KASPERSKY THREAT INTELLIGENCE SERVICES ANALYSIS

Usmanbayev Doniyorbek Shuxratovich
Muhammad al-Xorazmiy nomidagi Toshkent axborot
texnologiyalari universiteti katta o‘qituvchisi

ABSTRACT

This article presents a classification of Kaspersky Lab's common services in conducting threat intelligence in the field of information security, each of which is substantiated by its type of activity.

Keywords: Kaspersky, threat intelligence, cybercrime, platform, threat intelligence, botnet.

INTRODUCTION

Tracking, analyzing, interpreting, and mitigating ever-evolving IT security threats is a huge undertaking. Businesses across all industries face a lack of up-to-date information needed to help manage the risks associated with IT security threats.

Kaspersky Lab's knowledge, experience, and in-depth intelligence on every aspect of cybersecurity has made it a trusted partner to some of the world's most respected law enforcement and government agencies, including INTERPOL and leading CERTs. You can leverage that intelligence in your organization today.

Kaspersky Lab's threat detection services can give you access to the information needed to mitigate these threats.

Kaspersky Lab Threat Intelligence Services include:

- threat information;
- APT Intelligence Hisoboti;
- Tailored threat reporting;
- Kaspersky Threat Search;
- Kaspersky Phishing Tracking;
- Kaspersky Botnet Tracking;

Threat Intelligence Source

First-tier security vendors and enterprises leverage long-standing and reputable Kaspersky threat intelligence to develop top-tier security solutions or protect their businesses.

Cyberattacks happen every day. Cyber threats are constantly increasing in frequency, sophistication, and confusion as they try to compromise your defenses. Adversaries currently use sophisticated invasion killing chains, campaigns, and customized tactics, techniques, and procedures (TTP) to disrupt your business or harm your customers.

Kaspersky Lab offers constantly updated threat intelligence to keep your business or customers informed of the risks and consequences associated with cyberthreats, helping you to more effectively mitigate threats and protect against attacks before they start.

Rajvedka Zarayoni

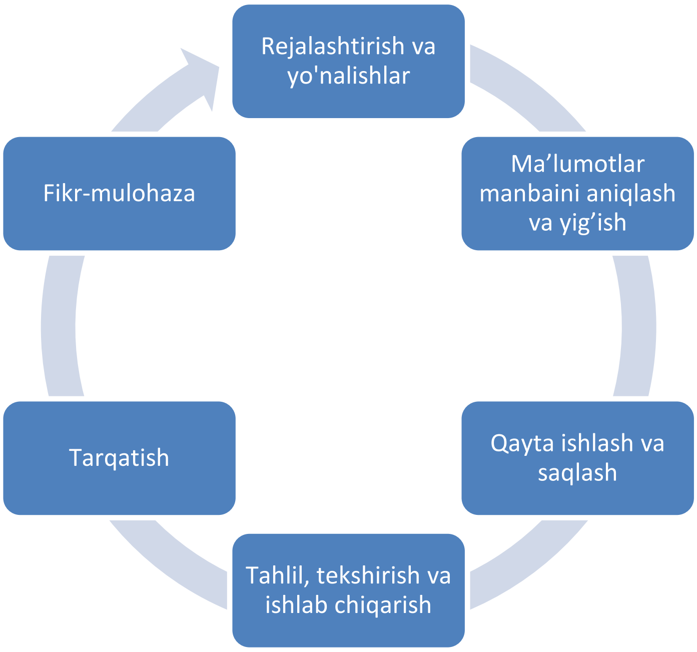

Rejalashtirish va yo'nalishlar
Ma’lumotlar manbaini aniqlash va yig’ish
Qayta ishlash va saqlash
Tahlil, tekshirish va ishlab chiqarish
Tarqatish
Fikr-mulohaza

Figure 1. Kaspersky Threat Intelligence Sources

Today, cybercrime knows no boundaries and technical capabilities are improving rapidly: we are seeing attacks becoming more and more sophisticated, as cybercriminals use dark web resources to threaten their targets. Cyberthreats are constantly growing in frequency, sophistication, and confusion as new attempts are made to compromise your defenses.

Attackers use sophisticated disruption chains and tailored tactics, techniques, and procedures (TTP) in their companies to disrupt your business, steal your assets, or harm your customers.

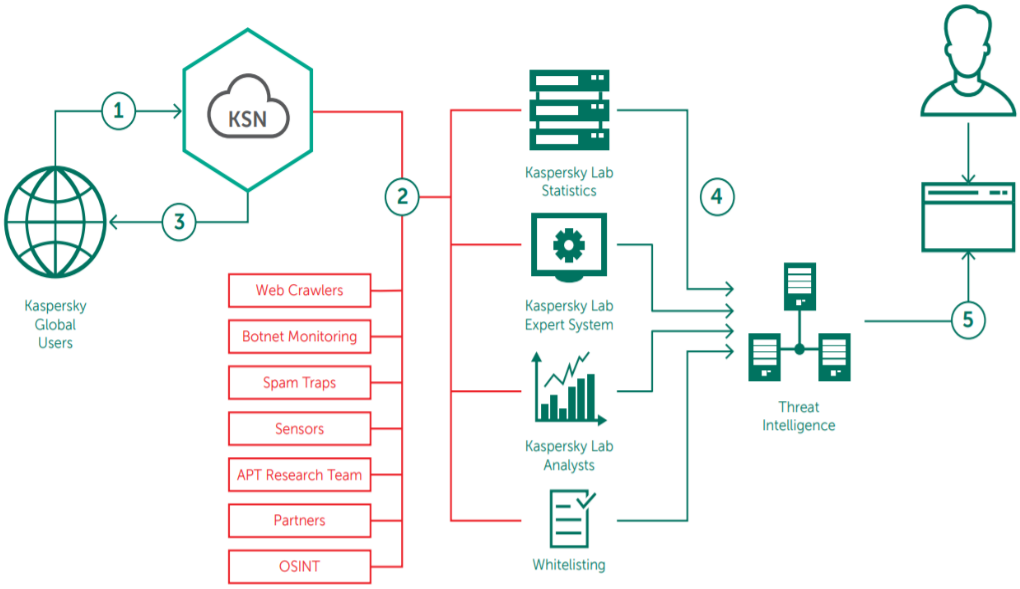


Figure 2. Kaspersky Global Users

Kaspersky Threat Data Feeds the most carefully researched threat metrics data captured from the real world in real time.

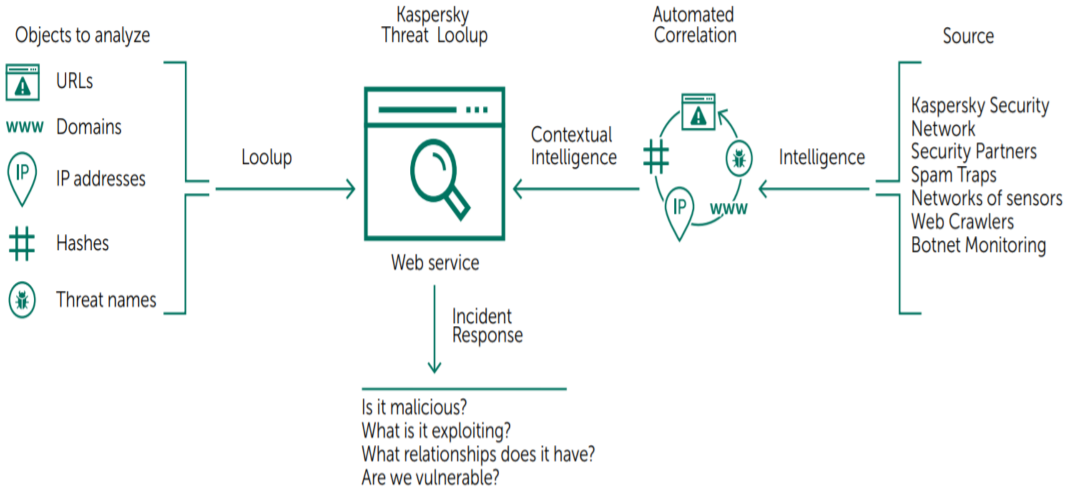
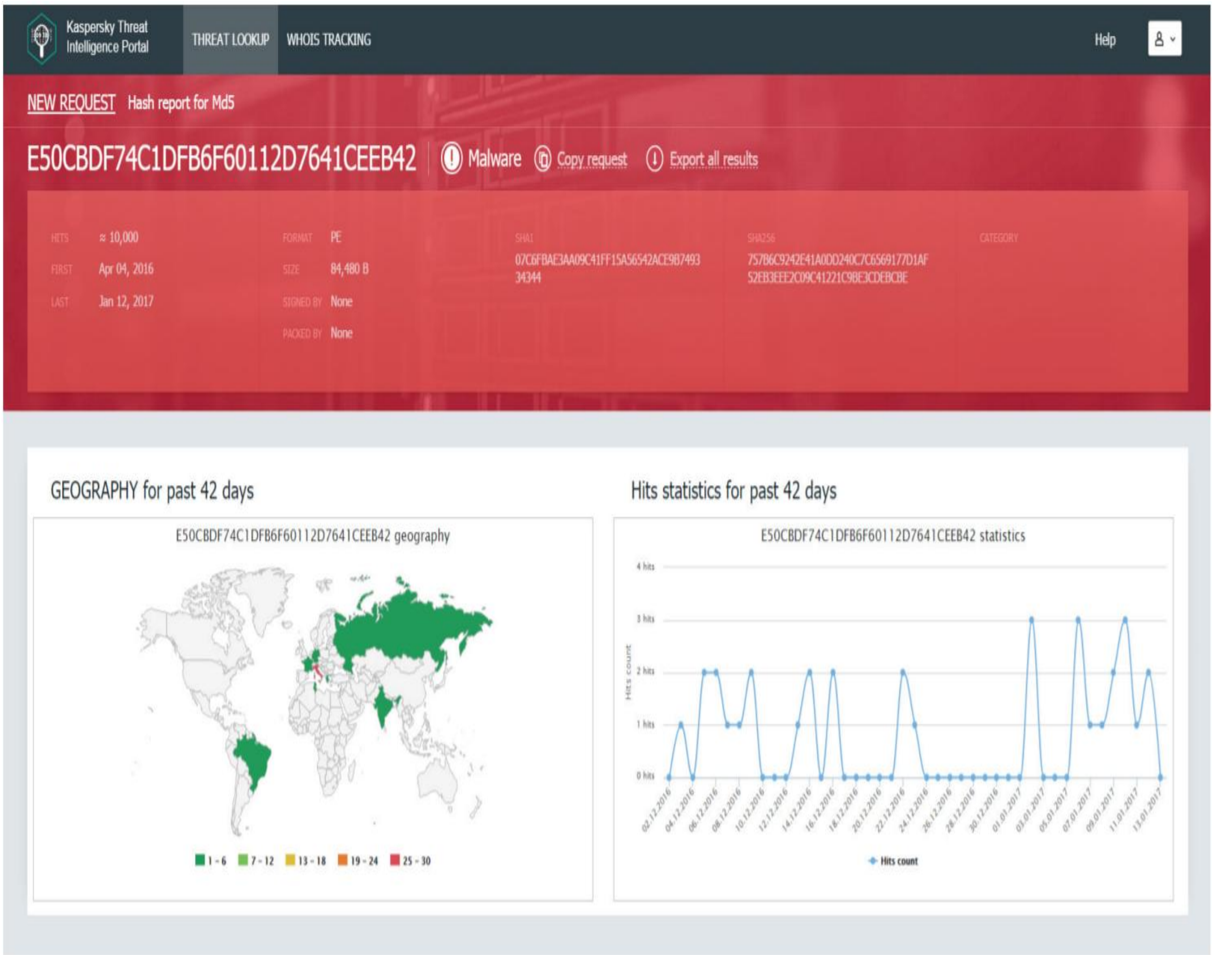


Figure 3. Threat Scanning

Kaspersky Threat Lookup combines all the knowledge gained by Kaspersky Lab about cyberthreats and their contacts into a single, powerful web service. The goal is to provide your security teams with as much information as possible to prevent cyberattacks before they affect your organization.



NEW REQUEST Hash report for Md5

E50CBDF74C1DFB6F60112D7641CEEB42

HITS ≈ 10,000
FIRST Apr 04, 2016
LAST Jan 12, 2017
FORMAT PE
SIZE 84,480 B
SIGNED BY None
PACKED BY None
SHA1 07C6FBAE3AA09C41FF15A56542ACE9B7493 34344
SHA256 757B6C9242E41A0DD240C7C6569177D1AF 52EB3EEE2C09C41221C9BE3CDEBCBE
CATEGORY

4-rasm. Botnet Tracking jarayoni

The platform receives the latest detailed information about URLs, domains, IP addresses, file hashes, threat names, statistics/behavioral information, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps, and more.

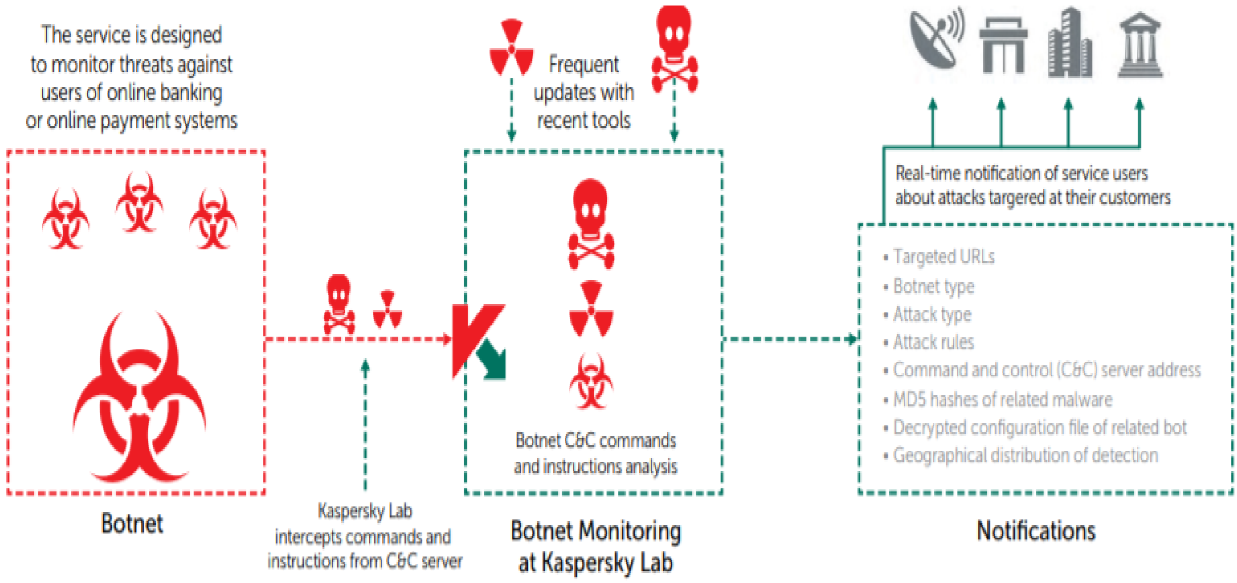

The service is designed to monitor threats against users of online banking or online payment systems
Frequent updates with recent tools
Real-time notification of service users about attacks targered at their customers
Targeted URLs
Botnet type
Attack type
Attack rules
Command and control (C&C) server address
MD5 hashes of related malware
Decrypted configuration file of related bot
Geographical distribution of detection
Botnet C&C commands and instructions analysis
Botnet
Kaspersky Lab intercepts commands and instructions from C&C server
Botnet Monitoring at Kaspersky Lab
Notifications

Figure 5. Expert monitoring and reporting services for botnet detection.

New and emerging threats with global visibility as a result will help strengthen your organization's defenses and incident response.

The threat information provided by Kaspersky Threat Lookup is created and monitored in real time by fault-tolerant infrastructure, ensuring uninterrupted availability and consistent operation.

Use cases / Service benefits:

- Proactive warnings about threats from botnets aimed at online users will always remain the same;
- a Botnet designed for online users Command and Control Server allows you to identify a list of URLs and block them by sending a request to CERT or law enforcement;
- understand the nature of the attack and improve your payment cabinets;
- Teaches your online users to recognize and avoid the social engineering rules used in attacks.

REFERENCES

1. Shukhratovich, U. D. (2023). Machine Learning Methods and Algorithms for Network Intrusion Detection Systems. Eurasian Journal of Engineering and Technology, 14, 87-91.
2. Usmanbayev Doniyorbek Shukhratovich. (2022). Specific features of the structure and operation of network attack detection systems. Open Access Repository, 8(04), 224–228.
3. Jiang, X., Luo, X., & Wang, Z. (2017). Deep learning for network intrusion detection: A review. IEEE Access, 5, 21954-21972.