Kaspersky Threat Intelligence Services

www.kaspersky.de
#truecybersecurity

Kaspersky Threat Intelligence Services

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Unternehmen aus allen Branchen verfügen oft nicht über die aktuellen und relevanten Daten, die für einen effektiven Umgang mit den Risiken der IT-Sicherheitsbedrohungen erforderlich sind..

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

Die 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 weltweiten Team aus Forschern und Analysten.

Die Threat Intelligence Services von Kaspersky Lab beinhalten:

- Threat Data Feeds
- APT Intelligence Reporting
- Tailored Threat Reporting
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

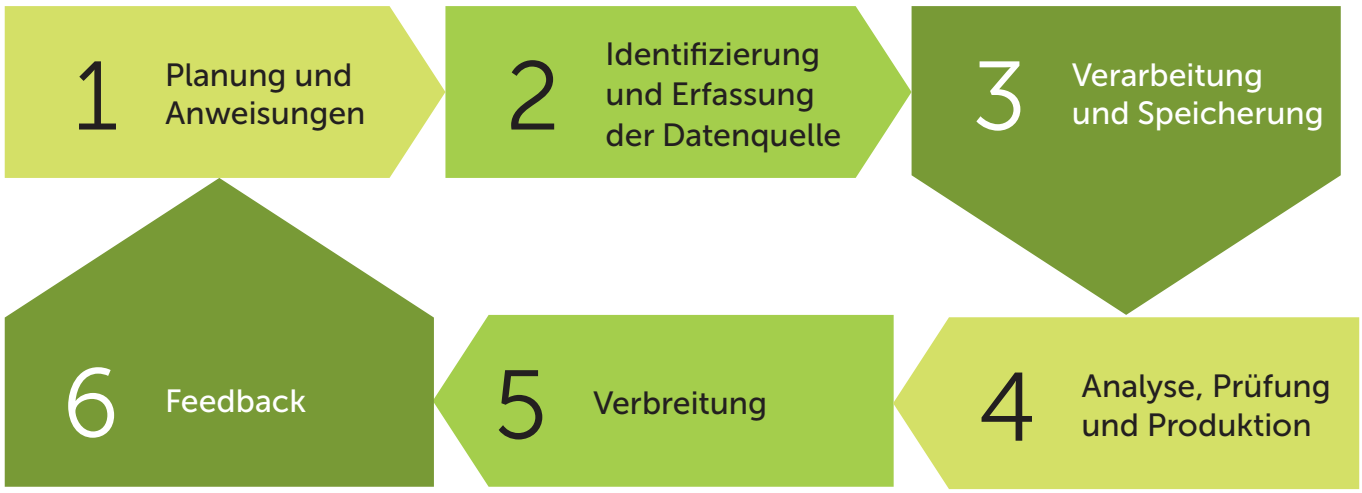
Threat Data Feeds

Andere Sicherheitsanbieter und Unternehmen nutzen Kaspersky Threat Data Feeds, um eigene **Sicherheitslösungen zu entwickeln oder ihr Unternehmen zu schützen**.

Cyberangriffe geschehen jeden Tag. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. **Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger.** Die Angreifer nutzen komplizierte **Kill Chains**, Kampagnen und angepasste **Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um in Systeme einzudringen und Ihre Geschäftsabläufe zu unterbrechen oder Ihre Kunden zu schädigen**.

Kaspersky Lab informiert Ihr Unternehmen bzw. Ihre Kunden **regelmäßig** mit **aktualisierten Threat Data Feeds über Risiken und Auswirkungen** von Cyberbedrohungen. Diese helfen Ihnen, **Bedrohungen effektiver zu bekämpfen** und Ihr Unternehmen **besser vor Angriffen zu schützen**, noch bevor diese eingeleitet werden.

Informationszyklus



Die Data Feeds

Die Feeds umfassen Folgendes:

- IP Reputation Feed – Gruppen von IP-Adressen mit Kontext zu verdächtigen und schädlichen Hosts
- Malicious and Phishing URL Feed – Enthält schädliche bzw. Phishing-Links und -Websites
- Botnet C&C URL Feed – Enthält C&C-Server für Desktop-Botnets sowie verwandte schädliche Objekte
- Mobile Botnet C&C URL Feed – Enthält C&C-Server für mobile Botnets, um infizierte Geräte zu erkennen, die mit C&C-Servern kommunizieren
- Malicious Hash Feed – Umfasst die gefährlichste, am weitesten verbreitete und neu aufkommende Malware
- Mobile Malicious Hash Feed – Unterstützt die Erkennung schädlicher Objekte, die mobile Android- und iPhone-Plattformen infizieren
- P-SMS Trojan Feed – Unterstützt die Erkennung von SMS-Trojanern, über die Angreifer SMS-Nachrichten stehlen, löschen oder beantworten und hohe Mobilfunkkosten für mobile Nutzer generieren können
- Whitelisting Data Feed – Versorgt Lösungen und Services von Drittanbietern mit systematischen Informationen zu legitimer Software
- **NEU! Kaspersky Transforms for Maltego** – Bietet Maltego-Benutzern eine Reihe von Transformationen, über die sie Zugriff auf Kaspersky Lab Threat Data Feeds erhalten. Mit Kaspersky Transforms for Maltego können Sie URLs, Hashes und IP-Adressen mithilfe der Feeds von Kaspersky Lab überprüfen. Die Transformationen können die Kategorie eines Objekts bestimmen und nützlichen Kontext darüber bereitstellen.

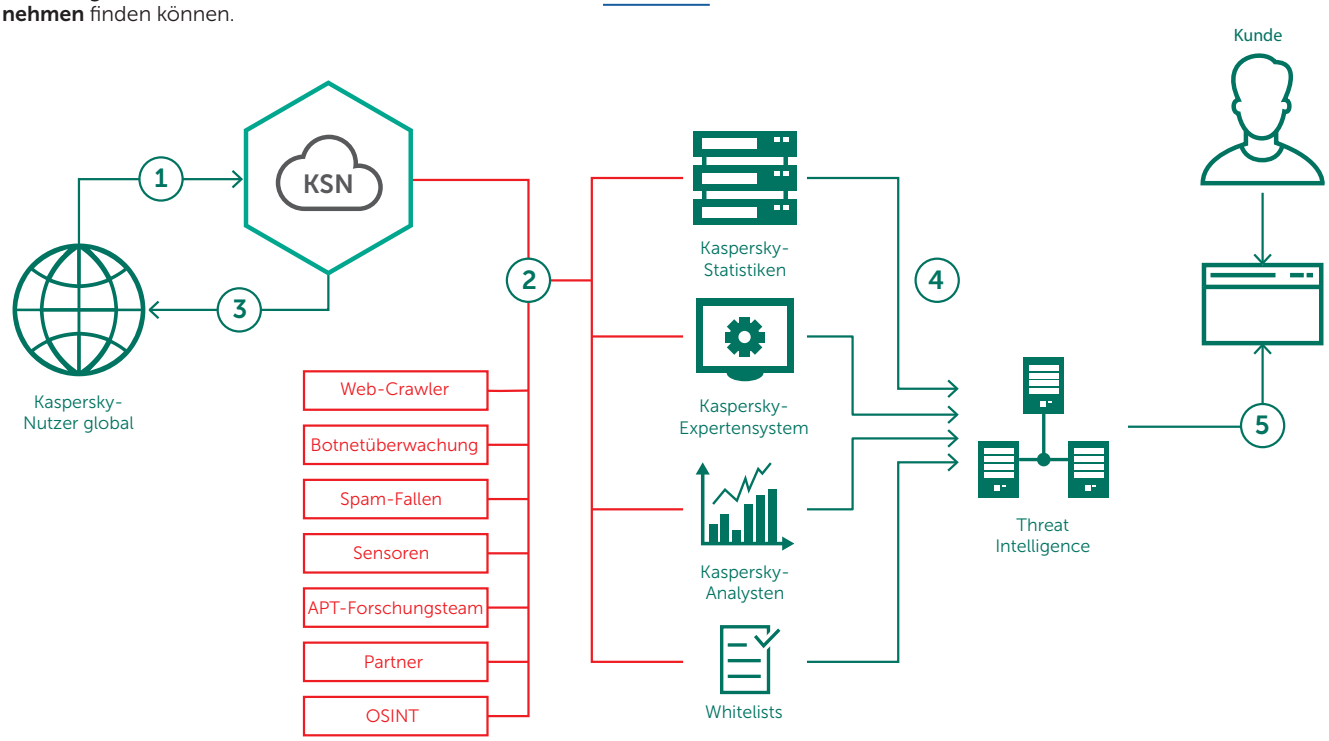
Kontextdaten

Jeder Datensatz in jedem Data Feed wird mit **umfangreichem Kontext** angereichert (Bezeichnungen von Bedrohungen, Zeitstempel, Geolokalisierungsdaten, aufgelöste IP-Adressen infizierter Webressourcen, Hashes, Beliebtheit usw.). Kontextdaten eröffnen den Blick auf das große Ganze und ermöglichen die weitere Analyse und vielfältige Nutzung der Daten. Wenn die Daten in einen Kontext gesetzt werden, liefern sie schneller Antworten auf die Fragen **„Wer?", „Was?", „Wo?" und „Wann?"**. Außerdem geben sie Aufschluss über Ihre Gegner, sodass Sie rechtzeitig Entscheidungen treffen und die **richtigen Maßnahmen für Ihr Unternehmen** finden können.

Erfassung und Verarbeitung

Unsere Data Feeds werden aus zusammengeführten, heterogenen und äußerst zuverlässigen Quellen bezogen, darunter das Kaspersky Security Network, unsere eigenen Webcrawler, unser Botnet Monitoring Service (ununterbrochene Überwachung von Botnets sowie ihrer Ziele und Aktivitäten) sowie Spam-Fallen, Forschungsteams und Partner.

Dann werden sämtliche zusammengefassten Daten in Echtzeit sorgfältig untersucht und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Expertensysteme von Kaspersky Lab (Sandboxes, heuristische Engines, Multi-Scanner, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Analysten und die Verifizierung anhand von Whitelists.



Kaspersky Threat Data Feeds enthalten sorgfältig geprüfte Daten zu Bedrohungsindikatoren, die in Echtzeit aus realen Datenquellen bezogen werden.

Service-Highlights

- Data Feeds mit vielen **False Positives** sind wertlos. Deshalb werden die Feeds vor ihrer Veröffentlichung umfassend getestet und gefiltert, um zu gewährleisten, dass nur überprüfte Daten bereitgestellt werden.
- Die Data Feeds werden automatisch in Echtzeit generiert – basierend auf den weltweit vom Kaspersky Security Network erfassten Daten, die einen Einblick in einen signifikanten Anteil des gesamten Internetdatenverkehrs und alle möglichen Datentypen von Millionen von Endbenutzern in mehr als 213 Ländern gewähren. So werden **hohe Erkennungsraten** garantiert.
- Sämtliche Feeds werden über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die **dauerhafte Verfügbarkeit** gewährleistet.
- Die Feeds ermöglichen die **umgehende Erkennung von URLs**, die für Phishing, Malware, Exploits, Botnet C&C URLs und andere schädliche Inhalte genutzt werden.
- **Malware** in allen Arten von Datenverkehr (Web, E-Mail, P2P, IM usw.) sowie gezielte mobile Malware kann **sofort erkannt** und identifiziert werden.
- Einfache **Verteilungsformate** (**JSON, CSV, OpenIoC, STIX**) über **HTTPS** oder Ad-hoc-Bereitstellungsmechanismen ermöglichen die einfache Integration der Feeds in Sicherheitslösungen.
- Hunderte von Experten, darunter **Sicherheitsanalysten** aus der ganzen Welt, weltweit anerkannte **Sicherheitsexperten aus unserem GReAT-Team und führenden Forschungs- und Entwicklungsteams**, tragen gemeinsam zur Bereitstellung dieser Feeds bei. Sicherheitsbeauftragte erhalten kritische, aus zuverlässigen Daten generierte Informationen und Benachrichtigungen, ohne Gefahr zu laufen, von unnötigen Anzeigen und Warnungen überflutet zu werden.
- **Einfache Implementierung**. Dank ergänzender Dokumentation, Beispielen, einem persönlichen technischen Account Manager sowie dem technischen Support von Kaspersky Lab geht die Integration schnell und einfach vonstatten.

Vorteile

- **Verstärken Sie Ihre Lösungen zur Netzwerkverteidigung**, einschließlich SIEMs, Firewalls, IPS/IDS, Sicherheits-Proxys, DNS-Lösungen und APT-Abwehr, mit regelmäßig aktualisierten Gefährdungsindikatoren (Indicators of Compromise, IOCs) und praktisch umsetzbarem Kontext. So erhalten Sie Einblicke in Cyberangriffe und können den Zweck, die Funktionen und die Ziele der Angreifer ermitteln. Führende SIEM -Systeme (einschließlich HP ArcSight, IBM QRadar, Splunk usw.) werden vollständig unterstützt.
- Entwickeln oder verbessern Sie den **Malware-Schutz für Geräte am Netzwerkrand** (wie z. B. Router, Gateways und UTM-Appliances).
- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Fähigkeiten**, indem Sie Ihren Sicherheits- bzw. SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe gezielter Angriffe bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill-Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Stellen Sie Unternehmensnutzern Bedrohungsinformationen bereit**. Nutzen Sie Informationen aus erster Hand zu aufkommender Malware und anderen Bedrohungen, um **Ihre Verteidigung präventiv zu stärken und Vorfälle zu vermeiden**.
- **Helfen Sie bei der Abwehr gezielter Angriffe**. Verstärken Sie Ihre Sicherheitsstellung durch taktische und strategische Bedrohungsinformationen, indem Sie Verteidigungsstrategien an die spezifischen Bedrohungen anpassen, mit denen Ihr Unternehmen konfrontiert ist.
- Nutzen Sie Bedrohungsinformationen, um **schädliche Inhalte zu erkennen, die in Ihren Netzwerken und Rechenzentren gehostet werden**.
- **Verhindern Sie die Extraktion vertraulicher Assets und geistigen Eigentums** über infizierte Geräte an Personen außerhalb des Unternehmens. Dank der schnellen Erkennung infizierter Assets vermeiden Sie den Verlust von Wettbewerbsvorteilen und Geschäftschancen und schützen den Ruf Ihrer Marke.
- Durchsuchen Sie Gefährdungsindikatoren, wie z. B. C&C-Protokolle, IP-Adressen, schädliche URLs oder Datei-Hashes mit von Experten validiertem Bedrohungskontext. Dieser ermöglicht es Ihnen, Angriffe zu priorisieren, vereinfacht Entscheidungen zu IT-Ausgaben und -Ressourcenverteilung und **unterstützt Sie dabei, sich auf die Abwehr der Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen**.
- Nutzen Sie unsere Expertise und praktisch umsetzbaren Kontextinformationen, um **den Schutz Ihrer Produkte und Services zu verbessern**, wie z. B. Inhaltsfilterung, Blockierung von Spam/Phishing usw.
- **Erweitern Sie als MSSP Ihr Geschäft**, indem Sie Ihren Kunden branchenführende Bedrohungsinformationen als Premiumservice bieten. **Als CERT** können Sie Ihre Fähigkeiten rund um die Erkennung und Identifizierung von Bedrohungen verbessern und erweitern.

APT Intelligence Reporting

Verbessern Sie Wahrnehmung und Wissen über hochkarätige Cyberspionagekampagnen 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.

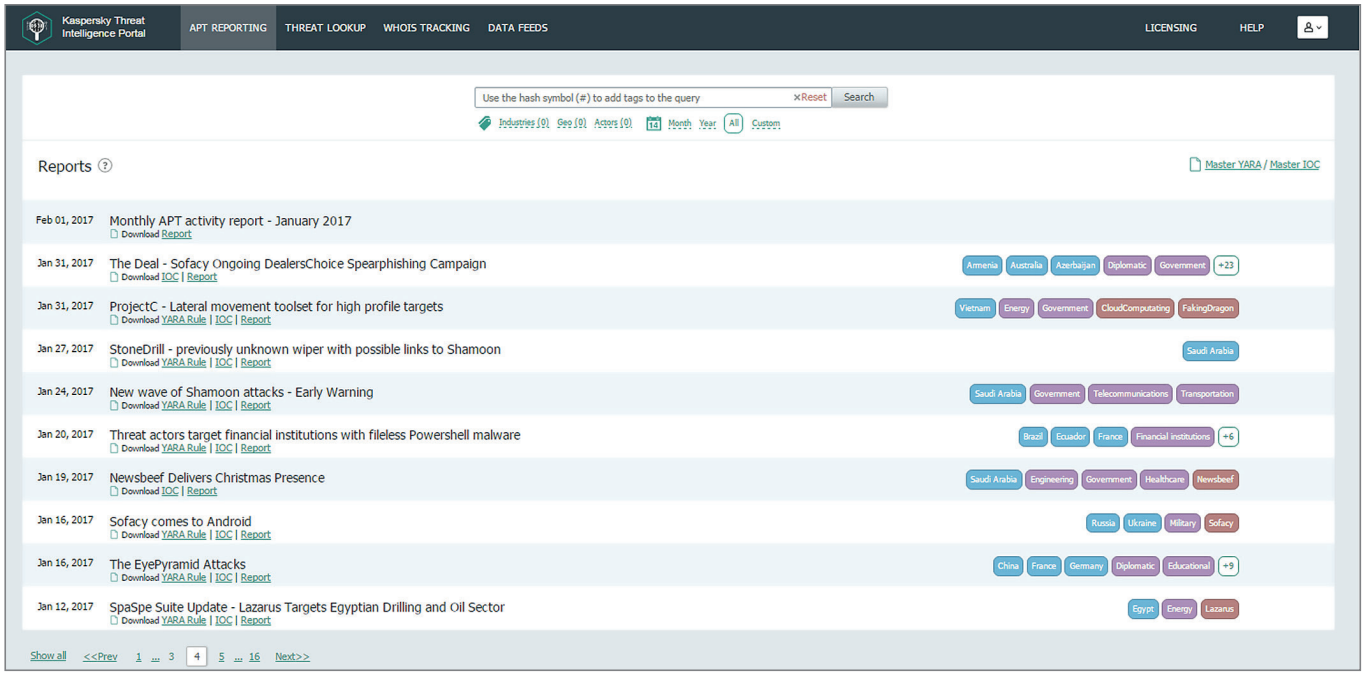
Kaspersky Lab hat einige der bedeutendsten APT-Angriffe aller Zeiten entdeckt. Nicht alle neu entdeckten APTs werden jedoch umgehend gemeldet – viele von ihnen werden sogar nie veröffentlicht.

Als Abonnent von Kaspersky APT Intelligence Reporting erhalten 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 aller Bedrohungen, die nie veröffentlicht werden. 2016 haben wir mehr als 100 Berichte erstellt.

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 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, 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 Abolaufzeit.

- **APT Intelligence Portal.** Alle Berichte, einschließlich der aktuellen IOCs, können über das APT Intelligence Portal heruntergeladen werden, um unseren Kunden eine nahtlose Benutzererfahrung zu bieten. Auch eine API ist verfügbar.

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.

Tailored Threat Reporting

Kundenspezifisches Threat Reporting

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 kundenspezifischen Berichte zu Bedrohungen 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 erkannt 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 und Ihre bevorzugten Datenformate festgelegt haben, ist keine zusätzliche Infrastruktur erforderlich, um mit der Nutzung dieses Services von Kaspersky Lab zu beginnen.

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

Der Service kann als einmaliges Projekt oder regelmäßig in Form eines Abonnements (z. B. vierteljährlich) in Anspruch genommen werden.

Länderspezifisches Threat Reporting

Die Cybersicherheit eines Landes umfasst den Schutz aller wichtigen Institutionen und Unternehmen. Hochentwickelte, anhaltende Bedrohungen (Advanced Persistent Threats, APT), die auf staatliche Behörden abzielen, können die nationale Sicherheit bedrohen. Mögliche Cyberattacken gegen Unternehmen in den Bereichen Produktion, Transport und Telekommunikation sowie im Bankensektor und anderen wichtigen Branchen können den Staat empfindlich treffen, beispielsweise in Form von finanziellen Verlusten, Produktionsunfällen, Störungen in der Netzwerkkommunikation und Unzufriedenheit in der Bevölkerung.

Mit einem Überblick über die aktuelle Gefährdungslage und aktuelle Trends in Bezug auf Malware und Hackerangriffe, die gegen Ihr Land gerichtet sind, können Sie Ihre Verteidigungsstrategie auf Bereiche konzentrieren, die als Hauptziele für Cyberkriminelle dienen. So können Sie Eindringlinge schnell und präzise bekämpfen und das Risiko erfolgreicher Angriffe verringern.

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

- **Identifizierung von Bedrohungsvektoren**: Identifizierung und Statusanalyse extern verfügbarer, wichtiger nationaler IT-Ressourcen, einschließlich anfälliger staatlicher Programme, Telekommunikationsanlagen, Komponenten von Industriesteuerungen (wie SCADA, PLCs usw.), Geldautomaten usw.

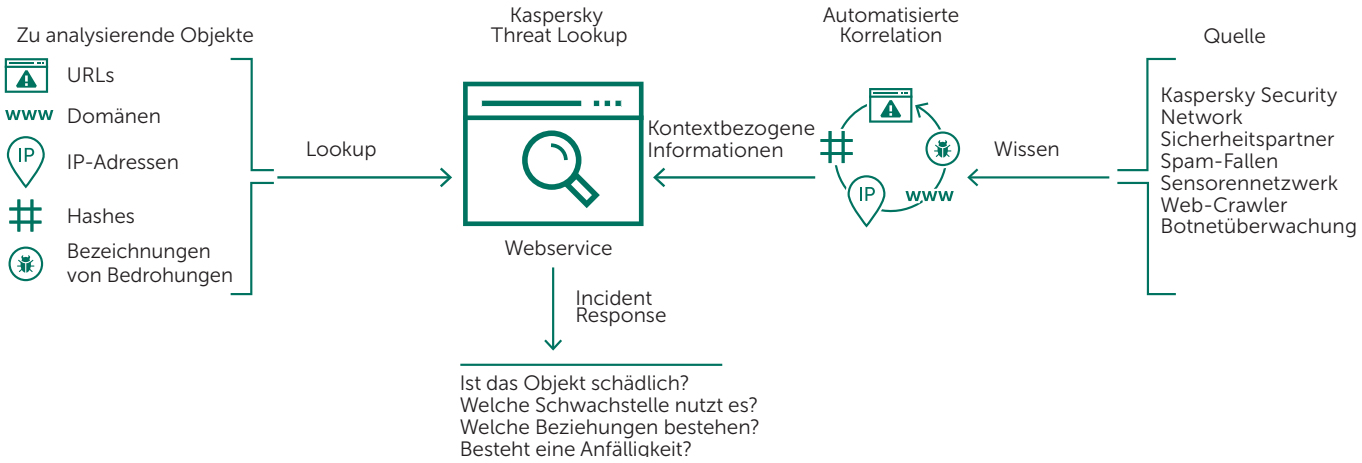
- **Tracking-Analyse von Malware und Cyberattacken**: Identifizierung und Analyse von APT-Kampagnen, aktiven oder inaktiven Malware-Proben, früheren oder aktuellen Botnet-Aktivitäten und anderen nennenswerten Bedrohungen, die auf Ihr Land abzielen, basierend auf den Daten aus unseren einzigartigen internen Überwachungsressourcen.

- **Informationslecks**: Durch diskrete Überwachung von Untergrundnetzen und Online-Communitys können wir ermitteln, ob Hacker Angriffspläne gegen bestimmte Unternehmen erörtern. Außerdem decken wir stark gefährdete Konten auf, die ein Risiko für geschädigte Unternehmen und Institutionen darstellen können (z. B. Konten von Mitarbeitern von Regierungsbehörden, die beim Ashley Madison-Angriff auftauchten und für Erpressungen genutzt werden könnten).

Kaspersky Threat Intelligence Reporting hat keine Auswirkungen auf die Integrität und Verfügbarkeit der untersuchten Netzwerkressourcen. Der Service basiert auf nicht invasiven Netzwerkanalysemethoden sowie auf der Analyse von Informationen aus frei zugänglichen Quellen und aus Ressourcen mit beschränktem Zugriff.

Zum Schluss erhalten Sie einen Bericht mit einer Beschreibung nennenswerter Bedrohungen für Branchen und Institutionen des Landes sowie zusätzliche Informationen zu detaillierten technischen Analyseergebnissen. Die Berichte werden in verschlüsselten E-Mails versendet.

Threat Lookup



Service-Highlights

- **Zuverlässige Sicherheitsinformationen**: Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Produkte von Kaspersky Lab zählen zu den führenden bei Anti-Malware-Tests[1]. Die hohen Erkennungsraten mit Fehlalarmquoten, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.
- **Aufspüren von Bedrohungen**: Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Erkennen und beenden Sie Angriffe so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.
- **Sandbox-Analyse**[2]: Dabei werden unbekannte Bedrohungen durch die Ausführung von verdächtigen Objekten in einer abgesicherten Umgebung erkannt sowie das gesamte Bedrohungsverhalten mitsamt der Artefakte in leicht verständlichen Berichten überprüft.
- **Breites Spektrum an Exportformaten**: Exportieren Sie die IOCs oder den praktisch umsetzbaren Kontext in gängige, strukturiertere und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV, um alle Vorteile der Bedrohungsinformationen zu nutzen, betriebliche Workflows zu automatisieren oder die Integration in bestehende Sicherheitskontrollen, wie z. B. SIEMs, zu ermöglichen.
- **Benutzerfreundliche Web-Oberfläche oder RESTful-API**: Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über ein einfaches RESTful-API zugreifen.

Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt heute kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die für ihre Angriffe zunehmend Ressourcen aus dem Dark Web einsetzen. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains" und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihre Kunden zu schädigen.

Kaspersky Threat Lookup bietet unser gesamtes Wissen über Cyberbedrohungen und ihre Interdependenzen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die aktuellen Bedrohungsinformationen zu URLs, Domänen, IP-Adressen, Datei-Hashes, Bedrohungsbezeichnungen, Statistik- und Verhaltensdaten, WHOIS-/DNS-Daten, Dateiattribute, Geolokalisierungsdaten, Download-Ketten, Zeitstempel usw. ab. Hieraus ergibt sich ein umfassender Überblick über neue und aufkommende Bedrohungen, der Ihnen hilft, die Verteidigung und Vorfallsreaktion Ihres Unternehmens zu verbessern.

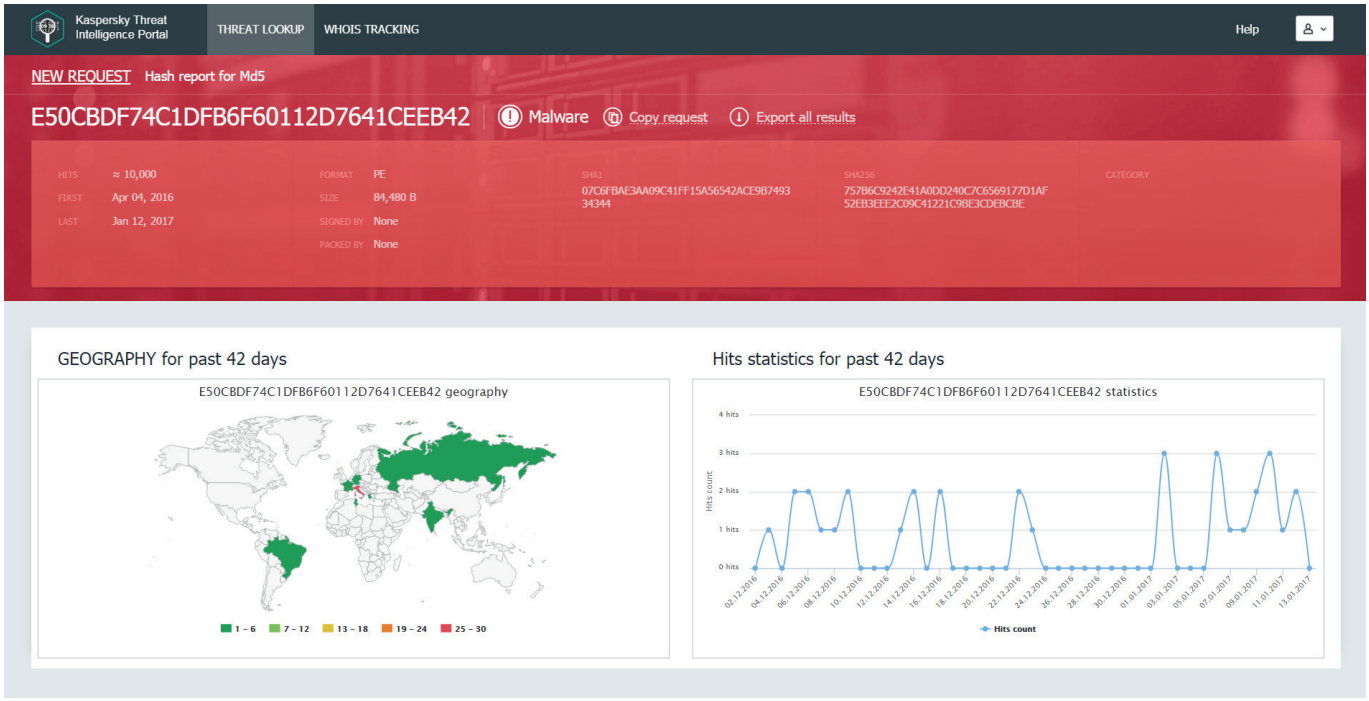
Die von Kaspersky Threat Lookup bereitgestellten Bedrohungsinformationen werden in Echtzeit über eine äußerst fehlertolerante Infrastruktur generiert und überwacht, die kontinuierliche Verfügbarkeit und ein gleichbleibendes Leistungsniveau gewährleistet. Hunderte von Experten, darunter Sicherheitsanalysten aus der ganzen Welt, weltweit anerkannte Sicherheitsexperten aus unserem GReAT-Team und führende Forschungs- und Entwicklungsteams, tragen gemeinsam zur Bereitstellung von wertvollen und praxisnahen Bedrohungsinformationen bei.

Hauptvorteile

- **Verbessern und beschleunigen Sie Ihre Vorfallsreaktion und forensischen Funktionen**, indem Sie Ihren Sicherheits-/SOC-Teams Zugriff auf relevante Bedrohungsinformationen sowie globale Erkenntnisse über die Hintergründe von gezielten Angriffen bereitstellen. Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen, verkürzen Sie so die Vorfallsreaktionszeit, und unterbrechen Sie die Kill-Chain, bevor entscheidende Systeme und Daten in Mitleidenschaft gezogen werden.
- **Führen Sie anhand hochzuverlässiger Bedrohungskontexte detaillierte Suchen innerhalb der Bedrohungsindikatoren aus**, z. B. in IP-Adressen, URLs, Domänen oder Datei-Hashes, um Angriffe zu priorisieren, Entscheidungen über Personal- und Ressourcenzuteilungen zu verbessern und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.
- **Wehren Sie gezielte Angriffe ab**. Verbessern Sie mithilfe taktischer und strategischer Bedrohungsinformationen Ihre Sicherheitsinfrastruktur, indem Sie die richtigen Verteidigungsstrategien einsetzen.

1 http://www.kaspersky.de/top3

2 Die Funktion soll in der ersten Jahreshälfte 2017 eingeführt werden.



Jetzt können Sie ...

- über eine webbasierte Benutzeroberfläche oder das RESTful-API nach Bedrohungsindikatoren suchen.
- nachvollziehen, warum ein Objekt als schädlich eingestuft wird.
- überprüfen, ob ein entdecktes Objekt weit verbreitet ist oder isoliert vorkommt.
- zusätzliche Details überprüfen, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu entdecken.

Dies sind nur einige Beispiele. Es gibt noch eine Vielzahl von Möglichkeiten, diese relevanten und fein abgestuften Sicherheitsinformationen zu nutzen.

Kenne deine Feinde und deine Freunde. Erkennen Sie nachgewiesen unschädliche Dateien, URLs und IP-Adressen, und beschleunigen Sie den Untersuchungsvorgang. Wenn jede Sekunde zählt, sollten Sie keine Zeit mit der Analyse von vertrauenswürdigen Objekten verlieren.

Unser Ziel ist es, alle Arten von Cyberbedrohungen abzuwehren und die digitale Welt unserer Kunden sicherer zu machen. Um dies zu erreichen und die Nutzung des Internets sicher zu machen, müssen Bedrohungsinformationen in Echtzeit weitergegeben und verwendet werden können. Ein zeitnaher Zugriff auf Informationen ist für einen effektiven Schutz Ihrer Daten und Netzwerke unerlässlich. Jetzt können Sie mit Kaspersky Threat Lookup effizienter und einfacher denn je auf diese Daten zugreifen.

Jede Benachrichtigung von Kaspersky Phishing Tracking wird per HTTPS bereitgestellt und beinhaltet Folgendes:

- Screenshot der Phishing-URL
- HTML-Code der Phishing-URL
- JSON-Datei, die folgende Felder
- enthält:
  - Phishing-URL
  - Name der Marke, auf die die Phishing-URL abzielt
  - Zeitstempel der ersten Entdeckung
  - Zeitstempel der letzten Entdeckung
  - Beliebtheit der Phishing-URL
  - Geostandort der Benutzer, die von der Phishing-URL betroffen sind
  - Art der gestohlenen Daten (Kreditkartendaten, Anmeldedaten für Banking, E-Mail oder soziale Netzwerke, persönliche Informationen usw.)
  - Angriffstyp (angedrohte Kontosperrung, Datei-Download, Aufforderung, persönliche Daten zu aktualisieren, usw.)
  - Aufgelöste IP-Adresse der Phishing-URL
  - WHOIS-Daten
  - und vieles mehr.

Phishing Tracking

Phishing – insbesondere gezieltes Spear-Phishing – stellt aktuell eine der gefährlichsten und effektivsten Methoden für Onlinebetrug dar. Gefälschte Webseiten erfassen Anmeldedaten und Passwörter, um die Online-Identitäten der Opfer zu übernehmen, um ihnen so Geld zu stehlen oder über ihre E-Mail- oder Social-Media-Konten Spam und Malware zu verbreiten. Diese Methode ist eine leistungsstarke Waffe im Arsenal von Cyberkriminellen, und die Häufigkeit und Vielfalt der Angriffe nehmen immer weiter zu.

Und es trifft nicht nur Finanzinstitute. Jeder – vom Onlinehändler über den Internetanbieter bis hin zur Regierungsbehörde – läuft Gefahr, Opfer von Spear-Phishing zu werden. Durch perfekt kopierte Fälschungen Ihrer Webseite samt vollständiger Corporate Identity oder durch Nachrichten, die direkt von eigenen Führungskräften zu stammen scheinen, werden Nutzer leicht in die Irre geführt und davon überzeugt, vertrauliche Daten preiszugeben – und so sich und dem gesamten Unternehmen großen Schaden zuzufügen.

Ein einziger erfolgreicher Phishing-Angriff kann verheerende Auswirkungen auf das angegriffene Unternehmen haben. Neben direkten Schäden entstehen auch indirekte Kosten, wie z. B. die Bereinigung kompromittierter Webseiten und Konten. Und zu guter Letzt schädigen erfolgreiche Angriffe den Ruf des Unternehmens. Ein solcher Verlust des Kundenvertrauens in Ihre Onlineservices kann zum jahrelangen Verlust von Kunden und Glaubwürdigkeit führen. Cyberkriminalität kennt heutzutage keine Grenzen mehr, und die technischen Möglichkeiten entwickeln sich rapide weiter: Wir erleben immer komplexere Angriffe, bei denen Cyberkriminelle Dark-Web-Ressourcen nutzen, um ihre Opfer anzugreifen. Cyberbedrohungen werden immer häufiger, komplexer und versteckter. Zuverlässige Abwehrmaßnahmen zu finden, wird zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains" und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihre Kunden zu schädigen.

Unsere Lösung – Kaspersky Phishing Tracking Service

Dieser Service verfolgt aktiv das Auftreten von Phishing-Websites, benachrichtigt Sie in Echtzeit und stellt präzise und ausführliche laufende Daten zu Phishing- oder betrügerischen Aktivitäten bereit, die für Ihr Unternehmen relevant sind. Diese Daten umfassen die injizierte Malware und die Phishing-URLs, die Anmeldedaten, vertrauliche Informationen, Finanzdaten und persönliche Informationen von Ihren Benutzern stehlen. Der Service überwacht darüber hinaus die spezifischen Top-Level-Domänen (TLD) oder sogar ganze Regionen hinsichtlich des Auftretens von Phishing-Sites.

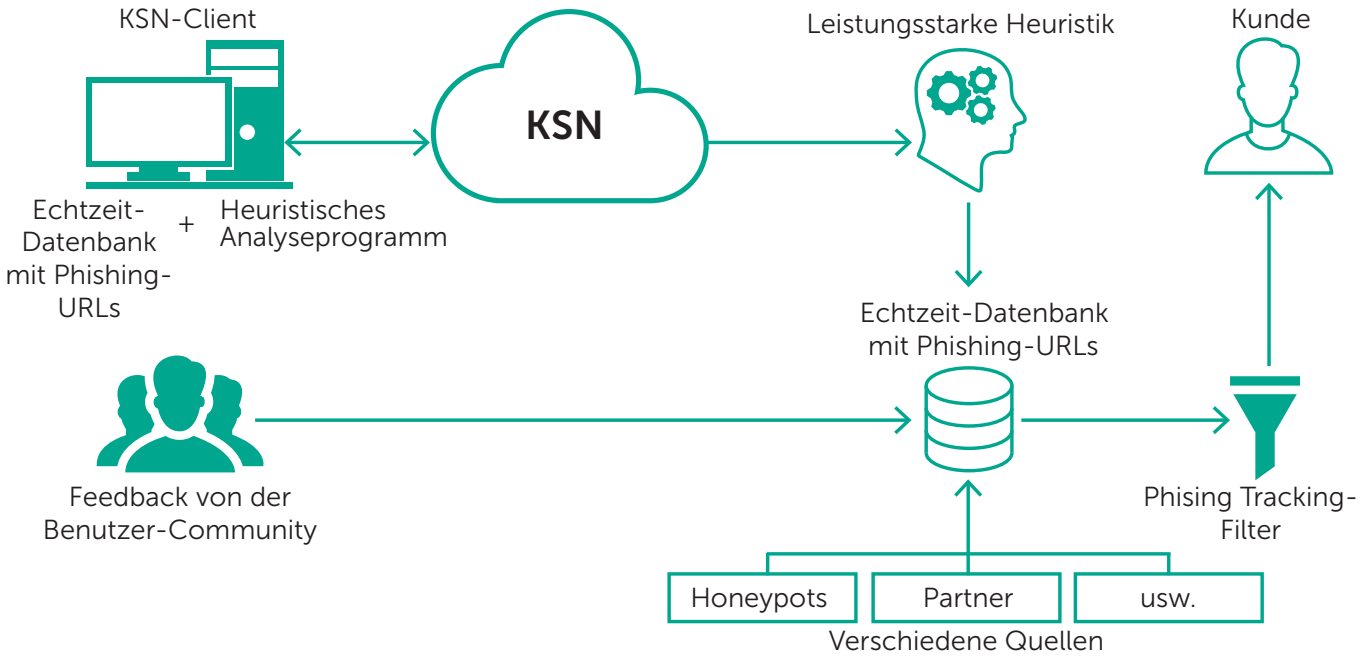
Im Rahmen des Service erhalten Sie E-Mail-Benachrichtigungen zu bestätigten Phishing-Bedrohungen gegen Ihre Marke, Ihren Unternehmensnamen oder Ihre Handelsmarken. Jede Benachrichtigung bietet tief gehende Informationen, hohe Präzision und zuverlässige Informationen zu den immer komplexeren Phishing-Angriffen. So können Sie schnell auf Phishing-Angriffe sowie dynamisch generierte Phishing-Domänen und -URLs reagieren. Neben einer Liste mit Phishing-Sites erhalten Sie zusätzliche Informationen, damit Sie umgehend spezifische Maßnahmen gegen jede beliebige Phishing-Attacke ergreifen können.

Mithilfe dieser frühzeitig bereitgestellten, professionell überprüften Informationen können Sie schnell und präzise reagieren, um die Auswirkungen von Phishing-Aktivitäten in Ihrem Unternehmen und unter Ihren Benutzern einzudämmen und sich optimal so vor Betrug zu schützen.

Quellen der Bedrohungsinformationen

Kaspersky Phishing Tracking nutzt Daten aus heterogenen und äußerst zuverlässigen Informationsquellen, einschließlich Kaspersky Security Network (KSN), leistungsstarker heuristischer Engines, E-Mail-Honeypots, Webcrawler, Spam-Fallen, Forschungsteams, Partner und Verlaufsdaten zu schädlichen Objekten, die wir in den letzten 20 Jahren erfasst haben. Die aggregierten Daten werden dann in Echtzeit überprüft und anhand verschiedener Aufbereitungsverfahren verfeinert, z. B. durch statistische Kriterien, Kaspersky-Expertensysteme (Sandboxes, heuristische Engines, Multi-Scanner, Similaritätstools, Erstellung von Verhaltensprofilen usw.), die Validierung durch Inhaltsanalysten und Verifizierungstools anhand von Whitelists.

Die Kombination der weltweiten Abdeckung des Kaspersky Security Networks, der Erkennungstechnologien von Kaspersky Lab sowie einer Vielzahl von Tests und Filtern gewährleistet maximale Erkennungsraten für jeden Phishing-Angriff und jede Bedrohung – und das ohne Fehlalarme, wie unabhängige Tests zeigen*.



Frühzeitige Warnung vor Phishing-Angriffen

Nutzen Sie den Kaspersky Phishing Tracking Service, und Sie erhalten den entscheidenden Vorteil gegenüber Angreifern. Durch die frühzeitige Warnung vor Phishing-Attacken – ob geplant oder im Gange –, die es auf Ihre Marken, Onlineservices und Kunden abgesehen haben, können Sie Ihre Ressourcen schützen und die Risiken pragmatischer, präziser und kosteneffizienter abwehren.

Einen Schritt voraus

Kritische Informationen werden in Echtzeit sowie über regelmäßige Berichte zu schädlichen Aktivitäten bereitgestellt, die Informationen zu geplanten und aktuell laufenden Angriffen enthalten. So sind Sie den Cyberkriminellen endlich einen Schritt voraus.

Verbesserung des Benutzererlebnisses

Sobald Sie die Phishing-Angreifer kennen und verstehen, können Sie den Schutz entsprechend planen: von der Blockierung veralteter Software bis hin zur Einführung SMS-basierter Autorisierung – damit sich Ihre Onlinekunden geschützt und sicher fühlen.

Minimierung der Auswirkungen

Wenn die URLs von Phishing-Webseiten bekannt sind, können die Internetanbieter benachrichtigt werden, die entsprechende Sites hosten. So wird ein weiterer Diebstahl persönlicher Daten durch die Site verhindert, und der Angriff wird im Keim erstickt.

Immer bestens informiert

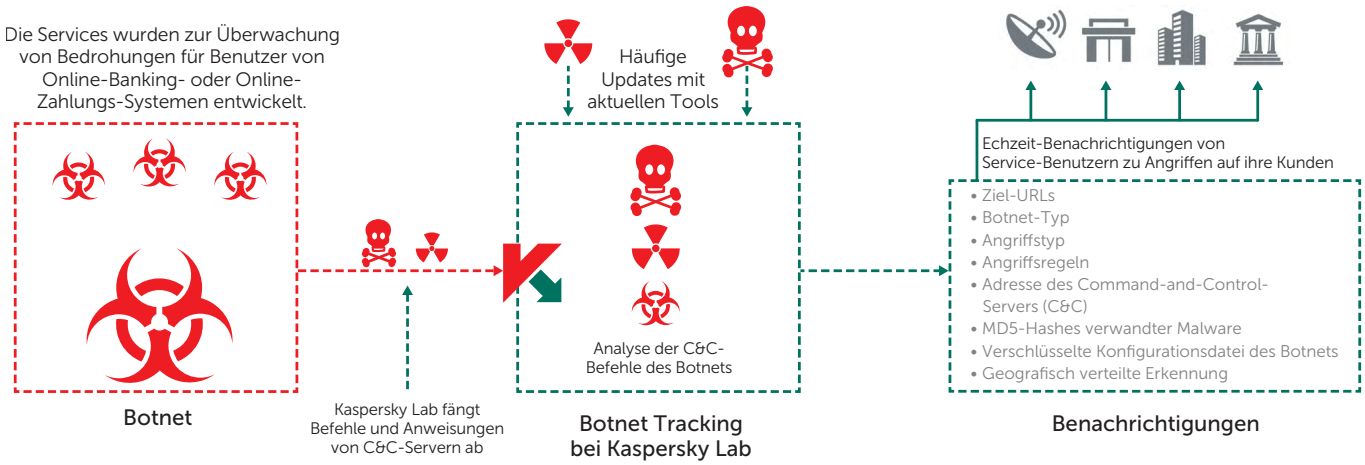
Dieser Fluss relevanter, präziser und ausführlicher Informationen ohne False Positives oder sonstigen unnötigen Aufwand bietet neue Einblicke, mit deren Hilfe Sie heute und in Zukunft die perfekte Sicherheitsstrategie finden. So schützen Sie sich und Ihr Unternehmen vor Onlinebetrug.

AV comparatives Approved 2016 Anti-Phishing

* Testberichte von AV-Comparatives sind auf Anfrage verfügbar.

Botnet Tracking

Zuverlässige Überwachungs- und Benachrichtigungsservices zur Identifizierung von Botnets, die Ihren Ruf und Ihre Kunden schädigen könnten.



Nutzungsszenarien/Servicevorteile

- Mit proaktiven Benachrichtigungen zu Bedrohungen durch Botnets, die es auf Ihre Online-Benutzer abgesehen haben, sind Sie dem Angriff immer einen Schritt voraus.
- Durch die Identifizierung einer Liste von Botnet-Command & Control-Server-URLs, die auf Ihre Online-Benutzer ausgerichtet sind, können Sie diese über Anforderungen an CERTs oder Strafverfolgungsbehörden blockieren.
- Verbessern Sie Ihr Online-Banking/Ihre Zahlungssysteme, indem Sie die Art des Angriffs verstehen.
- Schulen Sie Ihre Online-Benutzer, damit sie die bei Angriffen verwendeten Social-Engineering-Techniken erkennen und nicht darauf hereinfallen.

Bleiben sie dank Echtzeitinformationen handlungsfähig:

Zum Umfang dieses Service gehören personalisierte Benachrichtigungen mit Informationen zu übereinstimmenden Markennamen, die durch die Analyse von Schlüsselwörtern in den von Kaspersky Lab überwachten Botnets ermittelt wurden. Die Benachrichtigungen können Ihnen per E-Mail oder RSS im HTML- oder JSON-Format bereitgestellt werden. Sie erhalten u. a. folgende Informationen:

- **Ziel-URL(s) –** Bot-Malware wartet so lange ab, bis ein Benutzer auf die URLs des zu attackierenden Unternehmens zugreift, und startet dann den Angriff.
- **Botnet-Typ –** Bestimmen Sie präzise den Malware-Typ, der eingesetzt wird, um die Transaktionen Ihrer Kunden zu gefährden. Beispiele: Zeus, SpyEye oder Citadel usw.
- **Angriffstyp –** Verrät Ihnen, zu welchem Zweck die Malware eingesetzt wird, z. B. Injektion von Webdaten, Bildschirmlöschung, Videoaufzeichnung oder Weiterleitung an Phishing-URLs.
- **Angriffsregeln –** Verrät Ihnen, welche unterschiedlichen Regeln für die Injektion von Webcodes verwendet werden, z. B. HTML-Anfragen (GET/POST), Webseitendaten vor und nach der Injektion.
- **Command-and-Control-Serveradressen (C&C) –** Gibt Ihnen die Möglichkeit, dem Internetdienstanbieter den betreffenden Server zu melden, damit die Bedrohung rascher entschärft werden kann.
- **MD5-Hashwerte der Malware –** Kaspersky Lab stellt Ihnen den zur Malware-Verifizierung verwendeten Hashwert zur Verfügung.
- **Verschlüsselte Konfigurationsdatei des Botnets –** Vollständige Liste der betroffenen URLs.
- **Geografisches Verteilungsmuster (10 Hauptländer) –** Statistische Daten zur weltweiten Verteilung der Malware-Proben.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com