KASPERSKY lab

KASPERSKY SECURITY INTELLIGENCE SERVICES. THREAT INTELLIGENCE SERVICES

www.kaspersky.de

THREAT INTELLIGENCE SERVICES

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen erleben derzeit einen Engpass an aktuellen und relevanten Daten, die benötigt werden, um mit den Risiken in Zusammenhang mit IT-Sicherheitsbedrohungen effektiv umzugehen.

Security Threat Intelligence Services von Kaspersky Lab geben Ihnen Zugriff auf alle Informationen, die Sie zur Abwehr dieser Bedrohungen benötigen. Sie werden zur Verfügung gestellt von unserem weltweit einzigartigen Team aus Forschern und Analysten.

Wissen, Erfahrung und tiefgreifende Erkenntnisse über praktisch jeden Aspekt der Cybersicherheit haben Kaspersky Lab zum vertrauenswürdigen Partner angesehener internationaler Strafverfolgungs- und Regierungsbehörden, darunter Interpol und CERTS, gemacht. Sie können dieses Wissen noch heute für Ihr Unternehmen nutzen.

Die Threat Intelligence Services von Kaspersky Lab beinhalten:

- Feeds mit Bedrohungsinformationen (Data Feeds)
- Botnet Tracking
- APT Intelligence Reporting

DATA FEEDS

Verstärken Sie Ihre Netzwerksicherheitslösungen, darunter SIEM-Systeme, Firewalls, IPS/IDS, Anti-APT und Sandbox-/Simulationsverfahren, durch umfassende, laufend aktualisierte Daten, die Ihnen wichtige Einblicke in Cyberbedrohungen und gezielte Attacken liefern.

Die unterschiedlichen Familien und Varianten von Malware sind in den letzten Jahren exponentiell gewachsen. Derzeit erkennt Kaspersky Lab jeden Tag etwa 325.000 einzigartige neue Malware-Proben. Zur Verteidigung ihrer Endpoints vor dieser Art von Bedrohung setzen die meisten Unternehmen herkömmliche Schutzmaßnahmen wie Anti-Malware-Lösungen, Angriffsüberwachungs- und Bedrohungserkennungssysteme ein. In einer sich schnell ändernden Umgebung, in der Cybersicherheit stets versucht, dem Cyberverbrechen einen Schritt voraus zu sein, müssen diese klassischen Lösungen mit auf die Minute aktuellen Bedrohungsinformationen verstärkt werden.

Die Data Feeds von Kaspersky Lab fügen sich in bestehende SIEM-Systeme (Security Information and Event Management) ein, um Ihnen eine zusätzliche Schutzebene zu bieten. Dank der Integration der Bedrohungsdaten können die von unterschiedlichen Netzwerkgeräten an das SIEM-System gesendeten Protokolle mit den URL-Feeds von Kaspersky Lab korreliert werden. Eine Verbindung mit dem HP ArcSight-SIEM-System wird unterstützt. Konnektoren für Splunk und QRadar sind ebenfalls erhältlich.

NUTZUNGSSZENARIEN/SERVICEVORTEILE

Data Feeds von Kaspersky Lab:

- Verbessern Sie Ihre SIEM-Lösung durch Daten zu schädlichen URLs aus Feeds von Kaspersky Lab. Das SIEM-System wird anhand von Protokollen, die von den unterschiedlichen Netzwerkgeräten (Benutzer-PCs, Netzwerkproxys, Firewalls, andere Server) an das SIEM-System gesendet werden, über Malware-, Phishing-und Botnet C&C-URLs informiert.
- Versorgen primäre Netzwerksicherheitslösungen wie Firewalls, IPS/IDS, SIEM-Lösungen, Anti-APT, Sandbox-/Simulationsverfahren, UTM-Appliances usw. mit laufend aktualisierten Bedrohungsdaten
- Verbessern Sie Ihre forensischen Fähigkeiten, indem Sie Ihren Sicherheitsteams aussagekräftige Informationen über Bedrohungen und Einblicke in die Strategie von gezielten Angriffen zur Verfügung stellen
- Fördern Sie die Forschung. Informationen über schädliche URLs und die MD5-Hashes von schädlichen Dateien sind ein wertvoller Beitrag für die Bedrohungsforschung

Kaspersky Lab bietet drei Arten von Data Feeds an:

1. Schädliche URLs und Masken
2. Datenbanken mit MD5-Hashfunktionen für schädliche Objekte
3. Feeds zu mobilen Bedrohungen

FEED-BESCHREIBUNG

Schädliche URLs – Ein Datensatz mit URLs, der die schädlichsten Links und Webseiten beinhaltet. Es stehen maskierte und nicht maskierte Datensätze zur Verfügung.

Phishing-URLs – Ein Datensatz mit URLs, die von Kaspersky Lab als Phishing-Webseiten identifiziert wurden. Es stehen maskierte und nicht maskierte Datensätze zur Verfügung.

Botnet C&C-URLs – Ein Datensatz von Command-and-Control-Server-URLs (C&C) und verwandten schädlichen Objekten.

Malware-Hashfunktionen (ITW) – Ein Satz von Datei-Hashes mitsamt der zugehörigen Beurteilungen zu den gefährlichsten und am weitesten verbreiteten Malware-Objekten auf Grundlage von Informationen aus dem KSN.

Malware-Hashfunktionen (UDS) – Ein Datensatz mit Datei-Hashfunktionen, die von Cloud-Technologien von Kaspersky Lab (UDS: Urgent Detection System) basierend auf den Metadaten und Statistiken einer Datei (ohne das Objekt selbst) erkannt wurden. Ermöglicht die Identifizierung von neuen und aufkommenden schädlichen (Zero-Day) Objekten, die durch andere Methoden nicht erkannt werden können.

Mobile-Malware-Hashfunktionen – Ein Datensatz von Datei-Hashfunktionen zur Erkennung schädlicher Objekte, die mobile Plattformen infizieren.

Feed zu P-SMS-Trojanern – Ein Datensatz mit Trojaner-Hashwerten mitsamt dem zugehörigen Kontext für die Erkennung von SMS-Trojanern, die hohe Mobilfunkkosten generieren und es dem Angreifer ermöglichen, SMS-Nachrichten zu entwenden, zu löschen oder auf sie zu antworten.

C&C-URLs für mobile Botnets – Ein Datensatz mit URLs, inklusive Kontext zu C&C-Servern für mobile Botnets.

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 des Kaspersky APT Intelligence Reportings haben Sie exklusiven Zugang zu unseren Forschungsergebnissen und Entdeckungen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser 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.

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