KASPERSKY lab

INTELLIGENCE REPORTING

www.kaspersky.de

INTELLIGENCE REPORTING

Verbessern Sie Wahrnehmung und Wissen über hochkarätige Cyberspionagekampagnen durch umfassende, praxisorientierte Berichte von Kaspersky Lab.

Durch Nutzung der Informationen und Tools in diesen Berichten können Sie schnell auf neue Bedrohungen und Schwachstellen reagieren, indem Sie Angriffe über bekannte Vektoren abblocken, den durch hochentwickelte Angriffe angerichteten Schaden reduzieren und Ihre oder die Sicherheitsstrategie Ihrer Kunden erweitern.

APT Intelligence Reporting

Nicht alle neu entdeckten APTs werden umgehend gemeldet, und viele von ihnen werden nie öffentlich gemacht. Dank unserer umfassenden und praktisch nutzbaren Berichte bleiben Sie stets über APTs auf dem Laufenden.

Als Abonnent von Kaspersky APT Intelligence Reporting haben Sie exklusiven Zugang zu unseren Forschungsergebnissen und Entdeckungen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jeder APT, noch während diese aufgedeckt wird, inklusive all jener Bedrohungen, die nie veröffentlicht werden.

Unsere Experten, die zu den erfolgreichsten APT-Jägern der Branche zählen, halten Sie auch über Änderungen in der Taktik von Cyberkriminellen und Cyberterroristen 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 APT INTELLIGENCE REPORTING BIETET IHNEN FOLGENDES:

- **Exklusiver Zugriff** auf die technischen Details hochmoderner Bedrohungen noch während der Untersuchung und vor der Veröffentlichung.
- **Einblicke in nicht öffentliche APTs**. Nicht alle hochkarätigen 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, Proben und Tools, darunter eine umfangreiche Liste von Gefährdungsindikatoren (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).
- **Nachträgliche Analyse**. Zugriff auf alle zuvor herausgegebenen privaten Berichte während der Abolaufzeit.

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

INTELLIGENCE REPORTING

Kundenspezifische Berichte mit Bedrohungsinformationen

Was wäre die beste Methode, einen Angriff gegen Ihr Unternehmen vorzutragen? Welche Routen und welche Informationen kann ein Angreifer nutzen, der es speziell auf Sie abgesehen hat? Hat es bereits einen Angriff gegeben, oder sind Sie derzeit einer Bedrohung ausgesetzt?

Unsere kundenspezifschen Berichte mit Bedrohungsinformationen beantworten diese und weitere Fragen. Unsere Experten erstellen dazu ein umfassendes Bild Ihrer aktuellen Gefährdungslage, zeigen Schwachstellen auf, die mit großer Wahrscheinlichkeit genutzt werden, und weisen ggf. bereits stattgefundene bzw. geplante Angriffe nach.

Dank dieser einzigartigen Einblicke können Sie Ihre Verteidigungsstrategie auf die Bereiche konzentrieren, die als Hauptziele der Cyberkriminellen ausgewiesen wurden. Auf diese Weise handeln Sie schnell und präzise und minimieren das Risiko eines erfolgreichen Angriffs.

Unsere Berichte, die mithilfe von frei zugänglichen Informationsquellen (OSINT), einer tiefgreifenden Analyse mithilfe von Expertensystemen und Datenbanken von Kaspersky Lab sowie unserer Erkenntnisse über kriminelle Untergrundnetzwerke zusammengestellt werden, decken die folgenden Bereiche ab:

- **Identifizierung von Angriffsvektoren**: Identifizierung und Statusanalyse von extern verfügbaren, wichtigen Komponenten Ihres Netzwerks, z. B. Bankautomaten, Videoüberwachung und andere Systeme, die Mobiltechnologien nutzen, Mitarbeiterprofile in Sozialen Netzwerken und E-Mail-Konten von Mitarbeitern, die potentielle Angriffsziele darstellen.
- **Tracking-Analyse von Malware und Cyberattacken**: Identifizierung, Überwachung und Analyse von aktiven oder inaktiven, gegen Ihr Unternehmen gerichteten Malware-Proben, aller früheren oder aktuellen Botnet-Aktivitäten und aller verdächtigen netzwerkbasierten Aktivitäten.
- **Angriffe auf Dritte**: Beweise für Bedrohungen und Botnet-Aktivitäten, die sich speziell gegen Ihre Kunden, Partner und Abonnenten richten, deren infizierte Systeme dann für Angriffe auf Ihr Unternehmen genutzt werden könnten.
- **Informationslecks**: Durch diskrete Überwachung von Online-Foren und Communitys können wir herausfinden, ob es Angriffspläne gegen Ihr Unternehmen gibt, z. B. ob ein illoyaler Mitarbeiter mit Informationen handelt.
- **Aktueller Angriffsstatus**: APT-Attacken können jahrelang unentdeckt bleiben. Wenn wir einen aktuellen Angriff auf Ihre Infrastruktur entdecken, beraten wir Sie hinsichtlich einer effektiven Beseitigung.

SCHNELLER EINSTIEG – EINFACHE ANWENDUNG – KEINE RESSOURCEN ERFORDERLICH

Nachdem Sie die Parameter (für kundenspezifische Berichte) und Ihre bevorzugten Datenformate festgelegt haben, ist keine zusätzliche Infrastruktur erforderlich, um mit der Nutzung dieses Kaspersky-Service zu beginnen.

Kaspersky Threat Intelligence Reporting hat keine Auswirkungen auf die Integrität und Verfügbarkeit von Ressourcen, einschließlich der Netzwerkressourcen.

KASPERSKY lab

KASPERSKY lab