Addressing Big Data Security Challenges: The Right Tools for Smart Protection

Trend Micro, Incorporated

A Trend Micro White Paper | September 2012

EXECUTIVE SUMMARY

Managing big data and navigating today's threat environment is challenging. The rapid consumerization of IT has escalated these challenges. The average end user accesses myriad websites and employs a growing number of operating systems and apps daily utilizing a variety of mobile and desktop devices. This translates to an overwhelming and ever-increasing volume, velocity, and variety of data generated, shared, and propagated.

The threat landscape has evolved simultaneously, with the number of threats increasing by orders of magnitude in short periods. This evolving threat landscape, the number of sophisticated tools and computing power that cybercriminals now have at their disposal, and the proliferation of big data mean software security companies are wrestling with challenges on an unprecedented scale. Protecting computer users from the onslaught of cyber threats is no easy task. If threat detection methodologies are weak, the result is inadequate.

Successful protection relies on the right combination of methodologies, human insight, an expert understanding of the threat landscape, and the efficient processing of big data to create actionable intelligence. Understanding how data is organized, analyzing complex relationships, using specialized search algorithms, and employing custom models are critical components.

While the details of these components are not thoroughly examined here, this white paper summarizes how big data is analyzed in the context of cyber security to ultimately benefit the end user.

TODAY'S THREAT ENVIRONMENT – THE VOLUME, VELOCITY, AND VARIETY OF DATA

Today's threat environment imposes the three Vs of big data: volume, variety, and velocity. Each of these is increasing at an astounding rate and has required a shift in how security vendors manage threats.

Volume: A Growing Threat Landscape

The threat landscape is evolving in various ways, including growth in the sheer volume of threats. In the 1990s, the average personal computer user received one or two spam messages a day. As of August 2010, the amount of spam was estimated to be around 200 billion spam messages sent per day[1]. Similar increases are characteristic of file transfers and web page access. In January 2008, the industry saw more malware in one month than had been seen in the previous 15 years combined. Trend Micro estimates that the threat landscape for end users has experienced an increase of six-to-seven orders of magnitude over just the last several years.

Today's threat environment imposes the three Vs of big data: volume, variety, and velocity. Each of these is growing at an astounding rate and has required a shift in how security vendors manage threats.

The numbers are daunting, but this is only the tip of the iceberg. The Internet Protocol shift currently under way (from IPv4 to IPv6) is providing cybercriminals a new playground to exploit. Approximately four billion unique IP addresses are available for use with IPv4. This is a large, yet tractable number. By contrast, IPv6 is providing an almost infinite number of IP addresses. Growing demand for unique IP addresses for devices ranging from smart TVs to telephones motivated development of the new IPv6 standards. The goal was to generate sufficient IP addresses to avoid the need to later revisit the problem. While IPv6 fixed one problem, it simultaneously created an enormous opportunity for cybercriminals and introduced an entirely new set of challenges to the industry.

Variety: Innovative Malicious Methods

The lure of financial gain has motivated cybercriminals to implement innovative new methods and to become more thorough with each passing year. Today, cybercriminals are sophisticated, evolving their craft and tools in real time. For example, malware created today often undergoes quality control procedures. Cybercriminals test it on numerous machines and operating systems to ensure it bypasses detection. Meanwhile, server-side polymorphic threats drive rapid evolution and propagation and are undetectable using traditional methods. One hundred pieces of malware can be multiplied in thousands of different ways. And malware is no longer restricted to personal computers. Multi-platform malware means mobile devices are also at risk. By

[1] Josh Halliday (10 January 2011). "Email spam level bounces back after record low". guardian.co.uk. http://www.guardian.co.uk/technology/2011/jan/10/email-spam-record-activity.

August 2012, there were already 160,000 reported mobile malware attacks for the year. In 2011 there were only a few.

The number of distribution points for spam, viruses, malware, and other malicious tools that cybercriminals employ is constantly increasing, while geo-specific threats have become more common. A recent threat infected computer users with IP addresses based in Italy, while those who accessed the Internet from IP addresses outside Italy were connected to an innocuous web page. This requires software security company detection to become more granular geographically. Spear phishing threats now target individuals, rather than countries, cities, companies, or demographic groups – further complicating detection.

Velocity: Fluidity of Threats

The need to manage, maintain and process this huge volume and variety of data on a regular basis presents security vendors with an unprecedented velocity challenge. The fluidity of the Internet over time adds to the complexity of the problem. Unlike a physical street address, which cannot be relocated without leaving significant evidence behind, changing IP addresses on the Internet is trivial, rapid, and difficult to track. An individual or a company can move effortlessly and quickly from one location to another without leaving a trace.

Determining whether a particular Web site or page contains malicious content is fluid over time as well. Cybercriminals routinely transform legitimate sites into corrupt sites almost instantly. In one example of many such transformations, in early 2012, cybercriminals installed an iFrame redirection on a popular news site in the Netherlands. What had been a legitimate website that morning infected thousands of people as they perused the compromised site during their lunch hour.

Figure 1. The growing volume, variety, and velocity of data requires new methods of managing threats

SUCCESSFUL PROTECTION IN THE AGE OF BIG DATA

Use of Big Data to Manage Security Threats

Because of the scale of the Internet and the fact that the world's population is steadily coming online, protecting users from cybercrime can be viewed as a numbers game. The same forces that are driving big data are driving threats concurrently. New methods of addressing cyber threats are needed to process the enormous amount of data emerging from the world and to stay ahead of a sophisticated, aggressive, and ever-evolving threat landscape. No off-the-shelf solution can address a problem of this magnitude. The traditional rules of engagement no longer apply. Scaling up to manage the changes in the threat landscape is necessary, but it must be done intelligently. A brute force approach is not economically viable.

Successful protection relies on the right combination of methodologies, human insight, an expert understanding of the threat landscape, and the efficient processing of big data to create actionable intelligence.

Complicating the issue further, security software companies need to not only stop malicious behavior that has already been initiated, but to predict future behavior as well. Predicting the next threat can mean preventing an attack that could potentially cause millions of dollars in damages. Accurate prediction requires knowledge of previous history. Successful security software companies examine past behaviors and model them to predict future behavior. This means employing effective mechanisms to archive historical information, access it, and provide instant reporting and details. Consumers rarely glimpse the enormous amount of effort conducted below the surface to protect them from cyber threats.

Best Practices in Achieving End User Results

Addressing today's threat landscape requires a synergistic relationship with customers and other third parties that are constantly exposed to ever-evolving malicious content. A licensing agreement that allows customers to anonymously donate suspicious data for analysis and reverse engineering can provide valuable access to real data on real machines operating in the real world. Based on data gathered from this community network, specialized search algorithms, machine learning, and analytics can then be brought to bear on this data to identify abnormal patterns that can signal a threat.

For example, many computer users follow a typical daily pattern. That pattern may consist of visiting a news site, encountering several ad servers, and logging on to Facebook. If that pattern suddenly changes, perhaps moving the user to a domain never previously visited, this incident can be immediately prioritized for further analysis. These types of complex correlations can be identified only by a system that can perform a very large number of database searches per second.

A feedback loop for process improvement is another critical component. Keen observation and curation of key data that is fed back into the process allows for continual process improvement. Over time, the process can predict malicious behavior long before it occurs.

While big data in security is a numbers game, human experts need to play the most important role. Trained analysts need to constantly evolve the combination of methodologies, apply human intuition to complex problems, and identify trends that computers miss.

Using the right approach when an attack slips through the cracks is also crucial. A savvy security software company works directly with the ISP involved in an attack to drive a better end result. This often involves working closely with law enforcement agencies. Ultimately, relationships are formed with ISPs that drive a symbiotic relationship with a common threat protection goal. The end result is a safer Internet.

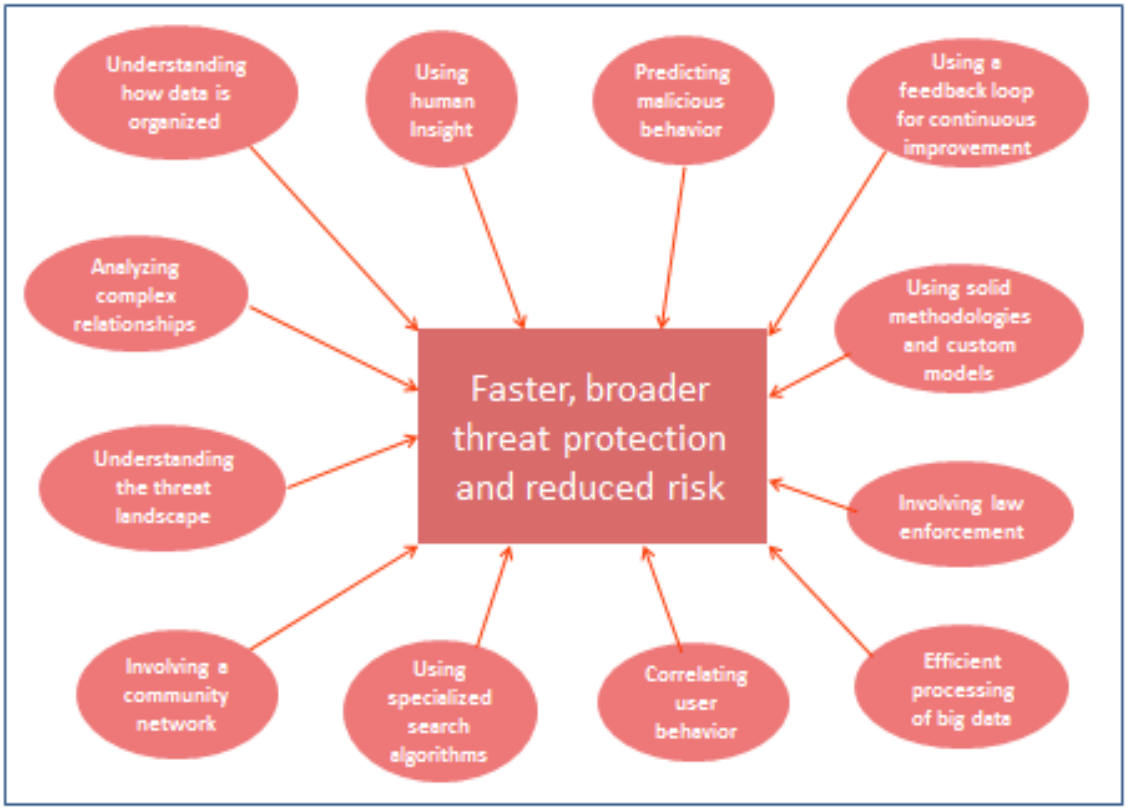

Figure 2. Core components of successful threat protection in the age of big data

CONCLUSION

Trend Micro blocks 200 million threats per day within their network of customers. Effectively managing and prioritizing the volume, variety, and velocity of data requires human insight, a multi-pronged approach, and multiple layers of defense.

Using big data tools to analyze the massive amount of threat data received daily, and correlating the different components of an attack, allows a security vendor to continuously update their global threat intelligence and equates to improved threat knowledge and insight. Customers benefit through improved, faster, and broader threat protection. By reducing risk, they avoid potential recovery costs, adverse brand impacts, and legal implications.

Smarter Protection Through Global Intelligence

The Trend Micro™ Smart Protection Network™ cloud security infrastructure rapidly and accurately identifies new threats, delivering global threat intelligence to all our products and services. Ongoing advances in the depth and breadth of the Smart Protection Network allow Trend Micro to monitor more extensively for threat data, and respond to new threats more effectively, to secure data wherever it resides.

Watch for future white papers to discuss more specific sets of best practices that are incorporated into Trend Micro's approaches and its Smart Protection Network infrastructure.

For More Information

For more information about the expanded Smart Protection Network please visit: http://www.smartprotectionnetwork.com.

TREND MICRO™
Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
Phone: +1 408.257.1500
Fax: +1 408.257.2003

www.trendmicro.com.