Kaspersky Threat Attribution Engine

The power of threat attribution

kaspersky

Learn more on kaspersky.com
#bringonthefuture

Biggest cyber heist ever
In February 2016, a group of hackers made an attempt to steal $851 million USD, and did manage to siphon $81 million USD from the Central Bank of Bangladesh.

The attack was conducted by Lazarus – a notorious cyber espionage and sabotage group responsible for a series of regular and devastating attacks. Lazarus is known for attacking financial institutions, casinos, software developers for investment companies and crypto-currency businesses in at least 18 countries around the world since 2009.

While conducting their operations, hackers normally follow a set of tactics, techniques and procedures. Cyber security experts are able to identify threat actors by studying these elements.

Prevention is the best protection: forewarned is forearmed

In our rapidly changing and connected world, computer networks are fundamental enablers of communication, data management and critical infrastructure oversight and control. On the other hand, cyberthreats can also spread around the globe in minutes across the same seamless digital channels. Government organizations and large enterprises are targeted and end up dealing with cyberattacks far more often than they would like to.

Businesses are mainly targeted for countable profit like funds or intangible assets including intellectual property and other valuable information that could be sold on the dark web or used by competitors. National and government organizations find themselves hostage to geopolitical or regional situations and often become targets for espionage operations.

Increased numbers of targeted attacks performed by well-organized threat actors, along with the techniques and resources involved, have taken information security tactics to the next level. At the same time IT security strategy needs to incorporate methods and tools to predict, detect, and defend against cyber threats and espionage under increasing pressure. Moreover, it must contain measures to minimize the impact of security incidents on day-to-day business operations. Finally, any state-of-the-art IT security strategy must also include forensic capabilities to establish the source of an incident, close the existing security gaps and prevent similar incidents from happening in the future.

A standalone division focusing on gathering security related information and dealing with cyber incidents or an outsourced SOC (Security Operations Center) has become a routine business requirement for many organizations. Equipping these with the most advanced cybersecurity services and solutions has turned into a business priority for big corporations and large-scale state institutions.

Kaspersky is now a trusted partner for major CERTs, government bodies and law enforcement agencies around the world, sharing up-to-the-minute knowledge on the latest cyberthreats and helping them to find and implement defense mechanisms. 20 years of cybersecurity experience, the power of globally recognized security experts and several petabytes of constantly updated data on the cyber threat landscape are included in the comprehensive Kaspersky Threat Intelligence Services portfolio.

Why threat attribution?

In August 2016, Kaspersky prevented an attempted cyberattack by the Lazarus group against a bank in a southeast Asian country. When investigating Lazarus' financial attacks Kaspersky researchers were able to identify 150+ different malware samples related to the group's activity.

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Threat intelligence (TI) has true value beyond the current hype around an emerging pocket in the information security industry. TI includes a number of different services that help organizations stay protected, increase awareness and assist with investigations. When it comes to threat intelligence, threat attribution is probably the most visible process and also a point of contention.

And there is a definite reason for this. The average time from detection to response against highly sophisticated threats is usually too long due to complex investigation and reverse engineering processes. Today, in the digital era, organizations are obliged to instantly investigate, prioritize all alerts and accelerate the time to response. Correct and timely attribution helps not only to shorten incident response times from hours to minutes but also to reduce the number of false positives.

Attributing targeted attacks is a powerful and essential tool that:

- Evaluates if you are a target or an unintended victim
- Provides insights into the actors behind the attack and their motivation
- Enables effective detection, investigation, containment and response based on the knowledge of the tactics, techniques and procedures specific to the threat actor

The art of threat attribution

We often hear “attribution is hard”, said either apologetically or half-jokingly. It’s easier than describing the process in detail and explaining that, in fact, attribution consists of a combination of technical indicators, hacker errors, overlaps, and sometimes just plain luck. And we mustn’t forget about the threat actors’ skill in creatively misdirecting researchers. Cyber threat attribution is a resource consuming art.

The classical approach to attribution is a case-to-case analysis based on indicators that require interpretation at every step of the attribution process. There are flags related to software and hardware tools that help to recognize the threat actor during targeted attack research. Let’s take a look at some of the major indicators.

Timestamps

One major benefit of the Portable Execution (PE) format is that compilation times are always included. Though they can be easily altered, many samples have the original timestamps. There are a few important indicators that timestamps can show. Along with obviously indicating the actor’s longevity, timestamps show how the actor’s toolkits evolve over time. When the number of samples belonging to the same actor is relatively large, activity peaks can help identify the time zone where the actor’s team is located.

Strings, debug paths and metadata

Implanted binary code can also expose interesting details about the authors. The artifacts include their preferred language as well as debug paths, which often reveal a username, as well as internal naming conventions for internal tools, projects or campaigns. While the language used rarely discloses the actor’s origin, incorrectly used language, often obtained by using Google translate, whether English or another language, can indicate a false flag. Another telling resource is metadata that might reveal the configuration of the developer’s system.

A good example can be found in the Lazarus case. They started to put Russian keywords (Picture 1) into their malware to confuse the trail and send researchers in the wrong direction. However, the way they used Russian words was strange, and it was easy to see that the Russian text strings were obtained using an online translator.

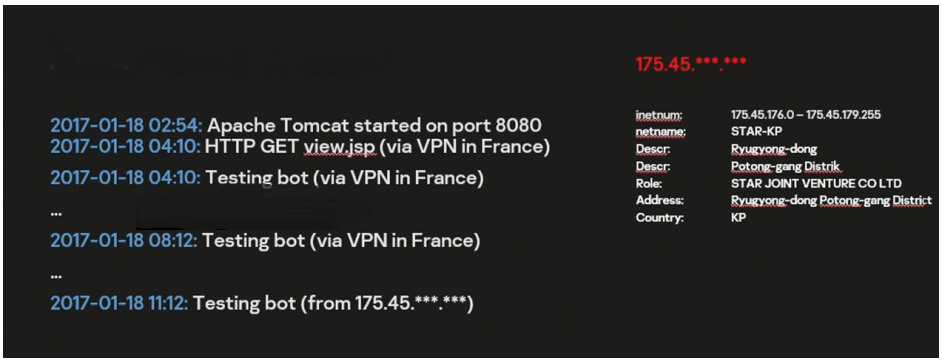
Picture 1. Russian language strings used by Lazarus

Infrastructure and backend

Command-and-control infrastructure can be costly and difficult to maintain, with the added complication that availability may be disrupted by researchers, law enforcement or a spooked system administrator in case of compromised infrastructure.

As a result, even well-resourced attackers tend to reuse command-and-control and phishing infrastructure. For threat intelligence teams building attribution databases, infrastructure reuse is the most telling sign that an attacker is resurfacing or retooling. When attackers retrieve data from the email account of an exfiltration server, prepare staging or phishing servers or check on the availability of a compromised domain, they almost always use an anonymizing service. However, mistakes happen more often than not.

The actor's origin might be revealed, for instance, by looking through the logs of the victim server. Sometimes the VPN was not used for some reason and the attackers' IP address was disclosed, as on the bottom of Picture 2. Everyone knows that there are no VPN services in North Korea. So, the probability of the threat actor behind this attack being North Korean is almost 100%.



Picture 2. From the server logs of C2 in Europe

Exploits

Zero-day exploits are a great source of details about the actor behind an attack. The presence of a "0-day" immediately sets an actor apart from ordinary attackers, thus justifying greater researcher involvement. When a specific implementation of a zero-day appears in separate unrelated instances within a given timeframe (even long-after the zero-day was identified and patched), it signifies code sharing which likely points to the same actor or activity cluster.

In 2015, Kaspersky noted that the Equation Group had used two of the same zero-day exploits prior to their use in Stuxnet. The similar use of both exploits together in different computer worms, at around the same time, indicated that the Equation Group and the Stuxnet developers had either been the same threat actor or had been working closely together.

Toolkit, malware code and password

Although even the most advanced threat actor may rely on publicly available tools, most take time to build their own toolkits, and develop custom backdoors, lateral movement tools, and exploits. In cases where an actor has been exposed or has found other motivations for a top-down retooling, code reuse can indicate a relationship between currently used tools and their predecessors. Coders can be quite lazy and even when the intention is a full retooling, malware developers will often reuse specific functions or pieces of code that have worked well in the past. This means that the zealous researcher may be able to hone in on these traits and connect new campaigns with old ones. This also applies to the reuse of passwords and to hard-coded encryption keys in different malware families or campaigns.

A recent example discovered by Kaspersky experts saw a threat actor deploying droppers with password-protected resources that contained the actual payload in an attempt to thwart sandboxes and automatic detection systems. The hard-coded password protecting the resource was the same even when different, seemingly unrelated malware families were being dropped, thus allowing researchers to tie the two malware families to the same threat actor.

Targeted victim

Though many indicators may be faked or altered, the dynamic between attacker and victim is harder to hide or directly manipulate as it involves 'real-world' publicly known circumstances or geopolitical conflicts. For research teams with skilled analysts, this insight allows for attacker profiling. A possible outcome is the mapping of a campaign to a geopolitical or regional situation that may point in the direction of a given perpetrating organization or nation.

Threat attribution takes time and requires patience

Identifying a targeted attack, profiling the attackers and creating attribution factors for the different threat actors is a long and in depth task; it can take years. Attribution that works is always based on many years worth of previously accumulated data and involves a highly-skilled team of researchers with experience in forensics and investigation.

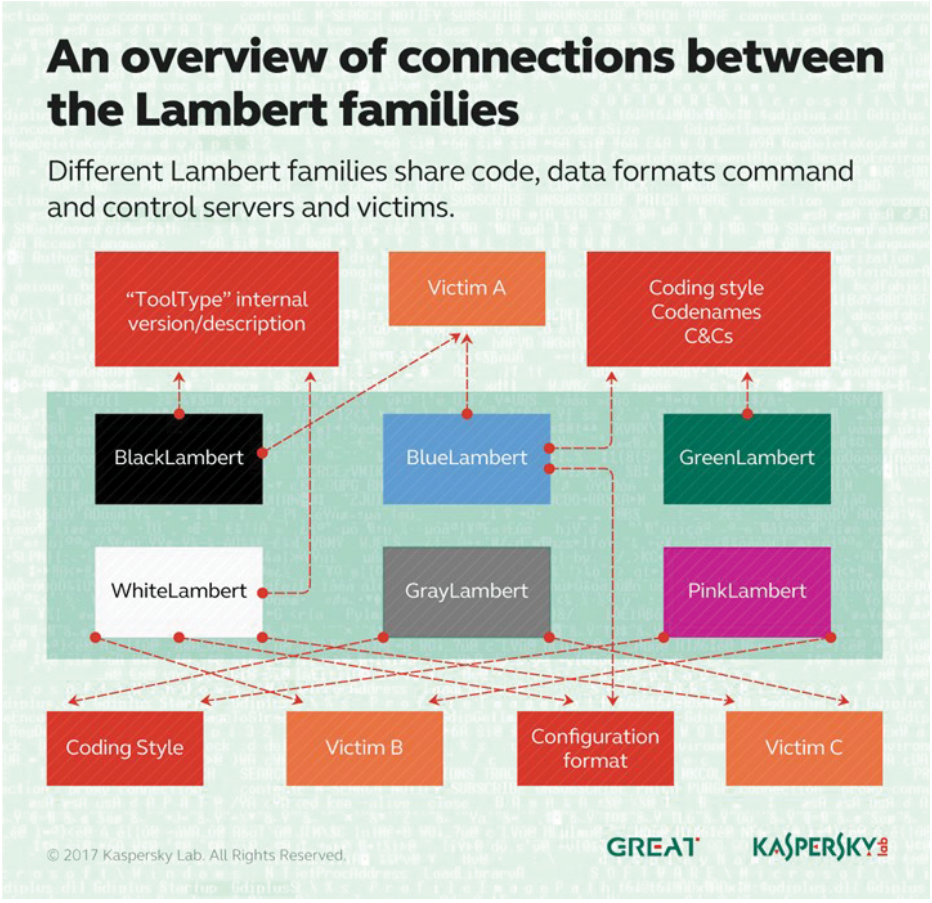
The Lamberts, discovered by Kaspersky, provide a good example of the threat attribution process.

The Lamberts is a family of the sophisticated attack tools that has been used by either one or multiple threat actors against high-profile victims since at least 2008. The Lambert family malware was first disclosed publicly in October 2014 and called Black Lambert. Over the next 3 years 9 implants related to the Lambert family were discovered, with the last one, the so called Brown Lambert, discovered in October 2017.

The threat actor's arsenal includes network-driven backdoors, several generations of modular backdoors, harvesting tools, and wipers. Versions for both Windows and OSX are known at this time, with the latest samples created in 2016.

Two variants of each discovered malware have had at least 1 flag in common: either the "ToolType" version and description, or codenames, or infrastructure, or coding style or configuration format as shown on Picture 3.

In a nutshell, during threat attribution, researchers patiently follow a groups' activity and populate a database with numerous bits of information. Such a database becomes a valuable research tool which can be used as a preventative tool.



Picture 3. An overview of connections between the Lambert families

- 22+ years – observation period
- 60K+ - number of APT malware samples
- 600+ - number of APT actors and campaigns tracked by Kaspersky
- 140+ - number of APT Intelligence reports released every year

Introducing Kaspersky Threat Attribution Engine

Code reuse provides quicker development because possible conflicts and technical issues in existing pieces of code have already been resolved. This is the main reason why reusing code remains so popular in software development, both legitimate and malicious. This in turn means that almost every new attack contains samples from previous ones, and the main challenge is to find the common elements.

Attributing targeted attacks using a database of malware samples remains the most reliable among the existing methods. There is no problem at all when there are unlimited server capabilities to scan over petabytes of data. However, this is obviously not just an inefficient but also an unfeasible solution for most organizations, except maybe Google Inc. or Amazon.

Kaspersky Threat Attribution Engine is a tool that incorporates the database of APT malware samples and clean files gathered by Kaspersky experts for 22+ years. A unique proprietary method of comparing samples and searching for similarities ensures a high attribution rate and brings down false positives almost to zero.

Kaspersky Threat Attribution Engine can quickly link a new attack to known APT malware, actors, campaigns and previous targeted attacks to identify high-risk threats among less serious incidents. The automation of reverse engineering analysis drastically improves malware analysis and incident response times and allows for a timely prioritization of threats. With Kaspersky Threat Attribution Engine, attribution only takes seconds compared to the years that were required in the past.

Kaspersky tracks 600+ APT actors and campaigns with 140+ APT Intelligence reports released every year. Ongoing research ensures the relevance of the APT collection that currently contains 60K+ files. The "digitalization" of Kaspersky APT expertise makes attribution as accurate as possible with an automated tool.

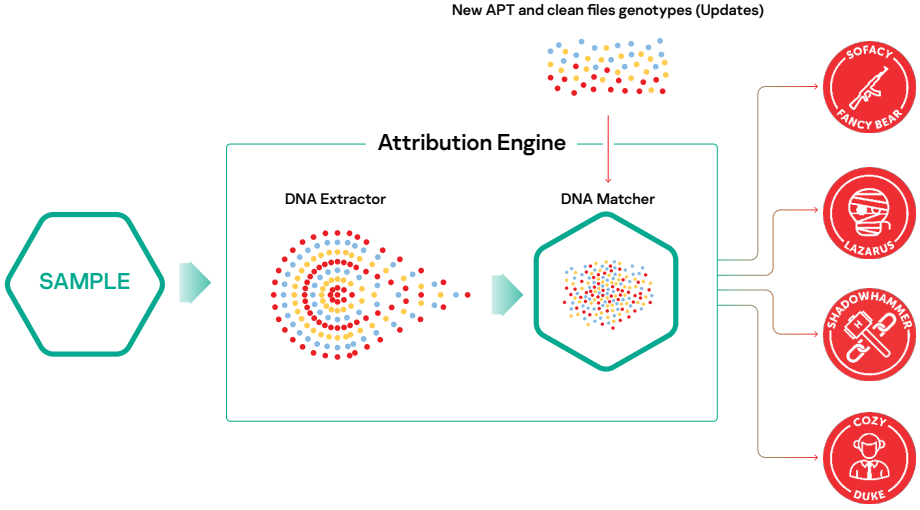
How to educate the Engine on private samples

- Client creates a new actor or campaign for the identified private sample or a collection of samples
- Client uploads the samples and associates them with the threat actor
- Kaspersky Threat Attribution Engine processes the file sample and extracts small pieces of binary code from the decompiled file
- Kaspersky Threat Attribution Engine puts the genotype of the private sample into the private database
- Kaspersky Threat Attribution Engine can now attribute files to this private genotype and the actor

How Kaspersky Threat Attribution Engine works

Kaspersky Threat Attribution Engine automates extraction and analysis of the "genetics" of malware and looks for code similarity with previously investigated APT samples and related actors. It compares the extracted "genotypes", i.e. small pieces of binary code from the decompiled files, with the Kaspersky database of APT malware samples and calculates the file's reputation score. By revealing the sample's genotype and code attribution, **Kaspersky Threat Attribution Engine** provides you with timely insights into the malware's origin and its possible authors.

Kaspersky Threat Attribution Engine supports deployment on Amazon Web Services (AWS) and can be also deployed in a secure, air-gapped environment restricting any 3rd party access to the processed information and submitted objects. There is an enhanced REST API interface to connect the Engine to other tools and frameworks in order to implement attribution into existing infrastructure and automated processes.

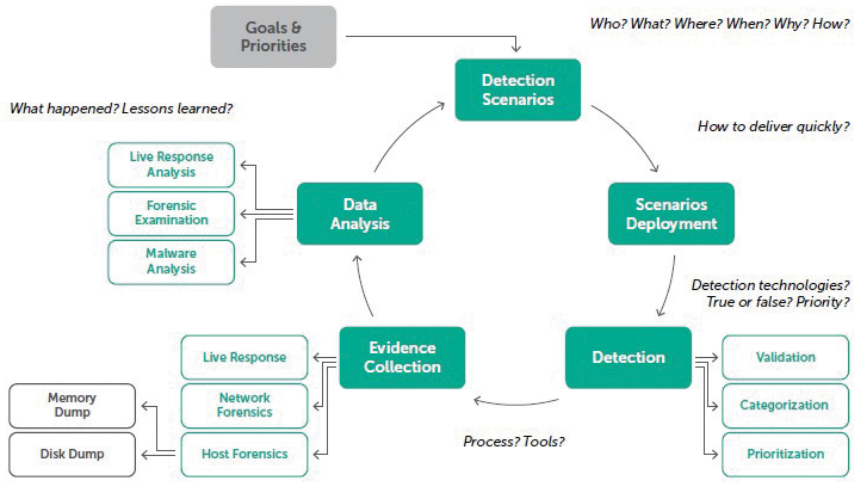


Picture 4. Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine: a member of the Kaspersky portfolio for Security Operations Centers and national cybersecurity agencies

Kaspersky Threat Attribution Engine further extends and strengthens the Kaspersky portfolio for national cybersecurity agencies and commercial Security Operations Centers (SOCs) by supporting them in establishing an effective incident management process.

Each step of an effective incident management process requires technical capability and expertise to answer a specific set of questions, as shown in Picture 5.



Picture 5. Incident management process and related challenges

In an effort to address the challenges that such agencies and SOCs might face while building out incident management capability, Kaspersky provides access to its global expertise and leading technologies:

Question	Specifics	Solutions
Who? When? Why? What? How?	Who are the potential attackers? When were they last seen? What is their motivation? What capabilities do they have? How do they use them?	Having an overview of the current attack surfaces and the trends in malware and hacker attacks targeting your organizations or country allows you to focus your defense strategy on those areas identified as prime targets for cybercriminals. This means you can act quickly and precisely to repel intruders and minimize the risk of a successful attack. **Kaspersky Country-specific Threat Intelligence Reporting, APT Intelligence Reporting and Digital Footprint Intelligence** provide a detailed view of the relevant threat landscape by leveraging various approaches ranging from Open Source Intelligence (OSINT) to deep analysis of proprietary, globally distributed, data gathering and analysis networks, and our extensive expertise and knowledge of the underground cybercriminal communities. **Kaspersky Penetration Testing, Red Teaming and Security Assessment** services will allow you to obtain information on vulnerabilities in key services and components, understand the possible consequences of their exploitation, evaluate the effectiveness of existing security controls, and plan further actions to fix identified flaws and improve security overall.
How to deliver quickly?	How can you quickly distribute detection logic across extensive IT networks? The tools and command-and-control centers used in attacks change rapidly (e.g. the lifespan of a server distributing malware can be only a few minutes), so speed is essential.	Kaspersky technologies and services ensure rapid detection logic delivery: ▪ **Kaspersky Security Network (KSN)** – Kaspersky's global cloud threat reputation database. ▪ **Kaspersky Private Security Network** – a private replica of KSN deployed at the customer's premises. ▪ **Kaspersky Security Center** – a centralized management console for Kaspersky products. ▪ **Kaspersky Threat Data Feeds** - up-to-the-minute and immediately actionable cyberthreat data integrated into existing security controls help mitigate threats more effectively and defend against attacks even before they are launched.

Question	Specifics	Solutions
What detection technologies should we use? How do we assign priority? True or False Positive? Tailored or commoditized?	What technologies should be used for detection? Detection at the endpoint or on the network? Which events should we analyze? How do we decide whether the detection is a True Positive or a False Positive? Is it tailored to my organization?	Kaspersky Sandbox complements Kaspersky Endpoint Security for Business and supports large organizations with distributed networks and CERT constituencies, without the need for information security analysts, to improve defenses against unknown and evasive threats, significantly increasing the number of automatically blocked ones. **Kaspersky Research Sandbox** is the instrument of choice for national digital forensics laboratories requiring detection and analysis of unknown threats without exposing confidential data outside the organization. Cloud deployment option is also available. **Kaspersky Threat Attribution Engine** is based on the biggest repository of APT threats in the industry and quickly establishes links between any new attack to known APT malware, previous targeted attacks and hacker groups helping to ensure timely and effective threat mitigation. **Kaspersky Anti Targeted Attack Platform** is a specialized platform that includes a set of technologies (web analysis, mail traffic analysis, endpoint event analysis, sandboxing), designed for proactive detection of known and new threats. **Kaspersky Endpoint Detection and Response** provides comprehensive visibility across all endpoints on the corporate network, advanced detection of complex threats and simplified automated response with centralized incident management. **Kaspersky Managed Detection and Response** allows proactive threat hunting for isolated networks with one-way inbound data flow, backed by our expertise, ensuring complete integrity and compliance.
How do we collect evidence? What tools should we use?	Effective incident investigation requires a correctly organized process using the right tools. A mistake can lead to highly undesirable consequences causing significant damage, while incorrect conclusions will result in adaptation errors, including setting wrong priorities and expectations.	**Kaspersky Cybersecurity Training** program offers a broad curriculum in cybersecurity topics and techniques, integrating a full range of specific skills, functionalities and competencies into a single body of knowledge. The program has been designed by the recognized experts who helped build our antivirus labs, and who now inspire and mentor the next generation of global experts. **Kaspersky Threat Lookup** is designed to reveal the relationships between various artifacts (hashes, IP address and URLs), boosting incident response and threat hunting activities while providing broader context. **Kaspersky Incident Response** offers all the assistance needed to effectively manage the aftermath of a security breach by bringing the full weight of our expertise onsite to bear on the resolution and mitigation of your cyber security incident.

Kaspersky, the world's largest independent security software company, partners with global law enforcement agencies including Interpol and national CERTs. The company and its products are identified as Leaders by Gartner, Forrester and IDC. The globally recognized team of cyber security experts, extensive threat intelligence portfolio and cloud-based tools monitoring cyberthreats across the globe in real time provide the foundation for undisputed leadership in the field of cybersecurity and make Kaspersky the right partner for national cybersecurity agencies and commercial Security Operations Centers .

www.kaspersky.com