mitigating and investigating suspicious activities on endpoints, including an IoC scanner. The solution will integrate fully with Kaspersky Anti Targeted Attack Platform.

PART OF A MULTI-LAYERED, ADAPTIVE SECURITY STRATEGY

Cybercriminals have adapted their techniques to sidestep traditional defences and lurk undetected on systems for months, or even years. It's time for enterprise security to adapt with an intelligence-driven, multi-layered approach to IT security.

Kaspersky Anti Targeted Attack Platform delivers a new, more strategic approach to detecting targeted attacks. Complemented by our multi-layered prevention technologies and solutions, as well as an extensive portfolio of Security Intelligence Services for response and prediction, Kaspersky Lab delivers a truly integrated, strategic approach to targeted attacks and threat detection and response. These technologies and services facilitate the most effective enterprise security strategies and the architectures that support them, including those built on the pillars of prediction, prevention, detection and response.

Our focus is not just whatever the 'threat-of-the-day' is, we constantly seek to out-think and out-smart threat actors; our track record in discovering some of the world's most sophisticated threats, along with our unrivalled performance in independent tests illustrate our commitment to success.

Kaspersky Lab's Anti Targeted Attack Platform incorporates security intelligence with a proven innovative approach to advanced threat detection. A security architecture that includes frequent security evaluation and updates combined with insights from global security intelligence reporting delivers the most comprehensive protection available – across the current threat continuum and into the future. Our technologies and vision combine to enable enterprise security strategies with a constant eye on the future and how organizations can prepare to meet new threat challenges.

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline