SOPHOS

How unauthorized applications impact security and how you can take back control

Employees who install and use legitimate but unauthorized applications, such as instant messaging, file sharing, games and virtualization software, are a real and growing threat to business security and productivity. This paper explains why it is important to control unauthorized applications, discusses the different approaches, and highlights how integrating this functionality into malware protection is the simplest and most cost-effective solution.

By John Stringer, Product Manager and John Metzger, Product Marketing Manager

A Sophos white paper

April 2010

How unauthorized applications impact security
and how you can take back control

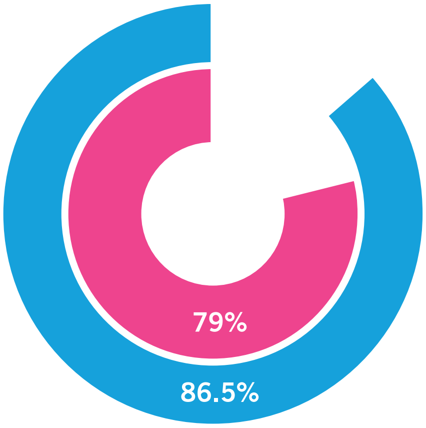
The changing perspective

IT departments have long understood the need to prevent viruses, spyware and other malicious applications or activity from compromising security and disrupting business continuity.

The rapid emergence of Web 2.0 has redefined how individuals interact with the internet, and the related technologies pose a range of new threats. Savvy users, who either have local administration rights or personal removable storage devices, are installing their own applications such as Instant Messaging (IM), peer-to-peer (P2P) file-sharing applications and (VoIP) services to help them communicate, sharefiles and work collaboratively online – for both official and unofficial business.

A recent Sophos online poll asked IT administrators to evaluate what kind of software applications they would like to prevent their users from being able to access and use. The results reveal that administrators have a clear desire to be able to exert more control and to prevent users from installing and using unwanted applications. For example, 86.5% of respondents said they would like the opportunity to block P2P file sharing applications with 79% indicating that blocking is essential.

Figure 1: Administrators want to control the use of file sharing applications.



Source: Sophos online poll, February 2010

In February 2010, the FTC notified nearly 100 organizations that sensitive data had been shared from their computer networks and was available on P2P file-sharing networks. The organizations had customer and employee information available on P2P networks that could be used to commit identity theft or fraud.

The business risk

A key part of the challenge is that many users have to be allowed to be local administrators, being given privileges necessary to download applications that they need to do their job, for example downloading updated Adobe Acrobat software. However, this means that they can also download a variety of other software that they might want to install and use. This makes life particularly difficult for the IT Administrator: malicious software would be blocked by antivirus software but applications like IM are not malicious in any way. They are not being installed automatically by stealth and are not attempting to self-replicate.

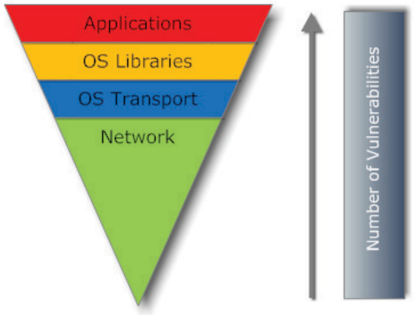
Nevertheless, the unauthorized or uncontrolled installation and use of such software by employees on business computers presents a real and growingthreat in four major areas:

- Security risks
- Legal, compliance and security breaches
- Employee productivity issues
- Extra IT support burden

Security risks

The risk of infection through unauthorized applications is clear. According to the September 2009 SANS report "The Top Cyber Security Risks," the number of vulnerabilities in applications is surpassing those in operating systems, and more exploitation attempts are being recorded on application programs[3] (See Figure 2). IM-based malware attacks, for example, are growing exponentially, and P2P applications are similarly on the increase and are notorious vectors for malicious code such as remote command execution, remote file system exploration or file-borne viruses.

Figure 2: Number of vulnerabilities in network OS and applications are on the rise



Source: 2009 SANS Report: The Top Cyber Security Risks

Legal and compliance breaches

The installation of unauthorized applications and devices can pose significant legal risk as well as security risks. The need to protect data is particularly important.

Government regulations such as the USA's Sarbanes-Oxley Act, HIPAA (Health Insurance Portability and Accountability Act) and state-level data breach disclosure laws, Canada's PIPEDA (Personal Information Protection and Electronic Documents Act), and the UK's Data Protection Act place requirements on IT administrators to maintain and protect data integrity within their networks. There is further pressure from recognized industry bodies, such as the Center for Internet Security (CIS Benchmarks) and the Payment Card Industry (PCI DSS).

Failing to protect data and comply with regulations can result in fines and, in the case of data loss, public disclosure, which has its own repercussions. Public disclosure can lead to reputation damage, loss of customers, and can even drive a company to close its doors forever.

Employee productivity issues

Although applications like VoIP IM and Facebook can have business value, non-authorized use is a distraction.

Extra IT support burden

Unauthorized applications can introduce infection to the network, but even without this, they can create an additional IT support headache. Applications that are not properly tested and deployed can cause stability performance issues across the network.

Now let's take a closer look at the applications that are introducing these risks and issues to your network.

Unauthorized applications introduce risk

Internet browsers

An increasing number of Web browsers are available to users, such as social network specialist browsers like Flock that allow users to integrate feeds from their favorite social networking Web sites. As a result, many users are rejecting company-approved browsers in favor of others that better suit their work style. When left unchecked, these unauthorized browsers can be a very real threat, as hackers regularly exploit unpatched vulnerabilities in browsers to infect users' computers.

On March 9, 2010, Microsoft warned users of a zero-day vulnerability in Internet Explorer 6 and Internet Explorer 7 that could allow remote code execution. IT administrators had to institute a workaround because a patch was not available and the vulnerability was being actively exploited by malicious hackers. By itself, this is a management headache, and the problem is compounded when users install unauthorized—and unmanaged—browsers.

> *I bet there are millions of bosses out there who hate me. If I had a penny for every hour that has been wasted playing Solitaire in the office, I could hire Bill Gates as my golf caddie.*
>
> *- Wes Cherry, Author Microsoft Windows Solitaire*

Peer-to-peer file sharing

Peer-to-peer (P2P) file-sharing applications, like BitTorrent and Limeware, are used to share files with other users connected to the same network. Many P2P applications configure read and write access to connected computers which in turn can lead to corporate files being shared. The vast majority of the files shared on P2P networks are pirated copies of copyrighted music and movies. This obviously poses a productivity issue, but it also creates a liability issue. Sharing these copies with third parties is illegal in most jurisdictions. By hosting these movies, songs, and software—albeit unwittingly—businesses make themselves vulnerable to breach of copyright litigation

Instant messaging

While enterprise-grade IM solutions are designed with security and privacy in mind, the same cannot be said for consumer IM client like Live Messenger and Yahoo! Messenger.The data transmitted over these networks is not encrypted or authenticated. As a result, data loss is a significant threat. Sensitive information sent in clear text can be intercepted, and hackers can hijack entire sessions by impersonating a user.

Synchronization tools

Synchronization tools are used to sync files and personal information between a user's computer and either a mobile device (e.g. Smartphone) or cloud based service (e.g. Gmail or Apple MobileMe). This enables users to take corporate data outside of the network, unbeknownst to IT. Once that data resides on a user-owned mobile device or within the cloud, IT no longer has control over its use. It could easily fall into the wrong hands should the device be lost, or transferred to yet another (unsecured) device where it is susceptible to theft.

Remote access systems

Remote access software like LogMeIn and GoToMyPC can be used by IT departments for remote systems management or by end users to remotely access system resources and data. Traffic between the host and remote systems is routed through servers that may not meet your organization's security requirements. Users can further expose data by accessing systems from unsecured public hosts such as those used at internet cafes.

Matching application use policy with corporate culture and need

Unauthorized applications can introduce security risks and management-complexity for IT, but of course not all applications are bad. Many applications have legitimate business purposes and are required by users to effectively do their jobs. To enable business, and not block productivity, it's critical for IT to match application-use policy with corporate culture and need.

For example, if an organization uses IM applications for legitimate business communications, its IT department must be able to allow the use of approved enterprise-grade IM clients and block those that pose risk to the company's data. Even within one organization application requirements may vary between departments. The marketing department may need consumer-grade IM clients to communicate with customers. Therefore, IT must be able to setup application control policies by group, application type and specific applications so its users don't introduce a security risk or lose a business opportunity.

The tools that enforce an organization's security policy must be flexible enough allow usage of specific applications where required, to monitor usage patterns, and provide comprehensive reporting to aid in identifying abuse, security risks, and productivity hazards.

Control strategies

In response to the wide-ranging threats posed by the unauthorized use of applications and devices, IT administrators have tried a number of different strategies. Each strategy has some merit, but there are also disadvantages.

Locking down computers

One of the most straightforward ways to restrict the use of unauthorized applications is to simply limit the provision of administrator rights. However, this is precisely where application control has broken down in the past.

Some departments—notably IT and technical support—have a clear and obvious need for administrator rights. It might seem an obvious answer to allow these technical groups to install applications and to prevent everyone else from doing so. Unfortunately, in practice this is not as simple as it sounds.

The inflexibility of the strategy means that countless policies need to be created. For example, many simple Windows functions, such as adding a printer driver, changing time zones and adjusting power management settings, are not allowed with a standard user account and therefore do require constant changing of the assigned rights. The increased staffing requirements and response times related to centrally administering every change to a computer create a significant cost for the business.

Removing administrative rights also has a limited impact as many applications either do not require these rights to install or execute (e.g., Google Chrome web browser) or are packaged in special pocket versions designed to run directly from removable storage.

But the real problem with lockdown is office politics. Computers are often considered personal property by their users who think thatand the ability to install screen savers, toolbars and games a right rather than a privilege. To implement a lockdown policy implies distrust and also creates a disparity between the treatment of administrators and those without administrator rights.

Installing specialist control products

So called “application whitelist” solutions are designed specifically for controlling which applications can and cannot be run on a computer. These products typically involve validating usage against large databases of allowed and blocked applications. Control can be extremely granular. Specific applications and even versions can be marked as authorized. By maintaining an allow list of authorized applications the IT manager can still allow users to have administrator rights where needed, but still prevent use of unauthorized applications.

These solutions have failed to gain significant market traction for several reasons. For IT administrators they are yet another product that needs to be evaluated, purchased, installed and managed. Management of these solutions is not an insignificant task and is often difficult due to the size and complexity of ***allow*** and ***block*** lists.

Finally, application control is not seen as the first line of defense within an organization—nor is it the second line of defense, and getting the budget approved to invest in extra products is not always easy.

Application control vendors realize this and now pitch their products as anti-virus solutions. However, not all malware is an application. A growing amount of malware comes in the form of HTML scripts that run within a legitimate e-mail client or Web browser. There are also macros that run in Word and Excel. You cannot replace your anti-virus software with an application control product and expect protection from all malware.

Using a client firewall

Client firewalls provide another means of controlling applications and are now a standard part of endpoint security suites.

A client firewall can help in limiting the use of unauthorized applications by controlling access to network or internet resources, for instance by looking for and blocking VoIP traffic.

However, there are two main limitations to using firewalls for applications control. First, they cannot stop applications being run—they only stop network traffic. Personal web browsers, toolbars and applications that don’t send network traffic, such as games, can still be used. Second, many of the popular IM applications are “port-agile” (such as Skype). Should their native port be closed, IM applications are capable of locating other open ports and tunnelling their traffic over a different port instead.

Getting more from an anti-virus solution

Sophos Endpoint Security and Data Protection (ESDP) includes integrated application control. This approach enables businesses to get more from their investment in protection against malware, and save system and management resources by leveraging the same scanning agent and management infrastructure.

Deploy only one client

Anti-virus software is a necessary investment that IT administrators have no choice but to purchase, install and manage. Deploying a single client that incorporates anti-virus, anti-spyware, HIPS, client firewall, data leak prevention, and control of unauthorized applications and devices will save time, money, and system resources, and improve security.

Simplify control and policy setting

Sophos ESDP allows different policies to be set for different user groups. Being able to set policies to control unauthorized applications and devices alongside anti-virus policies, can enhance efficiency and allow for specific needs of particular users.

Not all anti-virus solutions are the same

Using the same management and updating mechanisms for application control has obvious infrastructure and overhead benefits. However, the overall success of this combination of features, in terms of efficiency, depends on the actual way in which applications are detected.

Some solutions require administrators to create their own application signatures using filenames that appear in the application, and to maintain allow or block lists. This approach is time consuming and IT resource-intensive. It puts the burden of updating onto the administrator and is also unreliable as users can simply change the filename to avoid the application being detected.

SophosLabs creates and manages application detection signature in exactly the same way that malware detection is automatically updated, simplifying administration, updating and maintenance of detection. In this way, the latest versions of applications like IM and file sharing clients can be easily blocked to help prevent data loss. There is no dependency upon someone in the IT team manually updating an application signature.

Reduce the support burden

The Sophos approach not only stops applications from being run but also blocks their installation. This enables organizations to time spent by technical support staff to spend fixing computers that have been destabilized by the installation of unauthorized applications, or infected with malware that has entered systems via unauthorized devices.

Conclusion

The threats posed to corporate networks by the installation and use of unauthorized applications and devices are significant. Organizations stand to lose large amounts of money due to impacts on productivity, network bandwidth, IT support, malware threats, and data loss.

While there are a number of solutions available many require additional investment and only help IT administrators to manage the problem; they are not complete solutions. Furthermore, for many organizations, these solutions can be expensive, unwieldy, and difficult to maintain.

A better solution is one that completely integrates the blocking of unauthorized applications and devices into the existing anti-virus detection and management infrastructure. This gives IT administrators—for whom IT anti-virus protection is a must have—a simple solution that removes the cost and management overhead associated with dedicated white listing solutions from the equation.

FOR MORE INFORMATION:

Additional information on Sophos Endpoint Security and Data Protection can be found here:
http://www.sophos.com/products/enterprise/endpoint/security-and-control/

A full list of applications automatically detected by SophosLabs can be found here:
http://www.sophos.com/security/analyses/controlled-applications/

Take our application and device control capabilities for a test drive using the Sophos Computer Security Scan:
http://www.sophos.com/products/free-tools/sophos-computer-security-scan.html

Sources

1 Ponemon Institute's Fifth Annual US Cost of Data Breach Study published Jan 2010.

2 FTC notifies almost 100 organisations of P2P data leaks : http://www.sophos.com/blogs/gc/g/2010/02/23/ftc-issues-p2p-data-leak-warning-organisations/

3 2009 SANS report "The Top Cyber Security Risks" : http://www.sans.org/top-cyber-security-risks/

4 Security Threat Report 2010: http://www.sophos.com/security/topic/security-report-2010.html

5 Research Note FaceBook: Measuring the Cost to Business of Social Notworking : http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/

Boston, USA • Oxford, UK

SOPHOS
WWW.SOPHOS.COM