AFKC
Value-Added Distributor

WHITE PAPER

TARGETED ATTACKS

How to improve detection and respond faster, to stop them before damage is done

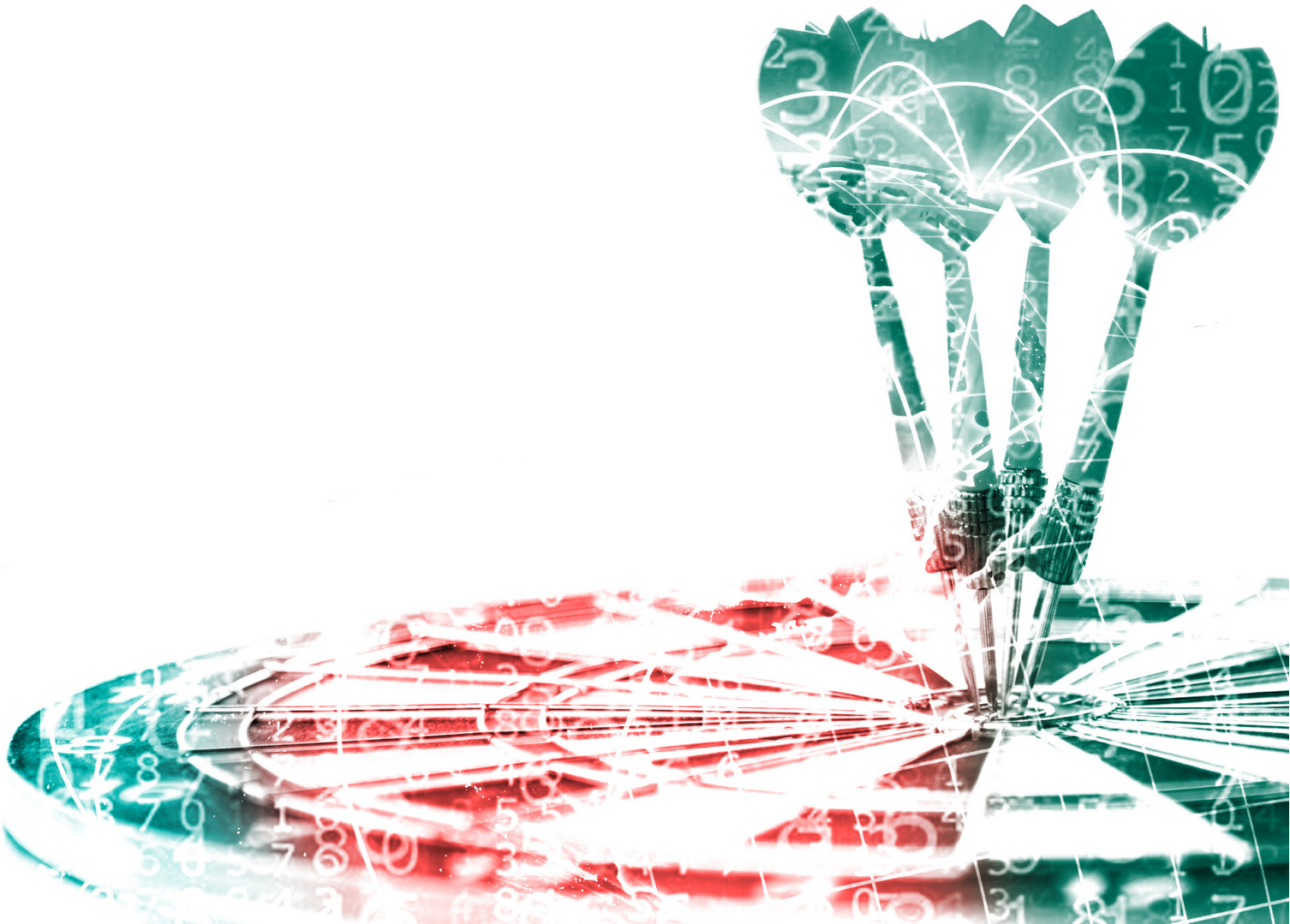


TABLE OF CONTENTS

1. INTRODUCTION

Cybercriminals today have evolved their techniques into more complex attacks. These kinds of threats are generally identified as **Targeted Attacks** and **Advanced Persistent Threats**.

This document is intended to give an overview on how these attacks differ from the others, and provide information on the techniques used to detect and prevent them. In this context, typical Network Security Platforms are insufficient to reveal a targeted attack.

The objective of this whitepaper is to **revert the process of detection through the use of dedicated platforms** aimed to correlate information from threat intelligence and different detection processes.

This is not a purely technical document, but it gives important information to Security Professionals to get introduced to this topic, that is growing in popularity in the businesses.

2. WHAT IS A TARGETED ATTACK?

A t**argeted attack** is designed for the purpose of **hitting a particular target** (corporation, industry, critical infrastructure) **to achieve a specific objective**, which can be to cause immediate economic/reputational damage to the target, or to obtain information (e.g. personal accounts, bank accounts, credit cards, projects, patents, etc.) and then sell them on the dark web or use them for unfair competition purposes.

A targeted attack is generally preceded by a **social engineering activity**, of greater or lesser length and complexity, which is to collect information on the target by, for example, examining its organisational chart, identifying key characters, understanding its ICT and Security infrastructure, analysing services externally, collecting personal data on employees, corporation processes, etc. The goal is to i**dentify which are the weaknesses allowing intruders to break inside**.

Then the attacker chooses specific attack vectors, that may be more than just one (email, compromised websites, gates let unintentionally open on perimeter devices, work places not properly protected or monitored) and inject the malicious code into them. This malicious code is specifically developed for the client infrastructure and thus is not detectable by those security tools which rely on the detection of an unknown code (signatures).

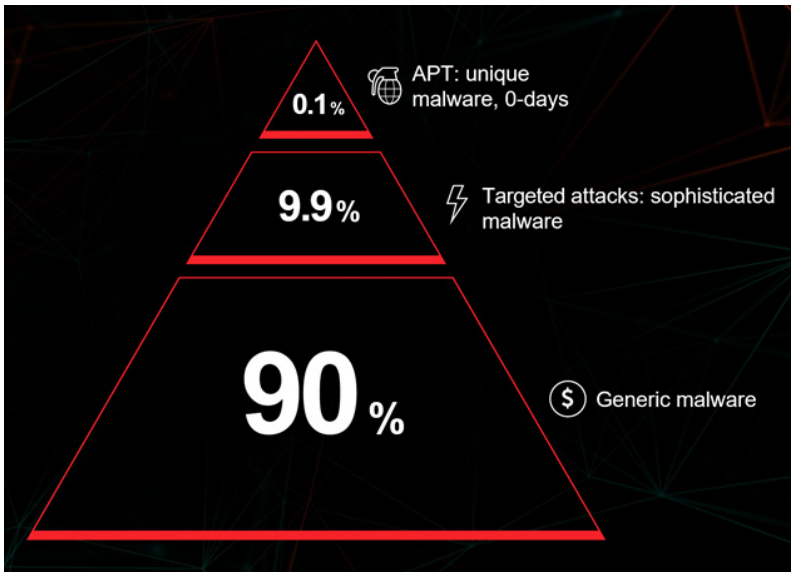
2.1 Targeted Attacks vs APTs

When talking about targeted attacks, it is common to automatically associate them with APTs (Advanced Persistent Threats). Actually, **APT attacks represent just a small percentage (around 1%) of all targeted attacks**.Their main characteristic is to be exclusively designed for information theft.

These attacks are developed to break into the victim's infrastructure, stay dormant for a certain period of time so they are not detected immediately, and only at later let information out with a slow and not repetitive process, until the malicious code is completely released.

An attack of this type requires a longer time and higher realization costs and it is used only for high-interest targets, hard to penetrate and where you don't want to leave a trail.

FIG.1
Distribution of Malware Types



Source: Kaspersky Lab

FIG 2 shows a general scheme of a targeted attack process. Some components may be more or less present depending on the complexity of the attack and on the capacity of identification and analysis of the victim.

Today, organizations need to learn to face constant infiltrations. Keeping Cyber Attackers out of corporation environment has become very challenging and, in some cases, almost impossible, since attacks are customizable and can easily overcome detection instruments for traditional threats and exploit the weaknesses within modern networks..

FIG.2
Process of an ATP attack

Source: Kaspersky Lab

3. TARGETED ATTACKS: THE SCENARIO

As reported in the Verizon DBIR 2017 (Fig.3), 75% of Data Breaches is perpetrated by Actors external to the organizations, while in the remaining 25% we have an internal involvement.

The Banking and Finance sector is not the only target: attackers focus their attention toward other business sectors too, regardless of the organizations' size (FIG. 4).

No one believes it will happen to him.
Until it does.

Most private companies and public organizations have arleady made huge investments in traditional IT security solutions, and especially in preventive security technologies based on the identification of known and common threats - such as malware, data theft, network attacks and others. However, it is interesting to see that in 66% of Data Breaches the main vector was a Malware, which clearly was not detectable by traditional systems, and that in 27% of the cases the Data Breach was detected by third parties, before organizations were even aware of it (Fig. 5).

FIG.3
Main perpetrators of data breach

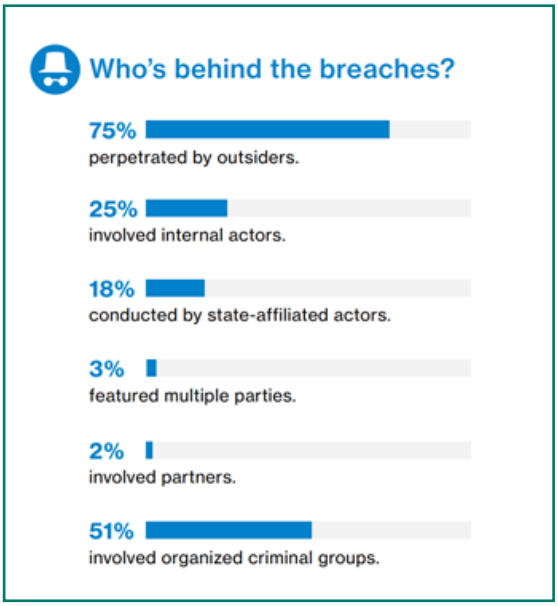


FIG.4
Main victims of data breach

FIG. 3,4 - Source: Verizon DBIR 2017

As we can observe from the last "Kaspersky Security Bullettin: overall statistics for 2017" more than 15 millions of unique Malicious Object (scripts, exploits, executable files, etc.) and about 200 millions of malicious URL between November 2016 and October 2017 have been identified. Geographic distribution of these Malicious Objects and URLs is represented by Fig.6.

During 2017 the Kaspersky Security Network has reported that several zero-day vulnerabilities were actively exploited not only through targeted attacks but also against mass users. Differently from the previous year statistics, exploit for Adobe Flash Player and Internet Explorer vulnerabilities are declining, substituted by Microsoft Office exploit.

FIG.5

Other common elements of data breach

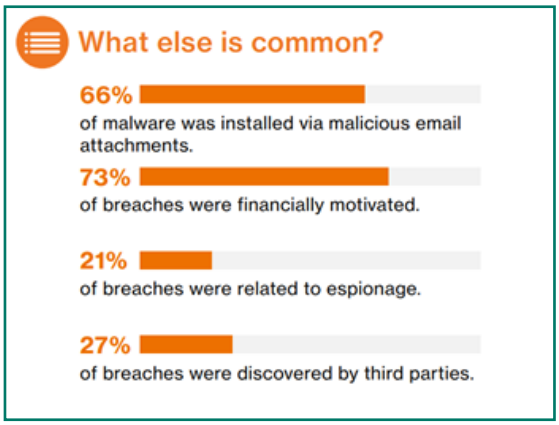
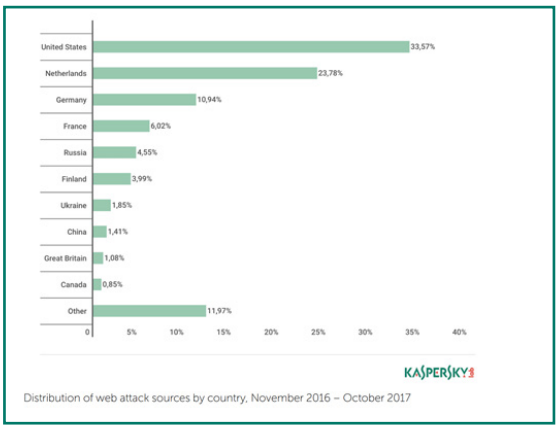


FIG.6

Sources of web attacks for the country



3.1 Why are targeted attacks increasing?

All of the data presented above show that in recent years the number of targeted attacks has risen exponentially, and this is due to a number of factors:

- **Today it has become way easier to collect informations about a company**, also thanks to the many information and communication channels provided by the web: channels like social network, forums, blogs, chats, e-mails, drive in cloud, which are used both by the firm and often by employees in a superficial way.
- There is an **almost complete lack of corporate processes** aiming to raise the awareness between employees on the utilisation of IT and security tools.
- The cost for the development of a unique damaging code on commission (so called MaaS - or Malware-as-a-service) has decreased enormously, as demonstrated by price lists published on the dark web by crime organizations.
- The lack of technology tool able to support corporate Information Security by detecting this type of attacks in a very short time.

4. PREVENTING A TARGETED ATTACK

There is no doubt that factors like the constant evolution of attack techniques, the multiple motivations of attackers and the organizations' increasingly wide attack surface (mainly due to modernization and to the way of conducting business) lead CISO and Security organizations to adopt a new approach to become more able and efficient in detecting and responding to cyberattacks before they turn into damage for the company.

Adopting new abilities, however, can be prohibitive and difficult for security teams, crushed by the lack of personnel and overwhelmed by the continuous expansion of applications, infrastructures and threats. The challenge which most of security teams have to face is to give all issues the right priority, keeping in mind the existing boundaries and, among the multitude of threats existing today, correctly sorting those which are more relevant and crucial.

In order to detect attacks before they switch to a damage, Security Teams are required to reduce the exploitation of passive threat detection techniques, such as signature-based scanning tools. Instead, Security Teams must actively hunt intruders, by constantly looking for every weak signal of dangerous or suspicious activities in their IT environment. To be able to find those first signals, organizations need to adopt new data analysis and incident response skills, as well as:

- Use **intelligence data and information** coming from the **Global Threat Intelligence Security Provider**, to know in advance potential techniques, tactics and attackers
- Acquire **detection tools for advanced attacks** (targeted and APT), capable of using data and intelligence information actively and in real time
- **Extend the digital activities' visibility**, from network infrastructures to end-point
- Using **advanced analysis to discover weak signals and hidden threats**, in order to be able to guide decisions based on the associated risk, and then define the response priority.
- **Detection of signature-less malware**, both on the network and on end-point
- **Improve the investigation process**, through data and information from the Global Threat Intelligence Security Provider
- **Empower security teams** to be more effective through efficient processes, automatic workflows, Threat intelligence and training

There is no solution that allows to prevent with certainty something which differs every time and that has been studied on the specific weaknesses of a company. There are, however, two things companies can do:

1. **Reduce the exposition perimeter to attack:**

   a. by taking action on an organisational and procedural level to regulate the use of corporate communication channels (e-mail, public drives, social networks), in order to limit exposition of corporate information

   b. by Initiating a training process addressed to every employee, with the aim of raise awareness on the use of IT tools, both corporate and private.

2. **Making the incident management process more efficient:**

   a. by exploiting the most updated sources on the major threats in the cyber world

   b. by acquiring an advanced technology platform that allows not only to detect standard attacks, but also to detect targeted attacks in the shortest possible time and to analyse their characteristics in order to adopt more effective countermeasures.

4.1 Characteristics of an Anti- Targeted Attack Platform

In order for a platform to be able to face targeted attacks as described above, it is possible to identify a series of necessary requirements:

- Control of all transmission channels toward the outside of the company, which may constitute a source of attack: network, web, mail.
- Control of processes, memory areas and network traffic of endpoint (server, PC, etc.), to identify the malicious code that is penetrated through peripheral devices.
- Possibility to execute the code (executable, mail attachments, script, etc.) moving through several channels and websites accesses, in a protected and isolated environment.
- Real time gathering of damaging signatures, Hash, IP Address, URL coming from authoritative sources
- Integration of analysis rules customized by the user

- Possibility to extract network traffic and the code which is reported as damaging, in order to allow their analysis by qualified personnel
- Correlation between events coming from single sensors, with the aim of following the evolution of attacks within the infrastructure
- Possibility of transmitting alarms and information to control instruments contained in the corporate SOC (e.g. SIEM)
- Possibility of expansion, both at a vertical and horizontal level, in order to adapt to infrastructural changes or the increase in information traffic within the organization.

When designing a solution which aims to face Targeted Attacks and APTs, a particular ly relevant component, if not essential, is the sandbox. The sandbox is devoted to the execution of the malicious code (executable, mail attachments, script, etc.), within a protected and isolated environment. A virtual machine is activated within the sandbox for every executable, preferably using the same OS as the one on the user's system, and the code is executed inside of it. Its behaviour is then analysed (kernel access, access to other executables in memory or in the file system, abnormal traffic on the network, etc.), in order to identify anomalies. At the end of the analysis, the virtual machine is destroyed and the outcome of the analysis is sent to a central component.

To function properly and efficiently, a sandbox needs to have a number of features:

- High computing capacity, in order to execute more virtual machines at the same time, with shortest launch, test and destruction time.
- Possibility to include more than one sandbox in parallel inside the architecture, to be able to process a greater amount of data
- Possibility to activate virtual machines with different OS, to closely simulate the client infrastructure
- Capacity to not be identifiable by the malicious code: last generation malware are able to recognize if the environment in which they are executed is simulated, and to block or modify their behaviour in order to not being identified.

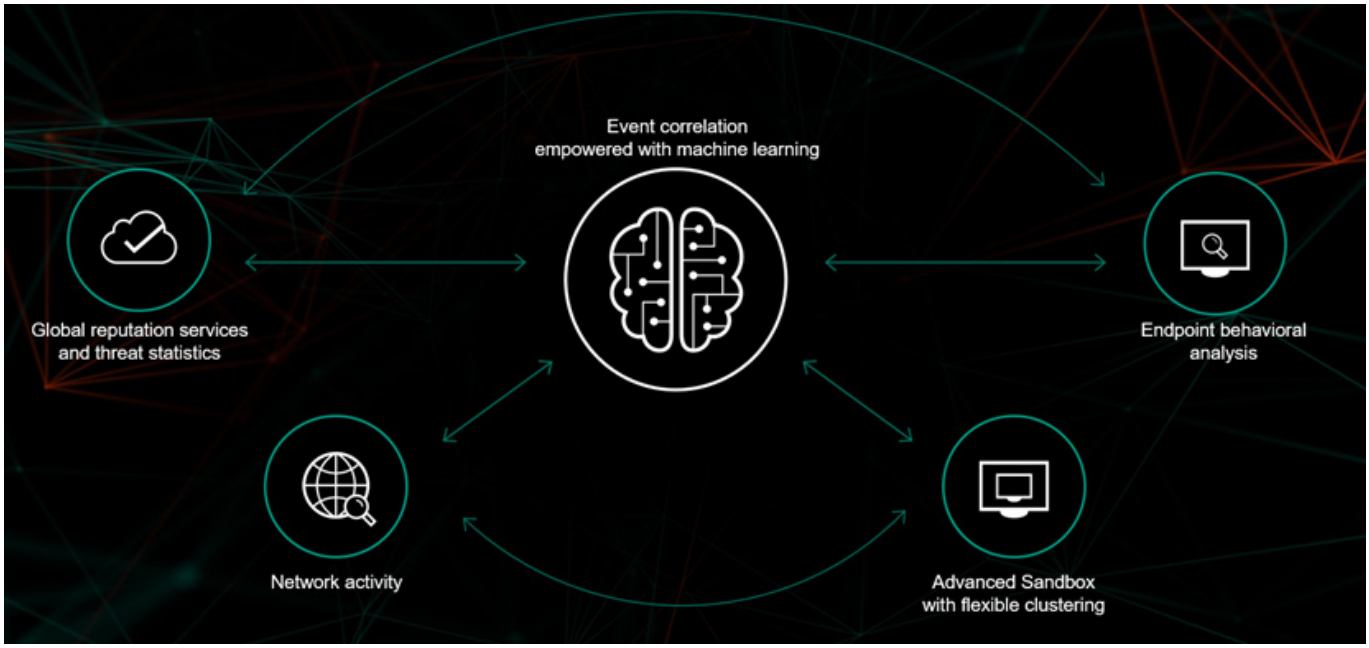
5. KASPERSKY ANTI TARGETED ATTACK (KATA)

Kaspersky Lab's **KATA** is today the most recent and complete solution on the market to fight targeted and APT attacks. It is the direct result of the experience built through years in labs entirely dedicated to the study of all Threats present in the internet world. It combines Machine Learning capabilities, Threat Intelligence, Network traffic analysis and Endpoint behaviour.

Kaspersky Lab chose to design and develop a solution which can be implemented completely at the customer's site, and equipped with all the necessary components to identify damaging activities through all the channels. It is structured in a modular way, to be easily inserted in complex infrastructures.

The architecture can scale on computing capacity, paralleling single module typologies, without the necessity of substituting components with the increase of needs.

FIG.7
Kaspersky Anti Targeted Attack (KATA)

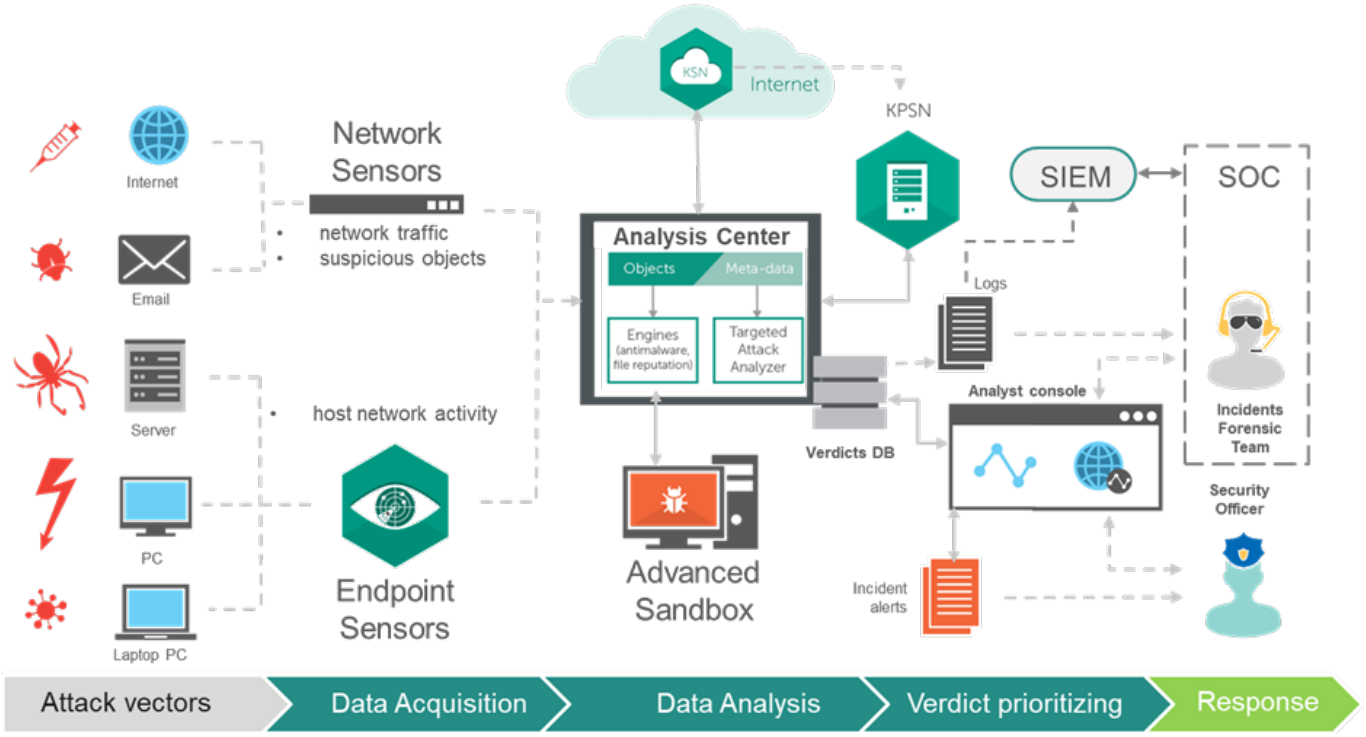


Source: Kaspersky Lab

5.1 KATA's Architecture

The architecture of KATA, as already pointed out, is modular. It includes one module dedicated to the collection of data to be analysed, one dedicated to the data analysis and the sandbox for the execution of the suspect code and one module dedicated to the collection of events, their management, storage and possible export.

FIG.8
KATA - Architettura



Source: Kaspersky Lab

5.2 Data Acquisition

The main attack vectors used by those who design a targeted attack are, as seen above: the network traffic, the traffic linked to Internet browsing, e-mail and endpoints on the customer's network.

How does the solution collect this type of information?

- **Network Sensor:** it is a module that collects:
  - Network traffic, through a SPAN connection with the network devices
  - Traffic related to web browsing, by receiving the ICAP protocol from the proxies server

  - The e-mail traffic, by receiving a copy of the e-mail, or through the POP3 protocol, or using the SMTP protocol and extracting the messages from the SMTP traffic through the SPAN connection

  In KATA's architecture it is possible to can have multiple sensor networks that can perform indifferently any of the functions indicated above

- **Endpoint Sensors:** it is a software agent that is installed on endpoints (server and client), analyses their memory, processes and network traffic, and sends evidence directly to the analysis component.

Within the acquisition component there are two modules dedicated to a primary analysis of the information collected and to the reporting of eventual malware

- A "URL Reputation" module that, by consulting the Kaspersky Data Base in Cloud, verifies that the site is not already reported as containing malicious code
- An "Intrusion Detection" (IDS) module based on the SNORT technology (very widespread on the market) where the user can enter his own customized rules.

5.3 Data Analysis

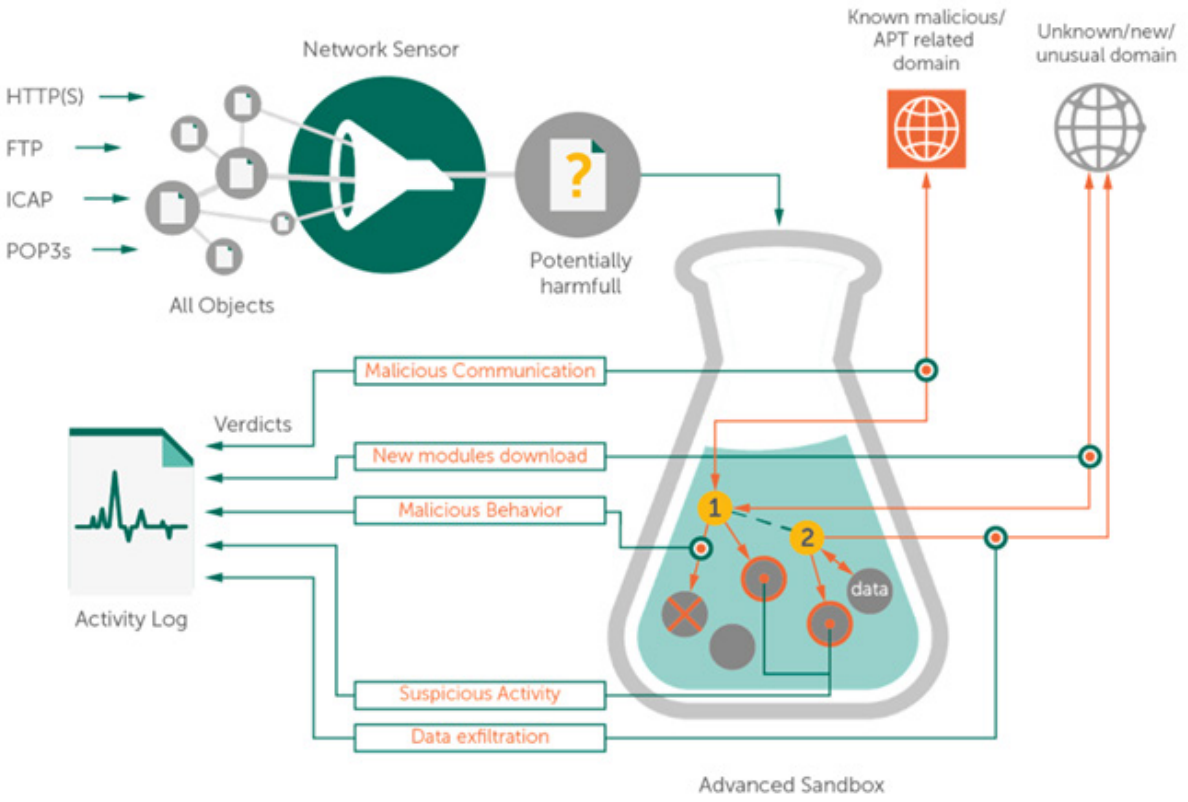
The data analysis component is the heart of the solution; it is based on a series of modules specialized in analysing the traffic collected by the acquisition component. Specifically, within it we can find:

- A module dedicated to the analisys of the correct composition of digital certificates
- A module dedicated to the analysis (through emulation) of applications for Android mobile devices (APK)
- A module containing a "YARA Engine" (anti-malware open source engine) that can be customized with user-entered rules and IoCs
- A module containing an antimalware engine
- An "IP Reputation" module which, consulting Kaspersky Data Base in Cloud, verifies that this is not an IP already reported as malevolent
- A module containing an event correlation engine
- A module containing a "Targeted Attack Analysis" engine devoted to the identification of anomalous behaviours based on the results coming from other modules
- A module that sends the code and the URLs to be analysed to the sandbox.

The sandbox is a component of architecture dedicated to the analysis, in a protected environment and totally isolated from the infrastructure of both executable code (applications, scripts, etc.) and access to websites. The main features of the KATA sandbox are: very high execution speed based on a hypervisor developed ad hoc (therefore also hardly identifiable) that allows you to activate a virtual machine in the order of seconds, with the possibility of analysing the same code in different operating environments simultaneously and with the ability to insert multiple servers (sandbox) in parallel, in order to increase the performance of the solution.

FIG.9

KATA - Advanced Sandbox



Source: Kaspersky Lab

5.4 Response

The "Response" component of the architecture is the one required to perform the following functions:

- Manage the Alerts/Suspicious events through the Incident Management Console
- Investigate on the Incidents through the Threat Intelligence Portal
- Scan of Indicators of Compromise (IoCs) in real time, covering retrospective data from entire network
- Define how the malware is trying to spread inside the infrastructure
- Respond/Blocking to an advanced Threats through EDR
- Sending events to external SOC management platforms like a SIEM (Splunk, QRadar, Arcsight, etc.) or Incident Management Platforms.

5.5 Facts and Figures

KATA platform has been evaluated quarterly and certified by ICSA LAB since December 2016. The results are reported below and the overall report can be downloaded from this link: https://www.icsalabs.com/sites/default/files/FINAL_Kaspersky_ATD_Cert_Testing_Report_20180103.pdf

FIG.10

KATA: ICSA evaluation Results

The KATA platform passed, having met all criteria requirements. As seen in Figure 1 below, Kaspersky's solution did remarkably well during this test cycle - detecting 100.0% of previously unknown threats while having zero false positives. Figures 2 and 3 below further highlight the solution's detection effectiveness and false positives. This is the 3rd consecutive test cycle where the KATA platform had no FPs and 100% efficacy.

Test Length	28 days	**Malicious Samples**	541	**Innocuous Apps**	524
Test Runs	1065	**% Detected**	**100.0%**	**% False Positives**	**0.0%**

Fig. 1 – High Detection Effectiveness & Few False Positives

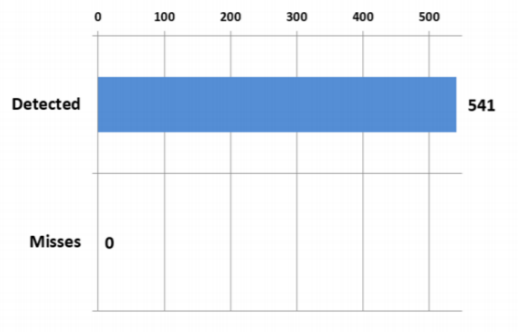


Fig. 2 – Detected 541 of 541 *New & Little-Known* Malicious Samples

Fig. 3 – No Alerts on Innocuous Applications

Source: ICSA Labs

In 2017 we performed several PoC and Deployments on different Customers environment. One of this PoC highlighted exceptional results.

Customer's industry: Financial Sector

Goals of the PoC: Demonstrate that Advanced Threats (APT, Unknown Threats, Non-generic Malware) could have been spotted by KATA where the traditional perimetral Security solutions failed.

Data Acquisition: Corporate Network through SPAN port, Mail System and Proxy Server.

SIEM integration: Splunk

The results achieved at the end of the test period are pictured in the FIG. 11 44.121) - ht

FIG.11

Malicious Events by Threats Category

	EVENT 1	EVENT 2	EVENT 3
Detection Time	26/01/2017	16/01/2017	09/01/2017
# of events	33 events in a few hours of HTTP Get	1 event related to webmail browsing	1 event related to Drive by Download and Data Exfiltration
Compromised Site	XX.XXX.XXX.XXX	XX.XXX.XXX.XXX	"kasdima.top" (213.252.244.121) - https protocol
Source IP	10.xxx.xxx.xxx	10.xxx.xxx.xxx	10.xxx.xxx.xxx
Malicious Event	Download of a 209 KB Trojan File	Email attachment file "invoice_10348.zip" containing "Trojan.Script.Agent.gen"	Command & Control communication by the malware «Rig Exploit Kit (EK)»
Result	The file (which was probably a 0-Day or a variation of a well-known Trojan) couldn't be recognised by the antimalware endpoint solution used by the customer	Detected a Trojan inside the attachment accessed by webmail. The workstation subject to the infection has been reported	Data exfiltration has been detected through the TOP 10 Website Upload, then through KATA further investigation a Botnet communication with C&C has been detected. The Botnet software has been download through an external compromised website

NOTE: Most of these events weren't detected for more than 3 days

6. CONCLUSION

With the adoption of the Kaspersky Anti Targeted Attack solution is possible to achieve the following technical benefits:

- Deeper understanding of threat landscape
- Ability to Detect Threats in Real-Time
- Enhanced visibility into early signs of an attack
- Have effective and efficient tools for detection and investigation
- Increased proportion of self-detected incidents
- Visibility into effectiveness of current controls
- Prioritization of incidents based on potential business impact
- Quickly investigate and validate false positives
- Rapidly conduct root cause analysis

With the following Business outcomes:

- Appropriately funded security incident and response operations
- Lower cost of investigation
- Reduced time to respond
- Better ROI for current security controls
- Less interruption business operations
- Reduce risk of loss of sensitive data (IP, PII, PHI, customer data, financial data, M&A information)
- Maintain or increase reputation of the Security Team
- Minimized unplanned expenses due to incident.

7. WHY AFKC

Despite its recent foundation in 2016, AFKC relies on a team of professionals with many years of experience in Cyber Security and Anti-Fraud

AFKC operates through offices located in Italy and The Netherlands, ensuring a consistent presence on the National and International territory.

Adding our knowledge to Kaspersky Lab's solutions, we are able to help our Partners protect End User's Business, Information and Infrastructures from Advanced Threats, Cyber Attacks and Cybercrime. We work in cooperation with our Partners (System Integrators, Solution Providers, MSPs, VARs and Resellers) offering highly specialized services and dedicated contact persons.

Our Services

SALES ENABLEMENT

PRESALES ENABLEMENT

INTEGRATED SOLUTIONS

EDUCATION

PROFESSIONAL SERVICES

TECHNICAL SUPPORT

AFKC
Value-Added Distributor

CONTACTS

AFKC B.V.

Papendorpseweg 100
3528 BJ Utrecht, Netherlands
+31 030 799 1037
info@afkc.eu

AFKC s.r.l.

Via Fiume Giallo, 3
00144 Rome, Italy
+39 06 522 44040
info@afkc.eu

WWW.AFKC.EU