White Paper

Five New Laws of Antimalware Protection: Keep Up with Evolving Threats

What You Should Know to Protect Your Networks

Malware has changed considerably since early PC viruses appeared over 25 years ago. Today malware evolves so quickly that many customers find staying ahead of the latest threats nearly impossible.

In addition to the dramatic increase in malware variants, sophisticated client-side attacks and advanced persistent threats (APTs) target victims in ways that evade traditional security measures.

Advanced malware is changing the way that security is managed. The question is no longer, “Will your network be attacked”, it is “When will it happen and how will you respond.”

These are the five new laws of antimalware protection that you should know:

1. Security Is a Big Data Problem Now

Since the first antimalware technologies were introduced several decades ago, security vendors have diligently performed some degree of sample collection, sample processing, detection generation, and detection publishing. The vendors who took this approach could quickly translate back-office intelligence into customer-facing protection.

The enormous volume of data that a typical vendor must deal with today has increased dramatically. Just a few years ago, companies dealt with hundreds of daily threats. Today, they confront hundreds of thousands of threats every day. Security experts estimate that more than 280 million viruses were released in 2012 alone.

Even worse, today’s threats are highly ephemeral. Approximately 75 percent of the threats we see today have a lifetime of zero, meaning the first time we see them on an endpoint is also the last time we see them. The amount of threat-related data is rapidly expanding with no signs of abating.

2. Collaboration Is Key

Traditionally, new threats have been addressed with new technologies. Unfortunately, these technologies often aren’t designed to work collaboratively. Consider traditional antimalware vendors, who describe their protection technologies as a “stack.” This term implies that technologies operate independently from each other. Typically, one of the technologies in the stack deems a threat malicious and immediately blocks it on a system. This approach may work against simplistic threats, but by operating alone, the different technologies lose important contextual information.

Today’s advanced threats require a more collaborative approach. The different technologies should form a tightly integrated system rather than operate independently. Different protection technologies should integrate natively and work in concert to arrive at a final disposition to determine whether a particular file or application represents a threat.

3. Don’t Think Endpoint—Think Endpoints

Traditional antimalware vendors have had a singular focus on “the endpoint.” The battle against advanced malware requires a more holistic approach. Because threats typically propagate across enterprises, knowing that a single endpoint was exposed to a threat tells you nothing about how that threat may have affected the rest of the enterprise.

IT security professionals need a broader perspective to answer critical questions, including these:

- How many threats targeted the organization as a whole?
- How have threats targeted different departments in the organization?
- How does the organization compare with the global population at large?

Knowing the answers to these questions and others is important in determining how to fight advanced malware.

4. You Know Your Threat Landscape Best

The threat landscape is often addressed as a single, uniform, monolithic object. Although the term conveniently describes overall global trends, the reality is that the threat landscape looks quite different for each organization and in many cases even for the individuals within it.

Factors that contribute to the threat landscape of an organization include the organization’s size, the value of the organization’s information assets, the organization’s profile (recognition within the industry), and the vulnerability of the organization’s system. For example, a small business that offers a commoditized service has different information security concerns than a multinational corporation that designs sensitive technologies for government customers.

Those responsible for securing the organization are often in the best position to understand the unique nature of its threat landscape. In the fight against advanced malware, these same people should have the autonomy to use their domain expertise instead of having to rely exclusively on their antimalware vendor to develop protection for new attacks.

5. Detection Is No Longer Enough

The result of this rapidly growing problem is that security professionals often don’t have visibility into the latest attacks, and they struggle to maintain control after the inevitable outbreak.

There is no such thing as 100 percent effectiveness against attacks despite best intentions, so clearly detection alone isn’t enough. Today the best solutions include technologies that can help you quickly respond to the inevitable outbreak and answer critical questions like these:

- Where did it start?
- How did it spread?
- Can it be controlled?

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco provides one of the industry's most comprehensive advanced threat protection portfolios, as well as a broad set of enforcement and remediation options that are integrated, pervasive, continuous, and open. This threat-centric security model lets defenders address the full attack continuum across all attack vectors—before, during, and after an attack. For ongoing news, go to http://www.cisco.com/go/security.

For More Information

For more information about Cisco antimalware protection, visit http://www.cisco.com/web/products/security/cisco-sourcefire.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-733279-00 11/14