SOPHOS

Eight threats your anti-virus won't stop

Why you need endpoint security

by John Metzger, Senior Product Marketing Manager, and Jonathan Shaw, Product Manager

News headlines are a constant reminder that malware attacks and data leakage are on the rise. High-profile incidents that make big news might seem out of the ordinary. Yet businesses of every size face similar risks in the everyday acts of using digital technology and the internet for legitimate purposes. This paper outlines eight common threats that traditional anti-virus alone won't stop, and explains how to protect your organization using endpoint security.

Security in a digital era

Anti-virus technology was a first and extremely necessary response to security threats that have escalated over the past decade. The original anti-virus concept blocked attacks by using patterns, or signatures, to identify malicious software code. Signature-based detection was sufficient when threats were fewer, farther between and generally less dangerous.

Now that organized criminals relentlessly troll for vulnerabilities, the risk is high for any organization that uses technology in ordinary and legitimate ways. Because exposure lies in such routine situations, organizations must update their protection beyond traditional anti-virus. As news headlines show, letting your guard down has dangerous consequences. Here are eight everyday threats, related incidents from the real world and countermeasures you can put in place.

Risky business: Where you need more than anti-virus

1. The zero-day threat
2. Working outside the firewall
3. The unpatched PC
4. The uncontrolled application
5. Web insecurity
6. The lost laptop
7. Misdirected email
8. The infected USB device

Threat protection advances

Security vendors have made tremendous strides to neutralize cyberthreats that grow more prevalent, stealthy and persistent every year. Today's security software integrates the multiple layers of defense you need to combat modern threats and protect sensitive information on laptops and PCs. Endpoint protection complements network-based safeguards by protecting computers and devices from malware and data loss.

Anti-virus 1.0	Anti-virus 2.0	Endpoint security 1.0	Endpoint security 2.0
• Signature-based anti-virus protection	• Signature-based anti-virus protection • Host intrusion prevention systems (HIPS)	• Signature-based anti-virus protection • Client firewall • Suspicious file and behavior detection • Application control • Device control	• Signature-based anti-virus protection • Live, "in-the-cloud" anti-virus lookups • Location-aware client firewall • Suspicious file and behavior detection • Application control • URL filtering • Device control • Data encryption • Data loss prevention (DLP) • Single agent • One management console for all platforms

less **Protection** more

Ordinary situations, staggering consequences

1 The zero-day threat

SophosLabs receives 50,000 new malware samples daily.1 Among these are zero-day threats: malware that is not recognizable because it does not match up with earlier threats. One example is the polymorphing threat, in which the malicious code can change upon every encounter.

Zero-day threats can also exploit zero-day vulnerabilities, or previously unknown security deficiencies that software vendors have not yet patched.

Risk: Unknown or new vulnerability

Add endpoint-based countermeasures:

- Suspicious file and behavior detection
- Live anti-virus with online, real-time lookups

What can happen: The infamous Operation Aurora started as a zero-day threat by taking advantage of an unknown vulnerability in Internet Explorer. Aurora used an exploit also known as Hydraq, a malware attack that drops data-stealing malware onto users' systems.

Criminals attacked more than 30 prominent companies in late 2009 to steal intellectual property. The New York Times reported that at Google, a single click on a link in an instant message led an employee to a malware-bearing website. The employee's computer became infected and ultimately let intruders gain access to other systems in the company.[2]

What you can do: Add defenses on top of signature-based anti-virus protection. Behavior-based detection methods, such as host intrusion prevention systems (HIPS) and buffer overflow prevention systems (BOPS), monitor for suspicious actions to stop malware from executing.

Live anti-virus is another proactive tool. Your endpoint PCs connect to the security vendor's database, which checks suspect data online to identify any match with all known malware. If unknown, a sample is requested and the file is monitored for suspicious behavior. Live anti-virus discovers and contains new outbreaks faster by detecting the latest threats across a community of millions of legitimate users. These in-the-cloud lookups provide instant protection without requiring signature updates.

Detect and remove Aurora-related malware with a free tool from Sophos: http://www.sophos.com/products/free-tools/aurora-malware-removal.html

2 Working outside the firewall

Not so long ago, most employees used their computers at the office. Back then, a network or gateway firewall would have been enough to protect your servers and PCs. Now people often work outside the perimeter of the organization's network—any time they connect their laptops to the internet from airports, hotels, cafés and home.

What can happen: Using an unsecured network is risky. The Conficker worm mostly spread using vulnerable networks. The highly persistent outbreak has created a botnet consisting of millions of infected PCs. Although the botnet has not been highly active (as of June 2010), criminals can push through payloads of malicious software and spam as long as Conficker stays on unprotected systems.[3]

What you can do: Add location-aware client firewall software on laptops and other endpoint PCs. A location-aware firewall enforces tighter security when the user is connected to any non-trusted network, such as a free Wi-Fi hotspot. Client firewalls with HIPS technology let

Risk: Using an unsecured network

Add endpoint-based countermeasures:

- Location-aware client firewall
- Suspicious file and behavior detection
- Software patches

you block suspicious incoming commands, and also stop suspect outbound communication to prevent data theft. Of course, you still need a gateway firewall on your organization's network.

To halt worms such as Conficker that exploit holes in operating systems, stay current with operating system patches. That way, if an infection seeds itself on a vulnerable computer, it won't have the chance to propagate to other systems on your network (*see #3: The unpatched PC*).

Download a free Conficker removal tool: http://www.sophos.com/products/free-tools/conficker-removal-tool.html

3 The unpatched PC

You probably notice how often your network pushes security updates to your laptop or PC. There is a good reason for the frequent updates: One small unpatched vulnerability in an application, browser or operating system can lead to huge problems.

What can happen: Known threats such as the notorious Conficker invade computers through unpatched vulnerabilities. One way the Conficker worm stays alive is by re-infecting previously clean systems after an unpatched PC or contaminated device connects to an organization's network. Criminals can then instruct infected PCs to transmit valuable information. Financial account credentials are among the prized targets.

What you can do: Patching is the first line of defense against a worm like Conficker. Use network access control, or NAC, to make sure any computer you allow on your network has all current patches and anti-virus updates in place. You should apply access policies to the systems your organization manages and those you don't, such as guests' laptops.

Risk: Intrusions and breaches, including incidents that result in non-compliance with regulations

Add endpoint-based countermeasures:

- Network access control (NAC)
- Data encryption
- Content scanning with data loss prevention
- Application control

When circumstances rule out the strict enforcement of NAC, maintain an auditable record by monitoring network access closely. You may also decide to quarantine non-compliant PCs in a walled-off part of your network.

Especially when your organization has to comply with data privacy laws, complement NAC with data loss prevention measures that include data encryption and content scanning. (*See #6: The lost laptop and #7: Misdirected email.*)

Be vigilant about the applications used in your workplace; they can easily multiply the security holes for hackers to exploit. Application control (*#4: The uncontrolled application*) shuts a backdoor to malware attacks and data breaches by keeping users' PCs free of applications with known vulnerabilities, and free of applications including P2P clients that expose data to unauthorized parties.

Check your computer's security with the Sophos Endpoint Assessment Test: http://www.sophos.com/products/free-tools/sophos-endpoint-assessment-test.html

4 The uncontrolled application

Most users have favorite personal applications they want to access from your organization's network. In many situations, however, letting unmanaged applications access the web brings unacceptable risk or performance issues. Security professionals use the term "potentially unwanted applications" (PUAs) to describe instant messaging (IM), social networking sites, peer-to-peer (P2P) clients, voice over IP (VoIP) and games. Such applications increase the "surface area" that is vulnerable to attacks.

Risk: Applications with questionable security

Add endpoint-based countermeasures:

- Application control

What can happen: When not configured correctly, P2P software makes a user's data visible to other users on the file-sharing network. In early 2010, the U.S. Federal Trade Commission sent letters to almost 100 organizations whose personal information, including sensitive data about customers and employees, had leaked onto P2P networks.4

What you can do: Application control lets you block users from installing non-essential applications on their laptops and PCs, so you have fewer applications to manage and secure. You can also disallow unwanted applications that hog bandwidth on your network.

The most effective type of application control prevents unwanted applications from running at the endpoint—the PC or laptop. To stop masquerading applications from bypassing controls, it's useful to identify applications based on their identity signatures rather than by common path and file names.

Look for granular application control that lets you balance user needs with safety. For example, suppose some of your users require desktop virtualization. Granular control lets you protect the organization from unauthorized users running unknown and uncontrolled virtual machines. Then you can focus on managing the security of the authorized virtual machines.

Learn about application control and download an Application Discovery Tool: http://www.sophos.com/security/sophoslabs/application-control.html

5 Web insecurity

Criminals abuse the web as their single biggest distribution point for malware. Legitimate websites are productive targets because visitors trust them.

Risks: SEO poisoning and drive-by attacks

Add endpoint-based countermeasures:

- URL filtering
- Malware scanning

What can happen: Search engine optimization (SEO) poisoning is a growing threat. This technique uses black hat SEO techniques to get poisoned results on the first page of users' searches. Automated programs piggyback on headlines minutes after a story breaks. No trending topic is off-limits: disasters, scandals, deaths. Practically any major news story you think of has been subverted in this way.

SEO poisoning drives or redirects visitors to sites where they can be tricked into downloading malware, such as the fake anti-virus programs known as scareware. Compromised legitimate sites host most of the SEO poisoning attacks that SophosLabs observes.[5]

The drive-by download is another variation, in which criminals don't have to do anything to lure users to the site. This type of attack loads malicious code into

the browsers, or browser plug-ins, when unsuspecting visitors reach a reputable site that is compromised.

What you can do: Protect yourself and your users with a combination of URL (reputation) filtering and scanning web pages for malware. URL filtering immediately blocks sites known to host malware. For sites not on the block list, such as those newly infected, scanning the returned web page for malware prevents malicious payloads from spreading.

Get the facts about safe web browsing:
http://www.sophos.com/security/topic/web-security-myths.html

6 The lost laptop

It's not that difficult to replace any of the thousands of laptops that are lost or stolen every year. The hard part is recovering the exposed information on those computers. Because of citizen notification laws and the loss of trust, the damage is expensive even when nobody actually misuses the data.

Risk: Data exposure when a laptop is misplaced or stolen

Add endpoint-based countermeasures:

- Data encryption

What can happen: A study conducted for Intel in 2009 found that a single lost or stolen laptop cost its corporate owner an average of $49,246. The estimate included forensics, data breach, lost intellectual property, lost productivity, legal, consulting and regulatory expenses. The tab could run as high as $100,000 in some situations.[6]

What you can do: Besides keeping an eye on your laptop, encrypt data on laptops and any removable storage devices. Then no one can access the stored information without an encryption key or password. You will stop the unauthorized use of confidential information, and comply with regulations that require sensitive data to be encrypted. In many jurisdictions, even small and medium-sized businesses have to meet data protection regulations.

Data encryption should be part of your organization's larger data loss prevention (DLP) strategy that controls every means of access to confidential and personally identifiable information (PII). (*For more, see #7: Misdirected email and #8: The infected USB device.*)

Learn how to protect data with disk encryption:
http://www.sophos.com/products/enterprise/endpoint/security-and-control/disk-encryption/

7 The misdirected email

One simple slip of the fingertip—in an instant, your document goes to the wrong email address. Such a slim margin of error is unacceptable when confidential data could leak. In some organizations, insiders use email to steal data files that they sell or exploit for identity theft.

What can happen: Some data leaks are accidental. In 2009, a Wyoming bank employee inadvertently sent an email to the wrong Gmail address. In addition to the information the requester asked for, the employee made the mistake of attaching a file holding the names, addresses, tax identification numbers and loan information of more than 1,000 customers.[7]

But the intent may not be innocent. During her final day on the job in 2008, a personnel specialist at the Department of Consumer Affairs in Sacramento, California sent the names and Social Security numbers of 5,000 people on the state payroll to her personal email account.[8] (The employee was later prosecuted and convicted.[9])

What you can do: Protect against data leaks by using data loss prevention software to scan for sensitive content. You can warn the user, or block the file transfer, before information moves from the endpoint

PC into email, an internet-enabled application or removable storage. And always make sure the files are encrypted before transfer so the data cannot be exposed or misused.

When you allow data to move onto USB devices and other removable storage, use device control to safeguard information. (*See #8: The infected USB device.*) Unencrypted devices can be blocked from connecting to users' PCs.

Every time users plug a USB device into a company computer, they bypass other layers of defense such as gateway firewall protection. That makes devices with USB ports an easy means of attack. If no protection is active on the endpoint system, the door swings open to malware (and data loss or theft). Don't forget that almost any external device with a USB port can ferry malicious software.

What can happen: In 2008, U.S. Strategic Command prohibited USB storage devices on Defense Department networks after a fast-spreading worm attack. Although the blanket restriction was partially lifted in 2010, the Army continues the ban until conditions for safe use have been met.

And never assume a USB device is squeaky clean when it ships from the factory. Some reputable vendors have distributed contaminated devices. A series of incidents has made news: smartphones, MP3 players, digital photo frames,[11] cameras[12] and even memory sticks distributed at a security conference[13] have all carried malware.

What you can do: Use device control to specify which USB devices users are permitted to plug into laptops and PCs. Your situation may call for completely blocking the use of USB devices. Or, you may want to use software that allows read-only access to devices. (*Find out how to stop USB devices from being an avenue for data loss and theft in #6: Misdirected email.*)

Find out more about data loss prevention and get a free trial: http://www.sophos.com/products/enterprise/endpoint/security-and-control/dlp/

Evaluating endpoint protection: Seven questions to ask

1. How do you protect users from malicious websites when they are out of the office and surfing the internet?
2. How does your current solution protect you against unknown threats not covered by the latest protection update?
3. How concerned are you about the lag between updates from your security vendor?
4. How do you manage updating protection across your organization?
5. How many of your users have installed unauthorized applications such as VoIP, IM, P2P or games?
6. How do you ensure employees aren't saving confidential information to removable storage devices?
7. Are you able to check that all computers that connect to your network have their anti-virus and firewall turned on and Windows Update enabled?

Conclusion

As high-profile incidents show, there is no longer anything unusual about malware attacks and data breaches. Most happen in everyday circumstances, and classic anti-virus software is designed to block just some of the threats. Your best defense at the endpoint is multiple layers of protection integrated into a single solution, including live anti-virus, behavior-based detection, URL filtering, application control, network access control, data encryption, data loss prevention and device control.

Get the Sophos Endpoint Security Buyers' Guide:
http://www.sophos.com/security/topic/endpoint-security-buyers-guide.html

Sources

1. http://www.sophos.com/security/topic/security-report-2010.html
2. http://www.nytimes.com/2010/04/20/technology/20google.html?sudsredirect=true
3. http://www.computerworld.com/s/article/9177574/Big_botnets_and_how_to_stop_them
4. http://www.networkworld.com/news/2010/022310-layer8-ftc-p2p-data-leak.html
5. http://www.sophos.com/sophos/docs/eng/papers/sophos-seo-insights.pdf
6. http://news.cnet.com/8301-13924_3-10225626-64.html
7. http://www.wired.com/threatlevel/2009/09/bank-sues-google/
8. http://articles.latimes.com/2008/aug/12/business/fi-idtheft12
9. http://www.sacbee.com/static/weblogs/the_state_worker/crime-and-punishment/
10. http://www.army.mil/-news/2010/02/20/34736-ban-on-usb-devices-in-army-remains----for-now/
11. http://www.sophos.com/blogs/gc/g/2010/06/02/samsung-wave-ships-malwareinfected-memory-card/
12. http://www.sophos.com/blogs/gc/g/2010/06/08/olympus-stylus-tough-camera-carries-malware-infection/
13. http://www.sophos.com/blogs/gc/g/2010/05/21/ibm-distributes-usb-malware-cocktail-auscert-security-conference/

Boston, USA | Oxford, UK

© Copyright 2010. Sophos Plc. All rights reserved.
All trademarks are the property of their respective owners.

SOPHOS
WWW.SOPHOS.COM