Kaspersky APT Intelligence Reporting

kaspersky BRING ON THE FUTURE

Kaspersky APT Intelligence Reporting

Kunden von Kaspersky APT Intelligence Reporting erhalten exklusiven Zugriff auf unsere Untersuchungen und Entdeckungen, einschließlich vollständige technische Daten (in verschiedenen Formaten) über jedes APT, sobald es entdeckt wird, sowie über Bedrohungen, die nie öffentlich gemacht werden. Die Berichte enthalten Zusammenfassungen, die sich an C-Level-Mitarbeiter richten und einfach verständliche Informationen zum entsprechenden APT enthalten. Der Zusammenfassung folgt eine ausführliche technische Beschreibung des APT mit zugehörigen IOCs und YARA-Regeln. So erhalten Sicherheitsforscher, Malware-Analysten, Sicherheitstechniker, Netzwerkanalysten und APT-Experten praktisch umsetzbare Daten, die eine schnelle, genaue Reaktion auf die Bedrohung ermöglichen.

Unsere Experten alarmieren Sie auch sofort, wenn sie Veränderungen in der Taktik von Cyberkriminellen feststellen. Außerdem erhalten Sie Zugriff auf die vollständige APT-Berichtsdatenbank von Kasperksy, einem weiteren leistungsstarken Forschungs- und Analysebestandteil Ihrer Sicherheitsstrategie.

Vorteile

MITRE ATT&CK-

Alle in den Berichten beschriebenen HTTP-Adressen werden MITRE ATT&CK zugeordnet. Dies ermöglicht eine verbesserte Erkennung und Reaktion durch die Entwicklung und Priorisierung der entsprechenden Anwendungsbereiche der Sicherheitsüberwachung, Schwachstellenanalysen und die Überprüfung der aktuellen Schutzmaßnahmen gegen relevante TTPs.

Informationen über nicht öffentliche APTs

Aus verschiedenen Gründen werden nicht alle komplexen Bedrohungen öffentlich bekannt gemacht. Wir teilen diese jedoch mit unseren Kunden.

Priorisierter Zugriff

Erhalt von technischen Beschreibungen der neuesten Bedrohungen während laufender Untersuchungen, bevor sie an die Öffentlichkeit gelangen

Nachträgliche Analyse

Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit

Zugriff auf technische Daten

Dies beinhaltet eine umfangreiche Liste von IOCs, die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere YARA-Regeln.

Profile von Bedrohungsakteuren

Einschließlich vermutetem Herkunftsland und Hauptaktivität, verwendeter Malware-Familien, angegriffener Branchen und Regionen sowie Beschreibungen aller verwendeten HTTP-Adressen und deren Zuordnung zu MITRE ATT&CK

Kontinuierliche Überwachung von APT-Kampagnen

Zugriff auf praktisch umsetzbare Informationen während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur usw.)

RESTful-API

Nahtlose Integration und Automatisierung Ihrer Sicherheitsabläufe

Kaspersky APT Intelligence Reporting

Weitere informationen

www.kaspersky.de

© 2022 AO Kaspersky Lab.
Eingetragene Marken und Servicemarken sind Eigentum ihrer jeweiligen Rechtsinhaber.