WEBROOT®

Threat Intelligence: What is it, and How Can it Protect You from Today's Advanced Cyber-Attacks?

A Webroot publication featuring analyst research

Issue 1

Featuring research from Gartner®

Welcome

Whether you're a network security vendor looking to bolster your solutions, or an enterprise looking to strengthen your security infrastructure, threat intelligence has become a must-have to stay ahead of today's advanced malware. The growth and sophistication of cyber-attacks against enterprises and individuals have rendered traditional cybersecurity measures virtually obsolete. The headlines are seemingly endless; companies continue to get compromised, while those responsible for securing corporate networks fall on their swords. Cybercriminals – smart, highly organized, and driven by financial motivations and/or strongly-held personal beliefs – only need to find a single vulnerability to exploit. On the other side, those endeavoring to protect assets need to set up flawless defenses. As Rob McMillan of Gartner Inc. points out in the Definition: Threat Intelligence section below:

- "CISOs have no direct control over threats to their organizations and can only be aware of the threats and prepared for their arrival."
- "CISOs should plan for not only the security threats that exist now, but also those that may emerge in the longer term."

To combat this new age of threats, more security vendors and enterprises are turning to threat intelligence. But what exactly does that mean? In the featured research Rob provides his definition of what threat intelligence really is—as well as what it isn't. This brief will provide some of the insight you need to take educated action when looking to integrate threat intelligence into your security infrastructure. In addition, you'll learn:

For this paper, "threat intelligence" is covered under the context of operational threat intelligence which can be used to set up proactive protection via policies based on IP or URL reputation, as an example, versus human-derived intelligence based on deep analysis and research of attacks or those launching them.

- What to look for in effective threat intelligence
- How advanced Big Data approaches are changing the security landscape
- Some key considerations for evaluating a threat intelligence solution

We'll also look at different ways to incorporate threat intelligence, whether you're a security vendor looking to integrate it into your solutions, or if you're an enterprise looking to bolster your security infrastructure.

From the Gartner Files:

Definition: Threat Intelligence

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Key Challenges

- Leading indicators of risk to an organization are difficult to identify when the organization's adversaries, including their thoughts, capabilities and actions, are unknown.
- CISOs have no direct control over threats to their organizations and can only be aware of the threats and prepared for their arrival.

Recommendations

- CISOs should plan for not only the security threats that exist now, but also those that may emerge in the longer term, such as three years from now.
- CISOs that utilize threat intelligence services should have a clear understanding about the characteristics that they require from such a service and should choose a service provider accordingly.

Introduction

There are many commercial providers of threat intelligence services. However, "threat intelligence" is sometimes a loosely used term, and organizations should clearly understand what services are actually provided to ensure the most value for the cost.

Analysis

Definition

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets to that can be used to inform decisions regarding the subject's response to that menace or hazard.

Context

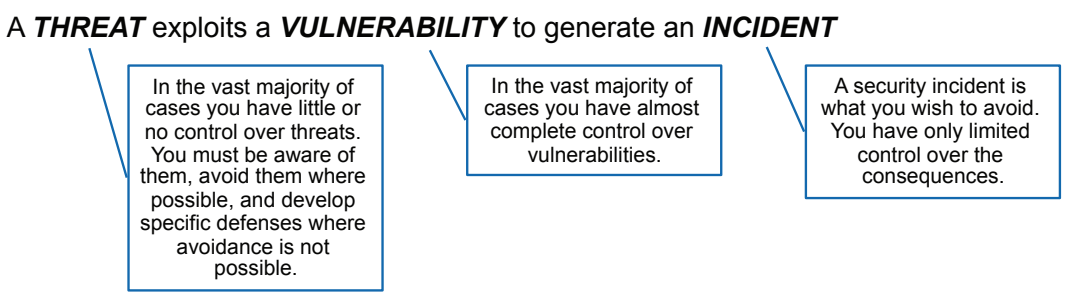
Two conditions are necessary for a security incident to occur (see Figure 1):

- A vulnerability, or weakness, must exist in some element of an organization's operations or its supply chain.
- A threat must exploit that vulnerability.

A vulnerability may exist in a variety of forms, for example:

- Unsecure software, due to a bug, bad programming practice or bad design
- Unsecure configuration of IT infrastructure
- Unsecure operational or business processes

FIGURE 1 The Prerequisites for a Security Incident



Source: Gartner (May 2013)

- Unsecure acts committed by staff or other people, by a mistake or a deliberate act

The threat is the agent (that is, a menace or hazard) that takes advantage of the vulnerability. Usually, CISOs have no direct control over the threats to their organizations. They can only be aware of the threats and be prepared for their arrival. They can exist in a variety of forms, such as:

- People (for example, "hackers" actively working to inflict damage to the physical, financial or intangible assets of the organization)
- Malware

"Intelligence" (Note 1) can be defined as:

- The act or state of knowing – the exercise of the understanding
- The capacity to know or understand
- Readiness of comprehension
- Information communicated, news, notice or advice
- Knowledge imparted or acquired through study, research or experience – general information

Attributes

- It is more-than-obvious, trivial or self-evident information about a threat. It is specific information that has been generated through some form of processing, such as collection, collation, validation, evaluation and interpretation.
- It includes value-added information that is only apparent from further analysis or correlation of multiple data points. Examples of this information include:
  - Goals of the threat actor or developer
  - Conditions under which the threat is likely to successfully exploit a vulnerability
  - Variants of the threat
  - Current activity implicating the threat
  - Outcomes for the organization should the threat successfully execute
  - Indicators that the threat is currently acting against the organization or otherwise impairing the assets of the organization
  - Defenses against the threat
- It may include formation such as an assessment of the reliability of the source of the information and reliability of the information itself.
- It may have a period of relevance, from the very brief (for example, operational intelligence about existing activity, which may be relevant for only the duration of that activity) to the very long (for example, strategic intelligence about the long-term plans that leaders of a country or other community may be making).
- For many organizations that consume threat intelligence, a key challenge is how to consume and act on that intelligence.
- It can be used to inform decisions in preparation for the threat, such as how to avoid it or reduce its potential impact.
- It can be used for responding to an incident stemming from the threat, such as identification, assessment, forensic support and remediation.

What Threat Intelligence Is Not

- It is not obvious, trivial or self-evident information about a threat that any untrained individuals of otherwise reasonable intelligence would be able to discern for themselves.
- It is not information about vulnerabilities. However, most threat intelligence service providers also provide such information.

- It is not support for incident response (for example, forensic support and compromised credential recovery), although incident response support service providers may consume threat intelligence.

Examples

Example vendors include Verisign iDefense, iSIGHT Partners and Mandiant. Most threat intelligence service providers, both government and commercial, do not make their intelligence content publicly available. However, an example was published in early 2013 by Mandiant, "APT1: Exposing One of China's Cyber Espionage Units."

A more generic list of threats, which organizations should consider as part of their security planning, is provided in Annex C of the ISO/IEC standard "Information technology – Security techniques – Information security risk management," ISO/IEC 27005:2011, Second Edition, 1 June 2011.

Note 1

Definition of "Intelligence"

As defined by Webster's 1913 Dictionary, www.webster-dictionary.org/definition/intelligence, retrieved 15 May 2013.

Source: Gartner Research, G00249251, Rob McMillan, 16 May 2013

A Big Data Approach to Threat Intelligence

Many security companies have recently turned (or are still turning to) a big data approach to security. One example is Webroot, which has been applying a big data approach to security since 2007. Rather than rely on thousands of human analysts, Webroot's approach is to capture large amounts of data from millions of their own sensors and other verified sources, then automatically analyze and classify that data within the cloud using advanced machine learning and behavioral analysis. They then apply deep contextual analysis to turn that data into relevant and actionable intelligence across a variety of Internet, File, and Mobile threat intelligence services available to technology partners and enterprises.

The Webroot® Intelligence Network

This big data approach used by Webroot is driven by the Webroot Intelligence Network (WIN), which was purpose-built to stay ahead of the ever-emerging volume and sophistication of cyber-attacks. WIN integrates billions of pieces of information from millions of sensors to create a huge threat detection net. (In addition to honeypots, spam traps, etc., each of Webroot's 8 million customers act as a sensor, automatically feeding data into WIN. An additional 27 million others are covered through Webroot technology partners, who also provide data back into the system.)

However, WIN goes beyond simple cloud-based data storage by using its massive data processing capacity to conduct real-time threat analysis in the cloud. Data is also correlated through a contextual analysis engine to produce real-time, highly accurate threat intelligence which is made available to Webroot partners and enterprise customers through their BrightCloud® Security Services for protection against both known and never-before-seen attacks.

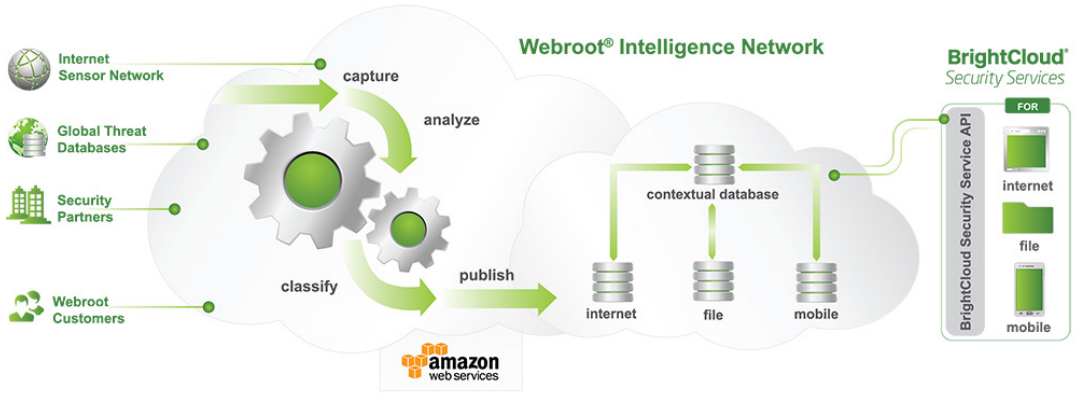
Big Data and Machine Learning

At the heart of the Webroot® Intelligence Network is Webroot's advanced machine learning approach.

On an average single day, Webroot:

- Discovers 25 Thousand new malicious URLs
- Uncovers 1 Thousand new phishing sites
- Handles over 4 Billion file lookups
- Updates a constantly changing list of 12 Million malicious IP addresses every 5 minutes

FIGURE 1 The Webroot Intelligence Network



Source: Webroot

Many security vendors today use either Bayesian Networks or Support Vector Machine (SVM) models to populate work queues for human analysts (who have a difficult time keeping up with the volume of threats, and are subject to human error). Webroot uses 3rd generation machine learning, known as Maximum Entropy Discrimination (MED), for highly accurate and scalable web threat analysis. Through MED, the Webroot Intelligence Network can classify 2,500+ URLs per second at an error rate of less than 1% (versus an average human error rate of 5-15%). To provide a sense of the volume of information, the Webroot Intelligence Network includes intelligence on:

- 13 Billion URLs
- 4 Billion File Behavior Records
- 460 Million Domains
- 900 Million IP Addresses
- 10 Million Mobile Apps

This threat intelligence is made available to Webroot technology partners and enterprise customers to help them keep ahead of the growing volume and sophistication of threats by accessing highly accurate, actionable, and relevant intelligence. Because the Webroot Intelligence Network is cloud-based, and doesn't rely on stagnant signature files:

- The vulnerability window between the launch of an attack and protection is minimized
- As soon as a threat is recognized, the entire network is protected in real time
- Few resources are needed, freeing up network space and keeping end user impact to a minimum

Source: Webroot

Consuming Threat Intelligence

Threat intelligence comes in many formats, but generally can be classified as:

- Internet: Web classification, Web reputation, IP reputation, anti-phishing
- File: file reputation (executable files, potential malware)
- Mobile: App reputation, mobile security

Security companies and enterprises integrate one or more of these depending on their needs. When selecting a threat intelligence source, it is critical to carefully evaluate:

- How and where the data is sourced, and its coverage of the global threat landscape
- The age of the data, including when it was sourced and how long it took to process
- Data efficacy, not only for false positives/negatives but also for correlation against other data
- Relevance for your specific needs, at the company, industry, or geographic level

Today, Webroot offers threat intelligence in the following categories, which may be purchased as a whole, individually, or mixed-and-matched based on need. Webroot BrightCloud® Security Services include:

- Web Classification: Provides content classification for billions of web pages to keep users safe from online threats
- Web Reputation: Forecasts the security risk of visiting a website and enables administrators to finely tune security settings
- IP Reputation: Publishes dynamic intelligence of high-risk IP addresses and insight into inbound and outbound communications

- Real-Time Anti-Phishing: Catches advanced phishing attacks by providing time-of-need protection through real-time scans before sites are visited

- File Reputation: Provides dynamic file reputation intelligence of known malicious and whitelisted files to stop the distribution of malware

- Mobile App Reputation: Categorizes and scores apps using multi-stage analysis and advanced algorithms to ensure they are safe and compliant

In addition, mobile technology partners can also incorporate a Mobile Security SDK or SecureWeb™ Browser SDK into their solutions.

Technology Partner Integration

Until recently, Webroot BrightCloud® Security Services were only available to technology partners for integration into their security or management solutions. Technology partners integrate these services through a single API/SDK, which makes incorporating one or more intelligence feeds a relatively simple process. Depending on the service and need, services can be integrated in a hosted, local database, or hybrid model, allowing partners to select the integration and deployment type best suited to their needs. Guidelines and sample code are provided for reference, and Webroot's dedicated support team is also available for assistance. Webroot technology partners who have integrated these services to-date include companies such as Cisco, F5 Networks, Palo Alto Networks, and RSA.

Enterprise Integration

Now enterprises can also take advantage of next generation threat intelligence by incorporating feeds directly into their existing infrastructure, including next generation firewall (NGFW) and security information and event management (SIEM) solutions. Enterprise customers wishing to integrate threat intelligence are able to do so through the BrightCloud connector, a virtual appliance that can be easily deployed in a VMware virtual environment on premise, or other integration mechanism specific to the enterprise's infrastructure or solution. For example:

- The BrightCloud IP Reputation Service for NGFW sends IP Reputation data to the NGFW device to block malicious IPs from penetrating the customer network. For some NGFW devices, such as Palo Alto Networks leveraging the BrightCloud connector, BrightCloud IP Reputation data can be customized for each individual PAN NGFW device in the customer environment to protect them from unknown threats targeting them.

- The BrightCloud IP Reputation Service for SIEM sends IP Reputation data to the SIEM to detect unknown IP threats. This enables the enterprise's incident response team to react quickly before IP-related incidents lead to costly breaches.

Source: Webroot

Summary

Not all threat intelligence is created equal. As Rob McMillan states, threat intelligence "is not obvious, trivial or self-evident information about a threat that any untrained individuals of otherwise reasonable intelligence would be able to discern for themselves." In order to get to actionable and relevant threat intelligence that can truly enhance a security solution or enterprise network, it has to be captured from a broad variety of verified sources, and analyzed, classified, and published in as close to real time as possible. It also has to be highly accurate and correlated against both similar and other types of disparate data points for greater efficacy. Finally, the intelligence has be relevant to your current solutions, and provide context around the threats that are targeting you or your customers.

The only way to achieve this level of sophisticated threat intelligence is by applying a big data approach to security. This permits the intake and automatic processing of vast amounts of data, and goes beyond simple queuing of data for human analysts. The speed, volume, and accuracy of this approach enables users of the threat intelligence to take proactive measures to protect their networks by setting policies specific to their needs and level of risk tolerance, such as blocking access to web sites based not only on the type of site being visited, but also its reputation score. Finally, threat intelligence needs to be simple to integrate in a manner that best suits your environment, with the ability to expand inputs as needed to meet your needs.

Source: Webroot

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to internet security with its BrightCloud® Security Services for enterprise customers and technology partners. Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held internet security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region.

To learn more about Webroot BrightCloud® Security Services, please visit www.brightcloud.com or write to info@brightcloud.com.

Contact us
Webroot
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021
USA