Confronting modern stealth

Cybersecurity in the age of fileless threats, targeted attacks and APTs

kaspersky BRING ON THE FUTURE

Introduction

Flashback: crime before cybercrime

In the early hours of August 8, 1963, a gang of thieves held up a Royal Mail train and stole 120 sacks of bank notes - worth about $7 million at the time ($50 million today). The UK heist seized the imagination of people all over the globe, making (anti-)heroes of the thieves, and spawning films, TV shows, books, songs and even video games (including a quest in **Runescape**). All but four of the 15 men were caught, arrested and sentenced.

The legendary Great Train Robbery:
$50 million (in today's money)

The NotPetya attack (2017-):
$10 billion

Cybercrime dwarfs the heists of old

On June 27, 2017, researchers from Kaspersky's Global Research and Analysis Team (GReAT) announced a ransomware-like wiper attack, which they called **NotPetya**, to distinguish it from 2016 Petya variants. The attack used a modified EternalBlue exploit to propagate within corporate networks. The total damage from the NotPetya attack is estimated at $10 billion, with some victims taking hits in the region of hundreds of millions. Merck lost $870 million, FedEx lost $400 million and Maersk lost $300 million. At the time of writing, only one arrest had been made so far.

Cybercrime: the ultimate remote heist

Criminals don't need to hold up trains anymore – they can plan and execute devastating (and highly profitable) attacks from the very remote comfort of their ergonomic office chairs.

Any kind of cybercrime naturally shrinks the footprints criminals leave behind at the scene and, as for fingerprints – cyber forensic experts can only dream of such evidence. Even the crime scene itself can be hard to pin down – with cyberattacks leaping over national borders, and breaking through corporate IT perimeters with barely a whisper.

Vanishing footprints

The evolution of crime from the Great Train Robbery to NotPetya tells a story of vanishing footprints, and of malice executed from an increasing distance. Yet that story is far from over. Within a few years, the techniques used by the NotPetya attackers might seem as antiquated as those of the Great Train Robbers.

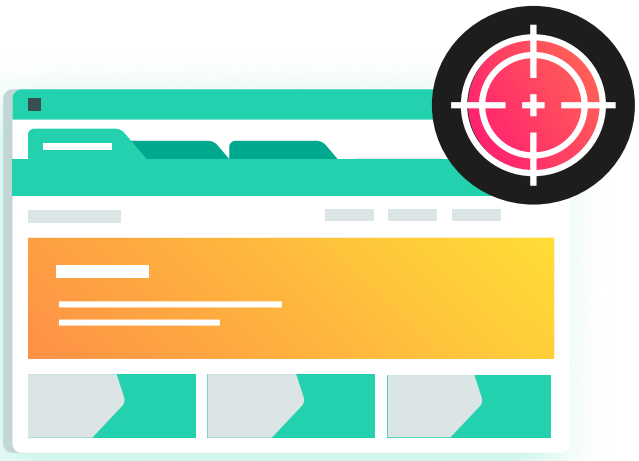
The new stealth

In this paper, we're going to look at some of the aspects of the 'new stealth' – the dizzying escalation in the sophistication of cybercrime techniques, which threatens to allow criminals to penetrate the armor of traditional cybersecurity solutions, and wreak havoc while barely leaving even a trace of a digital footprint. We'll also reveal some powerful (and straightforward) ways you can defend your organization effectively against evasive attacks, with no extra effort from your team – even in the context of the cybersecurity talent crisis.

The anatomy of targeted attacks

Targeted attacks are the hawkeyed villains of the new stealth – picking out victims and refining their methods to weaponize under-protected systems (and uneducated users) to bring businesses to their knees. Methods and characteristics include:

- Cybercriminals investigate a victim's endpoint protection system prior to launching an attack, in order to craft a mechanism to bypass it automatically
- Zero-day vulnerabilities and uncompromised accounts – catching under-protected businesses totally unaware
- Bespoke malicious software developed expressly to destroy a specific business
- Compromised objects that appear normal, and bypass inadequate endpoint protection, or absent endpoint detection and response
- Multi-vector assaults – attacking as many endpoints as possible, simultaneously
- Highly devious **social engineering** and attacks informed by specific and personal insider data, which may be targeted at senior personnel



False positives – drowning in (wrongly placed) red flags

False positive rates range from 30% to as high as 99%, and are a deadly double-edged sword. On the one blade, false positives cause exhaustion – with IT staff wasting precious hours investigating each alert, while true positives can slip by their potentially inadequate cyberdefenses. The second blade is that one of the most common ways for IT staff to relieve this exhaustion and stem this deluge of false positives is to reduce the sensitivity of their cybersecurity solutions, so that fewer emerge. Either way, false positives can be lethal.

The good news is that you can do away with false positives completely and focus on relevant threats alone. When **AV-Test** tested Kaspersky Endpoint Security for Business (along with endpoint protection solutions from 14 other vendors), our product returned a stunning zero false detection or blocking score.

Fileless threats

Cybercriminals are increasingly moving towards launching fileless attacks, creating a challenge for businesses that have historically relied exclusively on traditional endpoint protection solutions.

The day after we broke the news of the NotPetya attack, we advised global businesses how to stay safe. We were able to give very clear instructions to prohibit the execution of a file called perfc.dat, using the Application Control feature of the Kaspersky Endpoint Security for Business suite. No such instructions can be given for fileless attacks – a different approach is needed, which we'll cover below.

Techniques used in fileless attacks include (but are not restricted to):

- **Malicious scripts stored in WMI subscriptions**
- **Malicious scripts directly passed as command line parameters to PowerShell**
- **Malicious scripts stored in registry and/or OS task scheduler, and executed by OS scheduler**
- **Malicious executable extracted and executed directly in memory without being saved on the disk, via Reflection in .Net**

Due to their stealthy nature, fileless attacks are 10 times more likely to succeed than file-based attacks. One of the most high-profile fileless attacks was the breach at American consumer credit agency Equifax in 2017, which led to the theft of 146.6 million personal records.

Analyze behavior – not just files – with Kaspersky Endpoint Security for Business

When there is no suspicious file to detect, the only approach is to detect suspicious behavior. In fact, preventing fileless attacks without behavior detection technology is a completely hopeless endeavor.

Kaspersky's behavior detection technology runs continuous proactive machine learning processes, boosted by extensive threat intelligence from Kaspersky Security Network's data science-powered processing and analysis of global, real-time statistics.

Our exploit prevention technology blocks attempts by malware to exploit software vulnerabilities, and adaptive anomaly control can block process actions which don't fit a learnt pattern (e.g. prevent PowerShell from starting).

The cybersecurity talent crisis

Running alongside the new stealth is a perilous cybersecurity talent gap – cybercriminals are skilling up prodigiously, but cybersecurity experts capable of taking them on are increasingly scarce on the job market, with both recruitment and retention a perennial challenge.

In 2019, **Forbes Magazine** reported that "unfilled cybersecurity jobs are expected to reach 1.8 million by 2022, up 20% from 1.5 million in 2015." **Security Magazine's** proclamation was even more dramatic: "A war is raging for cybersecurity talent."

Tragically, far too many companies have suffered the bittersweet fate of finally recruiting and training an in-house IT security expert, only to have them jump ship and take their priceless expertise elsewhere – for a higher salary.

Even apart from the cybersecurity talent crisis, full-time in-house cybersecurity expertise can be cost-prohibitive for companies already stretched to people the IT teams they need to thrive in the age of constant digital transformation.

Until the cybersecurity talent crisis is resolved, technology is the only way to bring future-proof cyberdefense within reach of the budgets and skillsets of companies everywhere. Human expertise remains essential, but the right IT security technology can act as a crucial bridge between pressurized IT teams and industry-leading security analysis.

Our bridge between pressurized IT teams and industry-leading security analysis is Kaspersky Sandbox – it automatically blocks complex threats at the workstation and server level. When we built Kaspersky Sandbox, our number one goal was to relieve the pressure on IT teams, so that they would have more time to manage complex – and necessary – tasks.

Kaspersky Sandbox does just that, by allowing small organizations to confront modern threats without the need to hire full-time IT security professionals, while larger enterprises can significantly reduce outlays on IT security experts and associated costs by automating most of the tasks related to advanced threat prevention, including triage and analysis.

Based on dynamic threat emulation (sandbox) technology, Kaspersky Sandbox harnesses our best expert practices in combating complex threats and APT-level attacks, and is tightly integrated with Kaspersky Endpoint Security for Business. This is how it works:

- Kaspersky Endpoint Security for Business sends a request to Kaspersky Sandbox to scan an object
- Kaspersky Sandbox runs the scan in an environment isolated from the company's real infrastructure, on virtual machines equipped with tools that emulate a typical working environment
- Kaspersky Sandbox collects and analyzes artifacts, and uses behavioral analysis
- If the object performs malicious actions, Kaspersky Sandbox recognizes it as malicious, and assigns a verdict to it
- Depending on the verdict, Kaspersky Endpoint Security for Business either automatically blocks the file, or marks it as clean
- The verdict is sent in real time to the shared operational cache of verdicts, so that other hosts with Kaspersky Endpoint Security for Business can quickly obtain data on the scanned object without having to analyze the file again

Kaspersky Sandbox is fast, dynamic, efficient, and brings complex IT security expertise within the reach of companies everywhere. Its tight integration with Kaspersky Endpoint Security for Business means that Kaspersky Sandbox provides an essential barrier against complex modern threats, even for companies that have yet to hire in-house IT security experts.

Lateral malware movement in Advanced Persistent Threats

Old-fashioned malware attacks behaved similarly to the Great Train robbers – cybercriminals penetrated a system, took what they wanted and escaped as quickly as they could. In the era of new stealth, cybercriminals' ambitions have grown considerably, along with their techniques.

Lateral malware movement is part of what puts the Persistent into Advanced Persistent Threats (APT). Instead of busting in and busting out, cybercriminals weaponize a range of tools to expand laterally within a system, moving from device to device. Such attacks can result in a state of continuous compromise, with the victim being subject to a seemingly endless cavalcade of malicious incidents.

Lateral malware movement is hot, and getting hotter. In our **annual APT review for 2019**, we warned of two APTs that had recently been employing lateral malware techniques:

- New activity from BlueNoroff, with attackers moving laterally to access high value hosts, by using a public login credential dumper and homemade PowerShell scripts.
- Lateral movement by the Icefog threat actor, using a technique called load order hijacking.

"Increasing complexity and frequency of attacks elevate the need for detection of attacks and incident response."

Gartner, Inc.

Crushing APTs with the visibility, analysis and insight triumvirate

Removing the Persistent from APTs, and stopping lateral malware movement in its tracks, demands a range of very specific endpoint detection and response (EDR) capabilities, which can be grouped into two categories – visibility and analysis:

- **Visibility**
  - The power to visualize and monitor all endpoints simultaneously, and in real time, from a single centralized interface
  - Contextual information on individual endpoint activity as well as processes, timelines and interrelationships between endpoints across the company
  - Clear gathering of priceless security intelligence for use by an IT security expert for further investigation and response

Without EDR, the cost for system reimaging (to effectively look back in time) in the event of an incident falls in the range of $400 to $600 per occurrence.

"Use the EDR modules available from your incumbent EPP vendor."

Gartner, Inc.: Endpoint Detection and Response Architecture and Operations Practices

— **Analysis**
  - **In-built mapping or correlation of multiple verdicts from different detection mechanisms into a single unified incident, to understand a threat's main tactics, procedures and techniques**
  - **Retrospective analysis of lateral malware movement**
  - **Analysis of events that take place in the 'gray zone' that lies between trusted/legitimate objects and processes, and those that are definitely malicious, chiefly including:**
    - Zero-day vulnerabilities
    - Unique malicious software (not seen elsewhere)
    - New/unknown malware
    - Compromised legitimate software/processes

Without EDR, the cost for gathering and analyzing evidence from hundreds of different endpoints and systems for incident response is phenomenal – with security experts charging up to $600/hour.

A few words about the macOS cyber-resistance myth
macOS devices deserve special mention here, because of the dangerous myth that their operating systems are somehow inherently cyberattack-resistant. The only reason that macOS devices fall prey to cyberattack less frequently is that there are fewer of them – leading criminals to focus their malice on the herd at large (usually Windows). Historically reserved for designers and other creatives, who may have reduced access or permission to central systems, macOS devices are becoming increasingly popular, especially with startups and other innovative companies influenced by IT consumerization (the phenomenon whereby consumer IT behavior influences business choices).

Cybercriminals are increasingly focusing their attentions on the Achilles heel that under-protected macOS devices represent. In the first half of 2019, **we detected nearly 6 million phishing attacks** on macOS users, with a full 11.8% targeting corporate users. We also found two Trojan families targeting macOS users - Trojan.OSX.Spynion and Trojan-Downloader.OSX.Vidsler. The former contains a backdoor that allows attackers to remotely connect to the user's macOS, and is distributed along with several free macOS apps, while the latter is distributed from banner ad links.

A cacophony of devices: modern threats, the mixed environment and BYOD

Building the perfect IT environment means drawing from a full range of devices, operating systems, network protocols and technologies. With the popularity of Bring Your Own Device (BYOD) showing no signs of waning, the IT environment is often not only mixed, but also unpredictable.

A typical IT setup will include Windows and/or Linux for backend systems, with employees in the office using Windows or macOS devices. Mobile provisioning is increasingly complex, and often includes dedicated tablets or other devices for mission-critical operations and services.

In the era of the new stealth, the mixed environment presents a particularly tempting hunting ground for cybercriminals. Keeping track of a patchwork range of technologies and devices can be an enormous IT challenge, and potential chinks in a company's cyber armor can frequently emerge. In a hyper-connected world, one under-protected endpoint is all it takes for a threat to penetrate and, as we've seen above, move laterally throughout the IT estate of its victim.

It's clear that companies need an intuitive, granular, anywhere solution for managing their integrated cyberdefenses, but that may no longer be sufficient for protecting the mixed environment. With NEW Kaspersky Security Console Cloud, we've gone one step further, taking into account the unique texture of our customers' mixed environments by offering free dedicated provisioning (and upgrades).

NEW Kaspersky Security Console Cloud is device- and user-centric, and comes with role-based access control (RBAC) and server hierarchy support. It makes managing Kaspersky security applications for Windows, Linux and macOS a breeze, and comes with hypervisor functionality, and centralized automatic discovery and deployment – ensuring no chinks whatsoever in the cyber armor. Migration from on-premise Kaspersky Security Console is easy, with a migration wizard that offers options for staged and cutover migration (the latter via settings export).

The upside-down iceberg of volume vs cost

The simpler malware storm shows no sign of abating - cybercriminals are still bombarding businesses across the globe with phishing attacks, viruses, Trojans and basic spyware and malware. In fact, these attacks still comprise about 90% of all cyberattacks.

Yet the towering scale of the simpler malware storm obscures this very important, but often neglected, fact: the remaining 10% of attacks, comprised of APTs, cost almost 100 times more per attack than those caused by simpler malware. The average cost of a simpler malware incident is $10,000, compared to $926,000 for an APT incident.

The situation can be compared to an upside-down iceberg – the 90% is fully visible above the water, while the deadly 10% remains sunken and out of sight. The good news is that we don't need to neglect the 90% in order to turn our attention to the deadly 10%. In a test by **AV-Test** (October 2019), Kaspersky Endpoint Protection for Business achieved a perfect 100% detection rate for fileless threats, and the highest prevention rate of 14 vendors, at 94.12%.

Neglecting the hidden 10% is not an option, and incident response and remediation costs after an APT attack are not only financially destructive, but also a clear case of shutting the stable door long after the horse has bolted.

Viewing the threat iceberg as divided into two (albeit unequal) portions is also unnecessary – in fact, when it comes to the daily security operations of any company, there need be no division whatsoever. Both categories of threat have the same ultimate target in mind – it's only the devilishness of the techniques (and the level of cost and damage) that vary.

Failure to protect adequately against the simpler threats represented by the 90% above the water can result in death by a thousand cuts. Even the most basic attacks can cause exhaustion and feel like a war of attrition, especially when IT budgets are tight and security experts are hard to recruit and retain. Kaspersky Endpoint Security for Business removes the burden of fighting off a wide range of threats, freeing businesses to focus on APTs and other more evasive attacks. Meanwhile, Kaspersky Sandbox collaborates seamlessly with Kaspersky Endpoint Security for Business, by automatically blocking modern stealthy threats.

For the 10% of attacks that lurk beneath the water's surface, endpoint detection and response is essential. Some businesses find it hard to imagine exactly why EDR is so essential in today's threat environment. But if you ask a business that has fallen prey to an APT attack, the business case for EDR is crystal clear: shore up your business's cyberdefenses today to guarantee a safe and profitable tomorrow.

"An integrated package gives you the power to 'properly deploy, operate and get value out of' EDR."

Kuppinger Cole

Tight integration = watertight cyberdefenses

Treating the entire iceberg holistically is straightforward – Kaspersky Endpoint Detection and Response and Kaspersky Sandbox integrate seamlessly with Kaspersky Endpoint Protection for Business, and everything is managed by a single centralized interface – Kaspersky Security Console Cloud – just as it should be. There is no need to switch between divergent systems, or to learn new software management processes – an exhausting prospect given the new stealth threat horizon.

Our industry and customer acclaimed cybersecurity technologies – with EDR at the core – empower you to detect and prevent evasive attacks at lightning speed – with no extra effort from your team.

With the cybersecurity talent gap showing no signs of shrinking, our tightly integrated proactive cyberdefense system makes razor-sharp analysis effortless. Endpoint visibility and automated triage free you to focus your attention on only the most threatening targeted attacks.

Award-winning endpoint protection, automated sandbox and a unified cloud console, work alongside EDR to aggressively defend your IT estate.

Minimize the risks to tomorrow's business growth today.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

kaspersky BRING ON THE FUTURE