



ENJOY SAFER TECHNOLOGY™

ESET TECHNOLOGY

The multi-layered approach and its effectiveness

Document version:

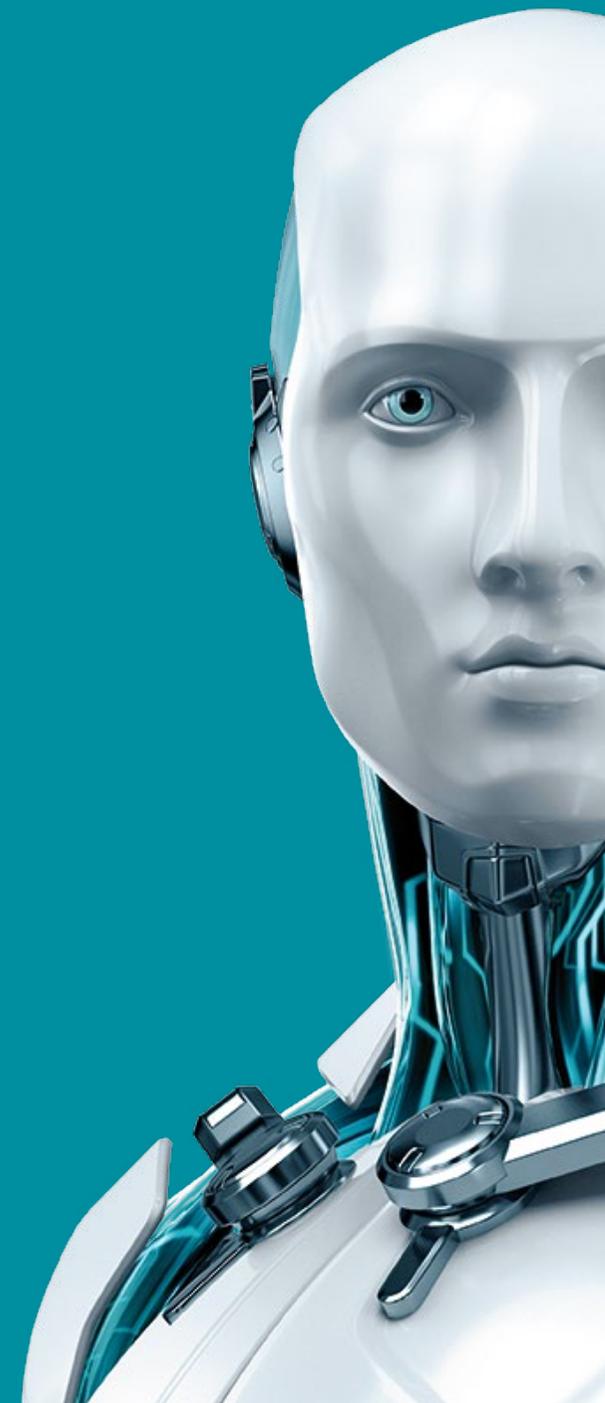
1.1

Authors:

Jakub Debski, Head of Core Technology Development

Juraj Malcho, Chief Research Officer

Peter Stancik, Security Researcher



ESET TECHNOLOGY

The multi-layered approach and its effectiveness

Contents

Objectives	2
Why antivirus is and is not dead	2
Multiple threats, multi-layered protection	3
Multiple threats, multiple platforms	3
Different distribution vectors	3
Malware design	3
The benefits of ESET's core technology	4
Network Attack Protection	5
Reputation & Cache	5
DNA Detections	5
Exploit Blocker	7
Advanced Memory Scanner	7
Cloud Malware Protection System	8
Botnet Protection	8
Automated and Manual Processing of Samples	10
About FPs and IOCs	11
Conclusion	12

Objectives

In this document we summarize the ways in which ESET uses multi-layered technologies to go far beyond the capabilities of basic antivirus. We do this by explaining which layers are involved in solving specific problems and what benefits they provide to the user.

Why antivirus is and is not dead

Most established antivirus companies grew out of a desire to help people who had problems with viruses or malware, and their technology evolved to meet the widening range of threats that security vendors were starting to address. Today, antivirus is perceived as a commodity business and security is a subject that resonates with everyone, whether or not they understand what it actually means. More recently, we have seen a proliferation of new, self-proclaimed “next-generation” companies. These typically have little experience of developing anti-malware solutions, but aggressively market their solutions as “innovative” while dismissing established vendors as “dinosaurs”. As with most silver-bullet salesmen, many of their claims are misleading and, ironically, their detection capability normally relies on a third-party detection engine from an established vendor, since very few of the dozens of solution-providers now in the market have the experience or capacity to enable them to develop their own core detection technology. ESET’s technologies are all proprietary and have been developed in-house.

AV is not dead. However, the simple detection by static signature that – according to newcomers – is compromising the effectiveness of the established anti-malware industry is, if not dead and gone, only a tiny component of the battery of technologies a modern security product deploys against modern threats.

Multiple threats, multi-layered protection

Established anti-malware companies that are still in business today have maintained their market share by evolving to address current threats. These threats are not static and their evolution did not stop in the early 2000s. Today's threats can't be fought effectively by just building on technology from the 1990s. Fighting modern malware is a cat-and-mouse game in which we face teams of skilled and (financially-) motivated bad guys. So security companies need to refine their products constantly, both reactively and proactively, to provide effective solutions, adding different layers by which modern malware can be detected and/or blocked. A single point of protection or a single method of defense is simply not enough. That is one the reasons why ESET too has evolved from an antivirus vendor into an IT security company.

Multiple threats, multiple platforms

Microsoft operating systems are not the only platforms on which malware runs nowadays. The field of combat is changing quickly as attackers try to seize control of previously unexplored platforms and processes.

- Anything that can be controlled to perform malicious activities can be used for attacks.
- Anything that runs executable code to process external data can potentially be hijacked by malicious data.

Linux servers have been a major target for attackers ([Operation Windigo](#), [Linux/Mumblehard](#)), Macs running OS X hosted one of the biggest botnets ever ([OSX/Flashback](#)), mobile phones are common targets ([Hesperbot](#)) and attacks on routers are becoming a serious threat ([Linux/Moose](#)). Rootkits are getting closer to the hardware (attacks on firmware or using the [UEFI rootkit](#)) and virtualization opens new vectors of attack (Bluepill, VM escape vulnerabilities). Also, web browsers and other applications have become as complex as operating systems and their scripting mechanisms are often used for malicious purposes ([Win32/Theola](#)).

Different Distribution Vectors

Historically, the first malware appeared as self-replicating processes, at first within systems and then as file-infecting and/or disk-infecting viruses spreading from PC to PC. As Internet use has become almost universal, so the number of ways of distributing malware has grown enormously. Malicious objects can also be sent by email as attachments or links, downloaded from web pages, dropped by scripts in documents, shared on removable devices, deployed remotely by taking advantage of poor authorization and weak passwords, executed via exploits or installed by end users tricked by social engineering techniques.

Malware Design

The era when malware was written mainly by teenagers as a prank or to show off is long past. Nowadays, malware is written with the aim of monetization or information theft, and serious money is invested in its development by both criminals and governments.

In the hope of making detection more difficult, malware is written in different programming languages, using different compilers and interpreted languages. Code is obfuscated and protected using customized software to make detection and analysis harder. Code is injected into

clean processes in an attempt to avoid behavioral monitoring – which is designed to spot suspicious activity - and to hamper removal, thus ensuring persistence in the system. Scripts are used to avoid application control techniques and “in-memory only” malware bypasses file-based security.

To sneak past protection, the bad guys flood the Internet with thousands of variants of their malware. Another method is to distribute malware to a small number of targets to avoid attracting the attention of security companies. To avoid detection, clean software components are misused or malicious code signed using certificates stolen from legitimate companies, so that unauthorized code is harder to spot.

Also, at the network level malware makes less use of hardcoded command-and-control (C&C) servers to send instructions and receive data from compromised systems. Decentralized control of botnets using peer-to-peer networking is commonly used, and encrypted communication makes identification of attacks harder. Domain generation algorithms reduce the effectiveness of detection based on blocking known URLs. Attackers take control of legitimate websites that have good reputations and even legal advertising services are used to serve up malicious content.

IMPORTANT NOTE

There are many ways that attackers can avoid detection so that a simple, single-layer solution is not enough to provide protection. At ESET we believe that constant, real-time, multi-layered protection is required to assure the highest level of security.

The benefits of ESET's core technology

ESET's scanning engine is at the core of our products and, while the underlying technology has been inherited from “old-style antivirus”, it has been greatly extended and enhanced and **is constantly being developed to cover modern threats**.

The purpose of the scanning engine is to identify possible malware and make automated decisions about how likely the inspected code is to be malicious.

For many years, ESET's performance was based on smart algorithms and manually-crafted assembly code to address performance bottlenecks caused by deep code analysis using the sandboxing technology integrated into the product. However, we have improved this approach. Now, for maximum performance, we use **binary translation together with interpreted emulation**.

With **in-product sandboxing** you have to emulate different components of computer hardware and software to execute a program in a virtualized environment. These components can include memory, the file system, operating system APIs and the CPU (central processing unit).

In the past the CPU was emulated using bespoke assembly code. However it was an “interpreted code”, which means that each single instruction had to be emulated separately. With binary translation you execute emulated instructions natively on a real CPU. This is many times faster, especially in the case of loops in the code: introducing multiple looping is a protective technique common to all executables where measures have been applied to protect them from analysis by security products and researchers.

ESET products analyze hundreds of different file formats (executables, installers, scripts, archives, documents and bytetimes) in order to accurately detect embedded malicious components.

The figure below shows various core ESET technologies and an approximation of when and how they can detect and/or block a threat during its lifecycle in the system:

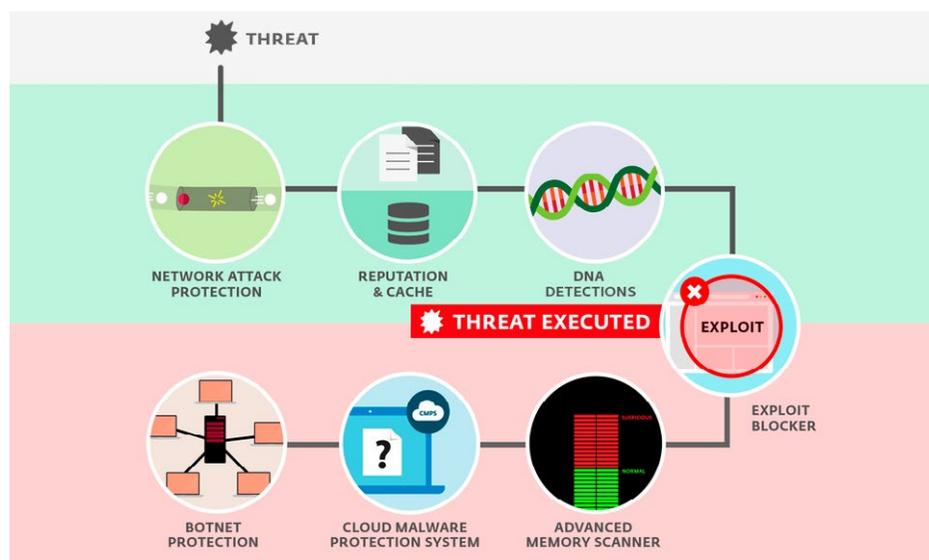
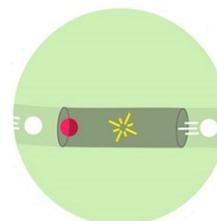


Fig. 1: ESET layers of protection

Network Attack Protection



Network Attack Protection is an **extension of firewall technology** and improves detection of **known vulnerabilities on the network level**. By implementing detection for common vulnerabilities in widely used protocols, such as [SMB](#), [RPC](#) and [RDP](#), it constitutes **another important layer of protection** against spreading malware, network-conducted attacks and exploitation of vulnerabilities for which a patch has not yet been released or deployed.

Reputation & Cache



When inspecting an object such as a file or URL, before any scanning takes place our products check the local cache (and **ESET Shared Local Cache**, in the case of ESET Endpoint Security) for known malicious or whitelisted benign objects. This **improves scanning performance**. Afterwards, our **ESET LiveGrid® Reputation System** is queried for object **reputation** (i.e. whether the object has already been seen elsewhere and classified as malicious or otherwise). This **improves scanning efficiency and enables faster sharing of malware intelligence with our customers**. Applying URL blacklists and checking reputation prevents users from accessing sites with malicious content and/or phishing sites.

DNA Detections



Detection types range from very specific hashes (useful, for example, in targeting specific malicious binaries or specific versions of malware, for statistical purposes or simply to give a more precise detection name to malware that we have previously detected heuristically) to **ESET DNA Detections, which are complex definitions of malicious behavior and malware characteristics**.

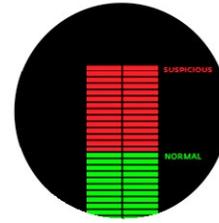


Exploit Blocker

ESET technologies protect against various types of vulnerability on different levels: our scanning engine covers exploits that appear in malformed document files; Network Attack Protection targets the communication level; and finally, Exploit Blocker blocks the exploitation process itself.

Exploit Blocker monitors typically exploitable applications (browsers, document readers, email clients, Flash, Java, and more) **and** instead of just aiming at particular [CVE identifiers](#) **it focuses on exploitation techniques**. Each exploit is an anomaly in the execution of the process and we look for anomalies that suggest the presence of exploitation techniques. As the technology is under constant development, new methods of detection are added regularly to cover new exploitation techniques. When triggered, the behavior of the process is analyzed and, if it is considered suspicious, **the threat may be blocked immediately on the machine**, with further attack-related metadata being sent to our ESET LiveGrid cloud system. This information is further processed and correlated, which **enables us to spot previously unknown threats and so called zero-day attacks**, and provides our lab with valuable threat intelligence.

Exploit Blocker adds another layer of protection, one step closer to attackers, by using a technology that is completely different from detection techniques that focus on analyzing malicious code itself.



Advanced Memory Scanner

Advanced Memory Scanner is a **unique ESET technology** which effectively **addresses** an important issue of modern malware – heavy use of **obfuscation and/or encryption**.

These malware protection tactics, often used in run-time packers and code protectors, cause problems for detection approaches which employ unpacking techniques such as emulation or sandboxing. What's more, whether checking is done using an emulator or virtual/physical sandboxing, there is no guarantee that during analysis the malware will display malicious behavior that will allow it to be classified as such. Malware can be obfuscated in such a way that not all execution paths can be analyzed; it can contain conditional or time triggers for the code; and, very frequently, it can download new components during its lifetime. To tackle these issues, Advanced Memory Scanner monitors the behavior of a malicious process and scans it once it declocks in memory. This complements the more traditional functionality of pre-execution or on-execution proactive code analysis.

Also, clean processes can suddenly become malicious because of exploitation or code injection. For these reasons, performing analysis just once is not enough. Constant monitoring is needed, and this is the role of Advanced Memory Scanner. **Whenever a process makes a system call from a new executable page, Advanced Memory Scanner performs a behavioral code analysis using ESET DNA Detections.**

Code analysis is performed not only for standard executable memory but also for .NET MSIL (Microsoft Intermediate Language) code used by malware authors to hamper dynamic analysis. Due to the implementation of smart caching, Advanced Memory Scanner has almost no overhead and doesn't cause any noticeable deterioration in processing speeds.

Advanced Memory Scanner cooperates well with Exploit Blocker. Unlike the latter, it is a post-execution method, which means that there is a risk that some malicious activity could have occurred already. However, **it steps into the protection chain as a last resort** if an attacker manages to bypass other layers of protection..

Moreover, there is a new trend in advanced malware: some malicious code now operates as “in-memory only”, without needing persistent components in the file system that can be detected conventionally. Initially, such malware appeared only on servers, due to their long uptime – since server systems stay up for months or years at a time, malicious processes could remain in memory indefinitely without needing to survive a reboot – but recent attacks on businesses indicate a change in this trend, and we are seeing endpoints also targeted in this manner. **Only memory scanning can successfully discover such malicious attacks and ESET is ready for this new trend with its Advanced Memory Scanner.**

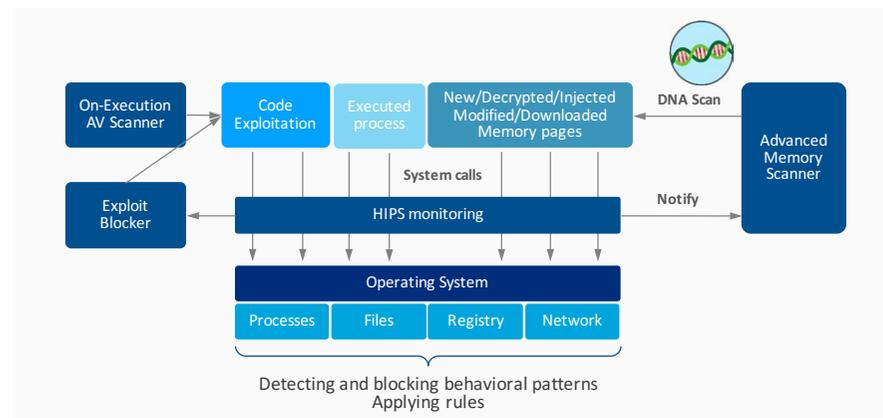
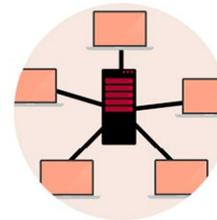


Fig.2: How ESET's behavioral detection works



Cloud Malware Protection System

The ESET Cloud Malware Protection System is one of several technologies based on ESET's cloud-based system, ESET LiveGrid. Unknown, potentially malicious applications and other possible threats are monitored and submitted to the ESET cloud via the ESET LiveGrid Feedback System. The **samples collected are subjected to automatic sandboxing and behavioral analysis**, which results in the creation of automated detections if malicious characteristics are confirmed. ESET clients learn about these automated detections via the ESET LiveGrid Reputation System without the need to wait for the next detection engine update. The mechanism's turnaround time is typically under 20 minutes, which allows for effective detection of emerging threats even before regular detections are delivered to users' computers.



Botnet Protection

One element of malware that is expensive for its authors to change is communication with C&C servers. **ESET's Botnet Protection is proven to successfully detect malicious communication used by botnets, and at the same time identify the offending processes.**

ESET's Network Detections extend Botnet Protection technology to address general problems associated with network traffic analysis. They **allow for faster and more flexible detection of malicious traffic**. Industry-standard signatures like Snort or Bro allow detection of many attacks, but ESET Network Detections are specifically designed to target network vulnerabilities, exploit kits, and communication by advanced malware in particular.

The ability to perform network traffic analysis on endpoints has additional advantages. It allows us to identify exactly which process or module is responsible for malicious communication, allows action to be taken against the identified object, and sometimes even allows the communication's encryption to be bypassed.

Reactive vs proactive protection today

While DNA Detections are excellent for detecting even whole malware families, they must be distributed to users in order to protect them. The same is the case for the scanning engine, heuristics or any change targeting new threats. Nowadays, communication with ESET's cloud-based LiveGrid system is needed to ensure the highest level of protection for many reasons:

- **Offline scanning is mostly reactive.** Being proactive nowadays no longer means just having the best heuristics in your product. As long as your protection tools are available to an attacker, it does not matter if you are using signatures, heuristics or machine learning classifiers: a malware author can experiment with your detection technology, modify the malware until it is not detected, and only then release it. ESET LiveGrid counters this malware strategy.
- **Updates are not real-time.** Updates can be released more often, and can even be pushed to users every few minutes. But can this be done better? Yes: ESET LiveGrid enables instant protection, by providing information whenever it is needed.
- **Malware tries to fly under the radar.** Malware authors, especially in the case of cyber espionage, try to avoid detection for as long as possible. Targeted attacks – as opposed to mass distributions such as email worms – deploy single pieces of malware to a small number of targets, sometimes to just one. We use this fact against the malware authors: objects that are not popular and do not have

a good reputation are assumed to be potentially malicious and analyzed in detail either on the endpoint or submitted for detailed automated analysis via our LiveGrid Feedback system. The ESET LiveGrid Reputation System contains information about files, their origins, similarities, certificates, URLs and IPs.

Protection using ESET LiveGrid

The simplest way to provide protection using a cloud system is by exact blacklisting using hashing. This works well for both files and URLs, but it is able to block only objects that match the hash exactly. This limitation has led to the invention of fuzzy hashing. Fuzzy hashing takes into consideration the binary similarity of objects, as similar objects have the same or a similar hash.

ESET has moved fuzzy hashing to the next level. We do not perform hashing of data but hashing of the behavior described in DNA Detections. Using DNA hashing we are able to block thousands of different variants of malware instantly.

Unique files detected by DNA hashes

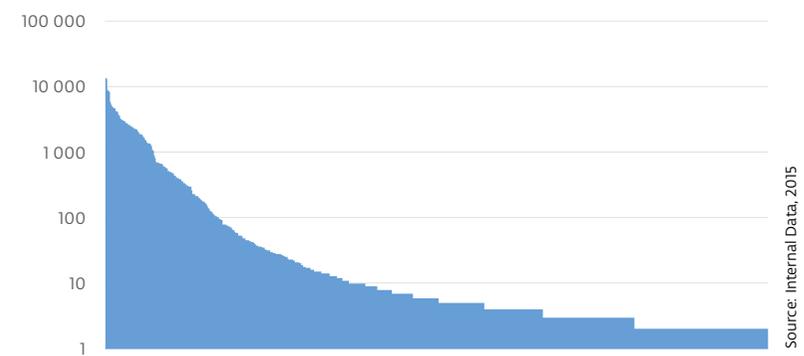


Fig.3: Number of unique files (y-axis) detected by individual DNA hashes (x-axis).

Providing instant blacklisting to users is not the only purpose of the ESET Cloud Malware Protection System. If a user decides to participate in the sample submission process, whenever a new sample with questionable reputation is identified it is sent to ESET for deep analysis. To make use of the full potential of the Cloud Malware Protection System, users should also enable the ESET LiveGrid Feedback System, which allows us to collect any suspicious samples with questionable reputation in order to conduct deep analysis.

Automated and Manual Processing of Samples

Every day, ESET receives hundreds of thousands of samples, which are processed automatically, semi-automatically and manually after preprocessing and clustering. **Automated analysis is performed by internally developed tools on an array of virtual and real machines.** Classification is performed using different attributes extracted during execution, according to static and dynamic code analysis, changes introduced to the operating system, network communication patterns, similarity to other malware samples, DNA features, structural information and anomaly detection.

All automated classifiers have drawbacks:

- **Choosing discriminator features for classification is not trivial** and must be performed using the knowledge of humans who are experts in the field of malware.
- **Machine learning classifiers require the participation of human experts** to verify the inputs used for learning. With fully automated processing, where samples classified by the system would be used as inputs to the system, a snowball effect from the positive feedback loop would quickly make it unstable. “Garbage in – garbage out”.

- Machine learning algorithms do not understand data and **even if information is statistically correct that does not mean it is valid.** For example, machine learning cannot distinguish new versions of clean software from malformed versions, cannot distinguish an updater linked to a clean application from a downloader used by malware, and cannot recognize when clean software components are used for malicious purposes.
- With machine learning, adding new samples to a learning process may cause false positives, and removing false positives may reduce the effectiveness of true positive detection.
- While automated processing allows instant responses to new threats by detection through ESET LiveGrid, additional processing of samples by detection engineers is crucial for assuring the highest quality and detection rate, and the lowest number of false positives.

Reputation services

ESET LiveGrid also provides reputation for objects. We judge the reputation of various entities including files, certificates, URLs and IPs. As described above, reputation can be used to identify new malicious objects or sources of infection. There are, however, other uses.

Scanning whitelisting

Scanning whitelisting is a feature that reduces the number of times the scanning engine needs to inspect an object. If we are sure that an object has not been modified and is clean, there is no need to perform a scan at all. This has a very positive impact on performance, and helps make ESET products so unobtrusive. As we say, “the fastest code is the code that does not execute at all”. Our whitelists are constantly adapted to the ever-changing reality of the software world.

Intelligence gathering

If a user decides to participate in sending statistics to ESET LiveGrid we use this information for global tracking and monitoring of threats. This information gives us copious research data to work on and **allows us to focus on the most urgent and problematic cases, observe trends in malware, and plan and prioritize development of protection technologies.**

About FPs and IOCs

Indicators of compromise (IOCs) are perceived as very important in contemporary corporate security, but they are far from special or advanced, even though they are sometimes stressed by "next-gen" security providers. Pictured here is a breakdown of the most prevalent IOCs and what they are based on.* As we can see, the features they address are extremely basic: in one quarter of cases it's about known MD5s, then filenames, etc. These results make it clear that this is not a method suitable for prevention and blocking, although it can be useful for forensics. It is ironic that some of the "next-gen" vendors who dismiss "obsolete" signature-based detections used in "old AV" praise IOCs so highly even though these are actually the weakest signature-based way to detect malicious files or events.

*Data source: IOC Bucket, April 2015. IOC Bucket is a free community-driven platform dedicated to providing the security community with a way to share threat intelligence.

Indicators of compromise

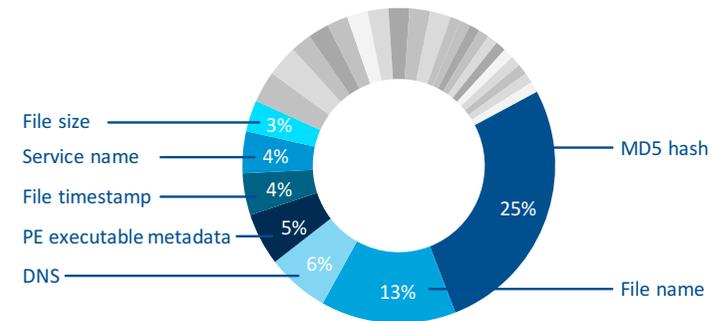


Fig.4: Analysis of indicators of compromise from IOC Bucket (April 2015 sample).

Conclusion

There is no silver bullet in security. Today's malware, being dynamic and often targeted, requires a multi-layered approach based on proactive and smart technologies that take into account petabytes of intelligence gathered over many years by experienced researchers. As far back as 20 years ago, ESET recognized that AV – the traditional approach – was an incomplete solution, at which point we started to incorporate proactive technologies into our scanning engine and gradually implemented different layers of protection to strike at different stages of the cyber kill chain.

ESET is one of the few security vendors able to provide a high level of protection based on more than 25 years of research. This allows us to stay ahead of malware, constantly evolving our technologies to go beyond the use of standard, static signatures. Our unique combination of endpoint-based and cloud-augmented technologies provides the most advanced security against malware on the market.