Kaspersky APT Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Kaspersky APT Intelligence Reporting customers receive unique ongoing access to our investigations and discoveries, including full technical data (in a range of formats) on every APT as it's discovered, as well as on threats that will never be made public. Reports contain an executive summary offering C-level oriented and easy to understand information describing the related APT together with a detailed technical description of the APT with related IOCs and YARA rules to give security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable data that enables a fast, accurate response to the threat.

Our experts will also alert you immediately to any changes they detect in the tactics of cybercriminal groups. You will also have access to Kaspersky's complete APT reports database, another powerful research and analysis component in your security defenses.

Benefits

MITRE ATT&CK

All TTPs described in the reports are mapped to the MITRE ATT&CK, 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

Information about non-public APTs

For various reasons, not all high profile threats are made known to the general public. But we share them all with our customers

Privileged access

Receive technical descriptions about the latest threats during ongoing investigations, before release to the general public

Retrospective analysis

Access to all previously issued private reports is available throughout your subscription

Access to technical data

Including an extended list of IOCs, available in standard formats including openIOC or STIX, and access to our YARA rules

Threat actor profiles

Including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with mapping to MITRE ATT&CK

Continuous APT campaign monitoring

Access to actionable intelligence during investigation with (information on APT distribution, IOCs, command and control infrastructures, etc.

RESTful API

Seamless integration and automation of your security workflows

www.kaspersky.com