kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky. 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 Global Research and Analysis Team (GReAT), recognized worldwide for providing invaluable insights into some of the most notorious threat actor campaigns, continuously reports on tactics and instruments used by cybercriminals in high-profile cyberespionage campaigns with cross-sector targeting, helping to countermeasure even the most sophisticated attacks.

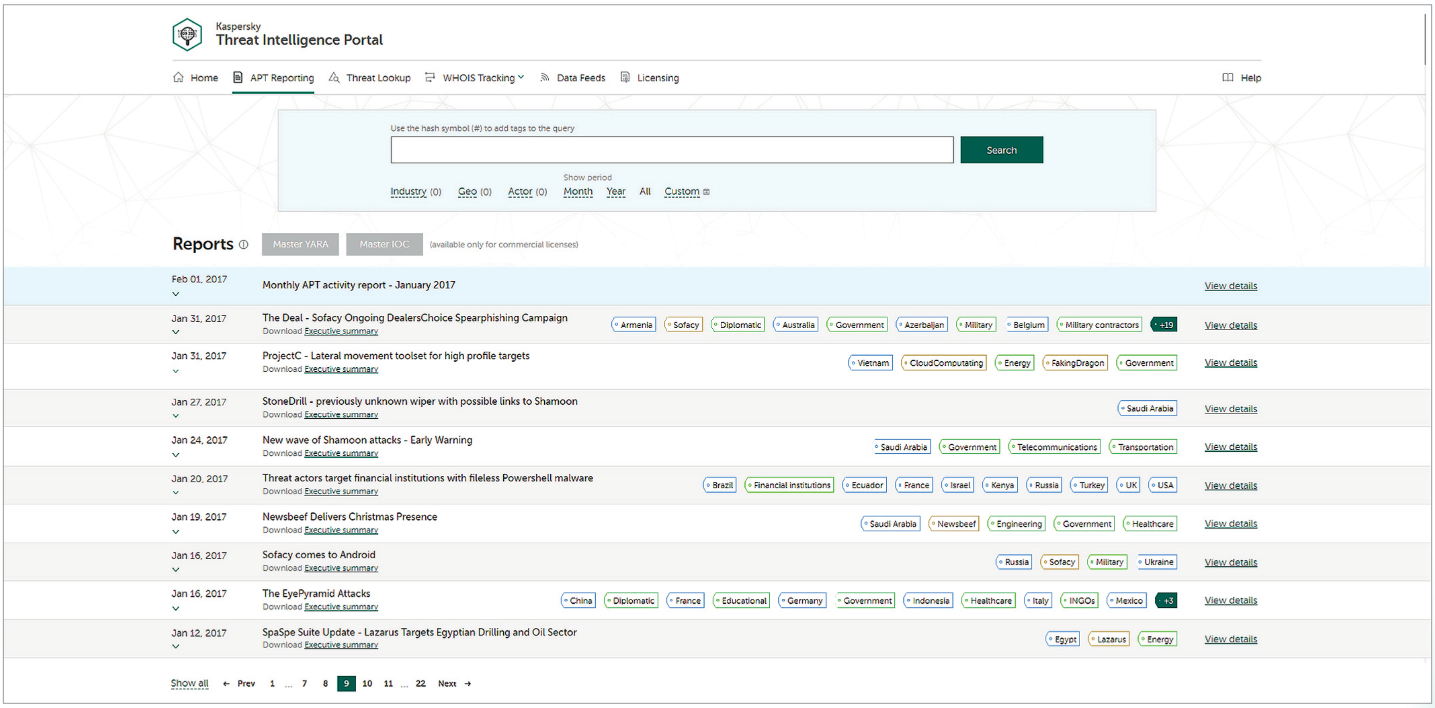
Our experts, the most skilled and successful APT hunters in the industry, will also alert you immediately to any changes they detect in the tactics of cybercriminal groups. And you will have access to Kaspersky's complete APT reports database - a further powerful research and analysis component of your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

Kaspersky 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.

Kaspersky APT Intelligence Reporting provides:

- **Exclusive access** to technical descriptions of cutting edge threats during each ongoing investigation, before public release.
- **Insights 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** access. Includes 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).
- **Addressing technical and non-technical audiences.** Each report contains an executive summary offering C-level oriented and easy to understand information describing the related APT. The 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 actionable data to enable a fast, accurate response to the related threat.
- **Retrospective analysis.** Access to all previously issued private reports is provided throughout the period of your subscription.
- **Threat actor profiles** with summarized information on the specific threat actor, including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with their mapping to the MITRE ATT&CK Framework.
- **MITRE ATT&CK Framework.** All TTPs described in the reports are mapped to the MITRE ATT&CK Framework, enabling improved detection and response through developing and prioritizing the corresponding security monitoring use cases, performing gap analyses and testing current defenses against relevant TTPs.



Kaspersky
Threat Intelligence Portal

Use the hash symbol (#) to add tags to the query

Industry (0) Geo (0) Actor (0)

Show period: Month Year All Custom

Reports

(available only for commercial licenses)

Feb 01, 2017	Monthly APT activity report - January 2017		View details
Jan 31, 2017	The Deal - Sofacy Ongoing DealersChoice Spearphishing Campaign Download Executive summary	Armenia, Sofacy, Diplomatic, Australia, Government, Azerbaijan, Military, Belgium, Military contractors, +19	View details
Jan 31, 2017	ProjectC - Lateral movement toolset for high profile targets Download Executive summary	Vietnam, CloudComputating, Energy, FakingDragon, Government	View details
Jan 27, 2017	StoneDrill - previously unknown wiper with possible links to Shamoon Download Executive summary	Saudi Arabia	View details
Jan 24, 2017	New wave of Shamoon attacks - Early Warning Download Executive summary	Saudi Arabia, Government, Telecommunications, Transportation	View details
Jan 20, 2017	Threat actors target financial institutions with fileless Powershell malware Download Executive summary	Brazil, Financial institutions, Ecuador, France, Israel, Kenya, Russia, Turkey, UK, USA	View details
Jan 19, 2017	Newsbeef Delivers Christmas Presence Download Executive summary	Saudi Arabia, Newsbeef, Engineering, Government, Healthcare	View details
Jan 16, 2017	Sofacy comes to Android Download Executive summary	Russia, Sofacy, Military, Ukraine	View details
Jan 16, 2017	The EyePyramid Attacks Download Executive summary	China, Diplomatic, France, Educational, Germany, Government, Indonesia, Healthcare, Italy, INGOs, Mexico, +3	View details
Jan 12, 2017	SpaSpe Suite Update - Lazarus Targets Egyptian Drilling and Oil Sector Download Executive summary	Egypt, Lazarus, Energy	View details

Subscription options

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

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.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.