To manage risk effectively, organizations must use a holistic “threats-in-context” approach that allows proactive identification of real threats to critical business systems. iDefense clients gain 24/7 access to an extensive intelligence-gathering network, a well-defined methodology and highly skilled professionals who deliver comprehensive, actionable intelligence. It does not look merely at the “what” and “how” of network-based security threats and vulnerabilities, but also the “who” and “why.” The iDefense Threat Indicators Service helps organizations understand the impact of a risk, and respond rapidly and appropriately to secure business-critical data and systems.

Today’s network threats are more numerous and damaging than ever. Sophisticated attacks can seriously compromise an organization—not only in terms of lost productivity, data breaches and possible penalties for noncompliance, but also lost trust and damaged reputation. Few organizations have the intelligence-gathering and threat analysis capabilities to address network vulnerabilities and threats in their full context, resulting in delayed responses to true threats, impaired threat prioritization, and costly, unnecessary emergency responses.

The iDefense Threat Indicators Service provides a list of vetted indicators of compromise, allowing customers to divert and block traffic from nefarious locations. This service features iDefense-discovered IP addresses, domain names, URLs, related hashes, malware family, and more.

**PART OF iDEFENSE SECURITY INTELLIGENCE SERVICES**

To manage risk effectively, organizations must use a holistic “threats-in-context” approach that allows proactive identification of real threats to critical business systems. iDefense clients gain 24/7 access to an extensive intelligence-gathering network, a well-defined methodology and highly skilled professionals who deliver comprehensive, actionable intelligence. It does not look merely at the “what” and “how” of network-based security threats and vulnerabilities, but also the “who” and “why.” The iDefense Threat Indicators Service helps organizations understand the impact of a risk, and respond rapidly and appropriately to secure business-critical data and systems.

Today’s network threats are more numerous and damaging than ever. Sophisticated attacks can seriously compromise an organization—not only in terms of lost productivity, data breaches and possible penalties for noncompliance, but also lost trust and damaged reputation. Few organizations have the intelligence-gathering and threat analysis capabilities to address network vulnerabilities and threats in their full context, resulting in delayed responses to true threats, impaired threat prioritization, and costly, unnecessary emergency responses.

**METHODOLOGY**

A threat indicator is a concise data point that generally indicates evidence of an attempt at compromise if detected on a host or within a network. Because of the high operational costs associated with false positives, iDefense provides the most precise indicator that will accurately encompass the threat. IP addresses, for example, may indicate threats accurately, but they can often lead to false positives. A single IP address may be responsible for hosting hundreds to thousands of domains, but only one might be malicious. In these cases, the full domain or even a specific URL provides a more precise indicator. Network indicators also include relevant host-based indicators to allow for triage of systems under investigation.

**HOW IT WORKS**

Threat indicators are thoroughly vetted to avoid false positives, emphasizing accuracy over volume. Every indicator is validated by our analysts before being published, and can be accessed real time via a RESTful API. The feed can be filtered by Indicator Type, Severity, Confidence, Threat Type, etc. It can be requested by a GET or a POST request. The output is available in JSON format and can be directly integrated into existing security tools.
CLASSIFICATION OF RESULTS
To help prioritize indicators, iDefense provides both a “confidence” and “severity” rating for each published indicator. Armed with this information, a security analyst can quickly identify a set of priority indicators that map to the risk profile of the organization, providing a tactical countermeasure to identify and block potential malicious activity.

“Confidence” rates the analytic certainty associated with a given indicator. The Threat Indicator feed only includes indicators at a medium or high confidence. Confidence levels are defined as follows:

**Low:** This indicator is applied in relation to a compromise, but may also be applied for a legitimate purpose or because not enough information is available to verify the indicator.

**Medium:** This indicator is applied in relation to a compromise, although information about that compromise may not be specific enough to rule out false-positive hits. IP addresses, which may be part of a shared infrastructure or reassigned to non-malicious servers, are more likely to get a medium rating. A typical example might include the compromised website used to serve up a redirect iframe for the purposes of delivering an exploit kit.

**High:** This indicator is specifically related to a compromise and is unlikely to result in a false-positive. These indicators have been verified by analysts through both static and dynamic analysis. A typical example might include an operator’s command and control specified URL, as encoded and seen on the wire of a specific piece of malware.

“Severity” denotes the most likely impact of intrusion, related to the indicator in question. The levels of severity are assigned as follows:

**Low:** This category includes malware infections that are mere nuisances with little chance of data exfiltration. Rogue antivirus and adware will fall into this category.

**Medium:** Threats that are likely to steal information and possibly cause harm to systems or networks will fall into this category. Banking Trojans, such as Zeus or SpyEye, are good examples of such threats.

**High:** Threats that are related to targeted information, including cyber espionage and advanced persistent threats (APTs), fall into this category.

GET INDICATORS IN CONTEXT WITH iDEFENSE INTELGRAPH
iDefense gives customers security intelligence, including threat indicators, in context with iDefense IntelGraph—a proprietary, next-generation security intelligence platform (and API). IntelGraph allows users to search, manipulate, visualize and contextualize relationships between elements within the 18+ year iDefense security intelligence knowledge base, covering more than 70,000 products from 1,000+ technology vendors.

ABOUT iDEFENSE SECURITY INTELLIGENCE SERVICES
iDefense Security Intelligence Services gives information security executives 24/7 access to timely and actionable cyber intelligence related to vulnerabilities, malicious code and global threats. iDefense’s in-depth analysis, insight and response recommendations help keep businesses and government organizations ahead of new and evolving threats and vulnerabilities.