

APT Intelligence Reporting

Verbessern Sie das Bewusstsein für und Wissen über hochentwickelte Cyberspionage-Kampagnen durch umfassende, praxisorientierte Berichte von Kaspersky Lab. Mit den Informationen in diesen Berichten können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, indem Sie Angriffe über bekannte Vektoren abblocken, den durch hoch entwickelte Angriffe angerichteten Schaden reduzieren und Ihre Sicherheitsstrategie oder die Ihrer Kunden erweitern.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie zudem über Änderungen in der Taktik von Cyberkriminellen auf dem Laufenden. Außerdem erhalten Sie Zugriff auf unsere vollständige Datenbank mit APT-Berichten – eine weitere effektive Recherche- und Analysequelle, die Sie zur Verteidigung Ihres Unternehmens nutzen können.

Kaspersky Lab hat einige der bedeutendsten APT-Angriffe aller Zeiten entdeckt. Nicht alle neu entdeckten APTs werden jedoch umgehend gemeldet – viele von ihnen werden sogar nie veröffentlicht. Dank unserer umfassenden und praktisch nutzbaren Berichte bleiben Sie stets über APTs auf dem Laufenden.

Als Abonnent von Kaspersky APT Intelligence Reporting erhalten Sie exklusiven Zugang zu unseren Forschungsergebnissen und Erkenntnissen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser aufgedeckt wird – inklusive aller Bedrohungen, die nie veröffentlicht werden. 2017 haben wir mehr als 100 Berichte erstellt.

Kaspersky APT Intelligence Reporting bietet Ihnen Folgendes:

- **Exklusiver Zugriff** auf die technischen Details aktueller Bedrohungen noch während der Untersuchung und vor der Veröffentlichung.
- Im Jahr 2017 wurden **mehr als 100 Berichte** veröffentlicht.
- **Einblicke in nicht öffentliche APTs:** Nicht alle komplexen Bedrohungen werden öffentlich bekannt gemacht. Einige von ihnen werden aufgrund der Angriffsziele, der Vertraulichkeit der Daten, der Art und Weise, auf die die Schwachstellen geschlossen werden, oder der zugehörigen Strafverfolgungsmaßnahmen nie veröffentlicht. Aber die Details werden unseren Kunden mitgeteilt.
- **Detaillierte** technische Daten, darunter eine umfangreiche Liste von Gefährdungsindikatoren (Indicators of Compromise, IOCs), die in Standardformaten wie OpenIOC oder STIX bereitgestellt werden, sowie Zugriff auf unsere Yara-Regeln.
- **Kontinuierliche Überwachung von APT-Kampagnen.** Zugriff auf praktisch nutzbare Informationen noch während der Untersuchung (Information über die APT-Verteilung, IOCs, C&C-Infrastruktur).
- **Inhalte für unterschiedliche Zielgruppen:** Jeder der Berichte enthält 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 Informationen für überragenden Schutz vor entsprechenden Bedrohungen.

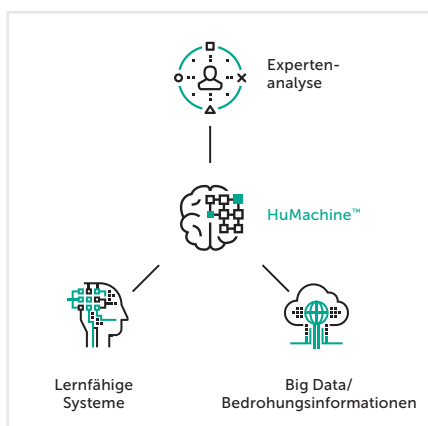
- **Nachträgliche Analyse.** Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Ablaufzeit.
- **Threat Intelligence Portal:** Alle Berichte, einschließlich der aktuellen IOCs, können über das Kaspersky Threat Intelligence Portal oder das zugehörige RESTful-API heruntergeladen werden, um unseren Kunden eine nahtlose Benutzenerfahrung zu bieten.

Abonnementoptionen

- Abonnement vollständiger Berichte zu jedem von Kaspersky Lab aufgedecktem APT mit zugehörigen IOCs und Yara-Regeln
- Abonnement von Zusammenfassungen zu jedem von Kaspersky Lab aufgedecktem APT mit zugehörigen IOCs
- Abonnement nur der Zusammenfassungen zu jedem von Kaspersky Lab aufgedecktem APT

Hinweis – Einschränkung von Abonnenten

Aufgrund der Tatsache, dass einige der in den Berichten enthaltenen Informationen äußerst vertraulich und spezifisch sind, können wir diese Services nur vertrauenswürdigen staatlichen sowie börsennotierten bzw. privat geführten Unternehmen zur Verfügung stellen.



Kaspersky Lab
 Enterprise Cybersecurity: www.kaspersky.de/enterprise
 Neues über Cyberbedrohungen: <https://de.securelist.com>
 IT-Sicherheitsnachrichten: www.business.kaspersky.com

#truecybersecurity
 #HuMachine

www.kaspersky.de

© 2019 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber.