APT Intelligence Reporting

Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky Lab.

Leveraging the information provided in these reports, you can respond quickly to new threats and vulnerabilities - blocking attacks via known vectors, reducing the damage caused by advanced attacks and enhancing your security strategy, or that of your customers.

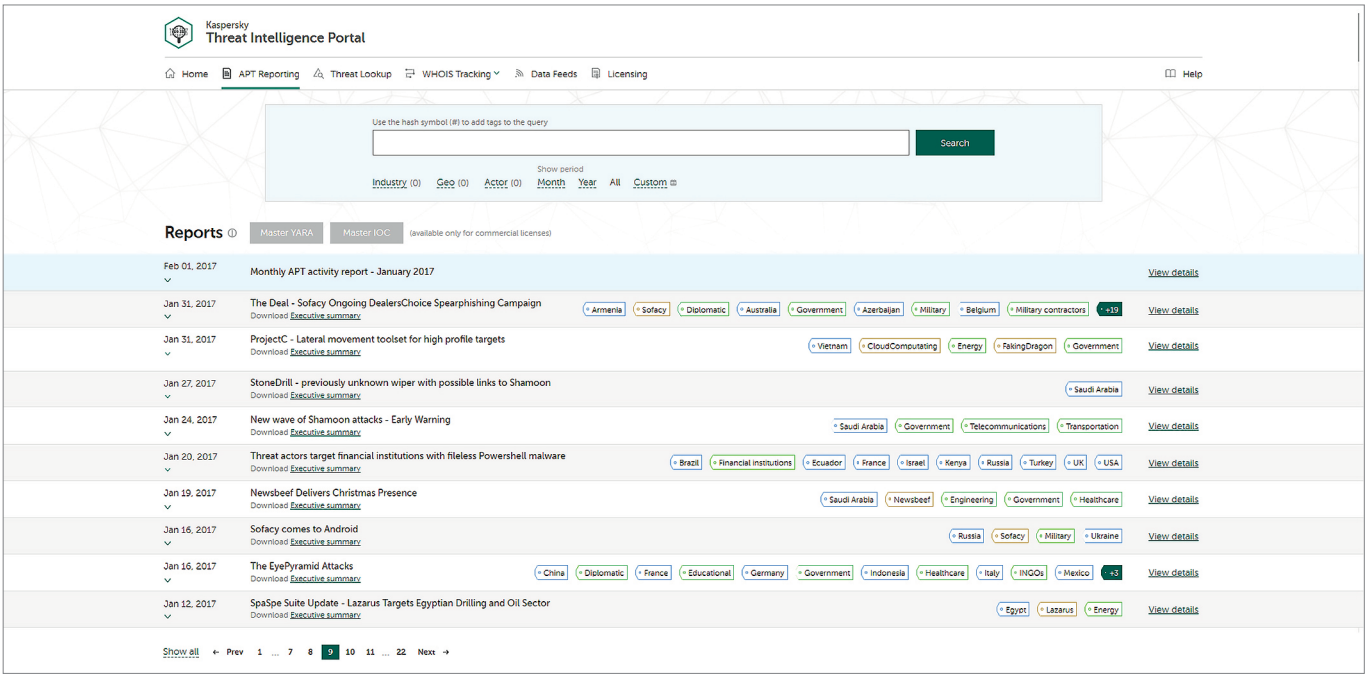
Our experts, the most skilled and successful APT hunters in the industry, will also alert you immediately to any changes they detect in the tactics of cybercriminal groups. And you will have access to Kaspersky Lab's complete APT reports database – a further powerful research and analysis component of your corporate security armory.

Kaspersky Lab has discovered some of the most relevant APT attacks ever. However, not all Advanced Persistent Threat discoveries are reported immediately, and many are never publicly announced. Be the first to know, and exclusively In the Know, with our in-depth, actionable intelligence reporting on APTs.

As a subscriber to Kaspersky APT Intelligence Reporting, we provide you with unique ongoing access to our investigations and discoveries, including full technical data provided in a range of formats, on each APT as it's revealed, including all those threats that will never be made public. During 2016 we have created more than 100 reports!

Kaspersky APT Intelligence Reporting provides:

- **Exclusive access** to technical descriptions of cutting edge threats during the ongoing investigation, before public release.
- **More than 100 reports** have been published in 2016.
- **Insight into non-public APTs**. Not all high profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability fixing process or associated law enforcement activity, are never made public. But all are reported to our customers.
- **Detailed supporting** technical data including an extended list of Indicators of Compromise (IOCs), available in standard formats including OpenIOC or STIX, and access to our Yara Rules.
- **Continuous APT campaign monitoring.** Access to actionable intelligence during the investigation (information on APT distribution, IOCs, C&C infrastructure).
- **Contents for different audience.** Each of the report contains executive summary offering C-level oriented and easy to understand information describing the related APT. Executive summary is followed by a detailed technical description of the APT with the related IOCs and Yara rules giving security researchers, malware analysts, security engineers, network security analysts and APT researchers an actionable advise for superior protection from the related threat.



- **Retrospective analysis.** Access to all previously issued private reports is provided throughout the period of your subscription.

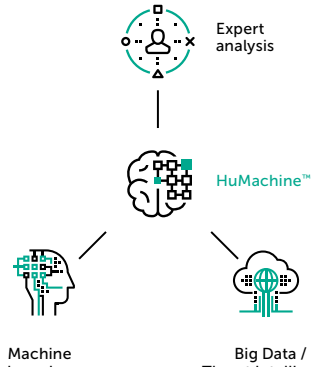
- **APT Intelligence Portal.** All of the reports including most recent IoC's are available via our APT Intelligence Portal creating seamless user experience for our customers. API is also available for the Portal.

Subscription options

- Subscription to full reports on each APT discovered by Kaspersky Lab with related IOCs and Yara rules
- Subscription to executive summaries on each APT discovered by Kaspersky Lab with related IOCs
- Subscription to executives summaries only on each APT discovered by Kaspersky Lab

Note – Subscriber Limitation

Due to the sensitive and specific nature of some of the information contained in the reports provided by this service, we are obliged to limit subscriptions to trusted government, public and private organizations only.



Kaspersky Lab
Enterprise Cybersecurity: www.kaspersky.com/enterprise
Cyber Threats News: www.securelist.com
IT Security News: www.business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.com