Academic Freedom or Application Chaos

An Analysis of Application Usage on University Networks

3rd Edition, April 2012

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 95054
www.paloaltonetworks.com

Table of Contents

KEY FINDINGS

In university IT departments, the subject of increased network security is met with varied levels of resistance that is based, among other things, on the premise of academic freedom. As a result of the educational freedom argument, university network security policies may be viewed as more open than those that might be used on an enterprise network. *Academic Freedom or Application Chaos (3rd Edition, April 2012)* from Palo Alto Networks sheds light on the types of applications in use on university networks and poses the question of whether or not the academic freedom argument is real or merely a banner behind which high risk application usage can hide. The finding that most aggressively questions this argument is the relatively high frequency of applications that enable circumvention were found. Specifically, external proxies, remote access and encrypted tunnels were all found to be in use at levels equal too, or higher than non-university environments.

Based on live network traffic assessments performed on 619 university networks between June 2009 and March 2012, the report shows that application usage is consistent when compared to the two previous reports published in 2009 and 2011 respectively. In addition to the use of circumvention tools, filesharing and streaming media continue to be popular and heavily used – to the point where 54% of the bandwidth is being consumed by these two groups of applications.

Key findings:

Circumvention tool use is high but unchanged

Compared with non-university environments, the frequency of use for external proxies and encrypted tunnels on university networks is high, while remote access tools are used at the same frequency in both environments (96%). The relatively high frequency of use introduces contradictions to the assumption that university networks are "open".

P2P filesharing and streaming media consumes 49% of overall bandwidth

Found in 94% of the participating universities, P2P filesharing consumed a staggering 29% of the overall bandwidth observed, up from 22% in the previous report, indicating that P2P remains the solution of choice for moving large files, legitimate or otherwise. Over 100 streaming media (video and audio) applications consumed 20% of the overall bandwidth.

Browser-based filesharing popularity forces use case segmentation

Browser-based filesharing remains popular with a total of 70 variants found and an average of 18 found on 97% of the university networks. Dwarfed by P2P in terms of bandwidth consumption, but more popular in terms of variants and frequency of use, this group of applications is clearly segmenting into two distinct categories: infrastructure/productivity and entertainment.

Securing port 80 does not equate to securing the network

Placing bars on the door and leaving the window open is considered poor home security. The same rule applies to focusing only on port 80 security, the attackers will merely look for another way in. The analysis shows that 68% of the applications and 75% of the bandwidth can use ports other than tcp/80 or they do not use tcp/80 at all.

The traffic analyzed in this report is collected as part of the Palo Alto Networks customer evaluation methodology where a Palo Alto Networks next-generation firewall is deployed to monitor and analyze the network application traffic. At the end of the evaluation period, a report is delivered to the customer that provides unprecedented insight into their network traffic, detailing the applications that were found, and their corresponding risks. The traffic patterns observed during the evaluation are then anonymously summarized in this report.

INTRODUCTION

Any application, anytime, anywhere. That is how most university students would respond if ask the question: what are you using on the university network today? The "any application" answer is a reasonable one, considering that most students have been raised online, and are always connected in both their personal and educational lives. If the conversation continued and the question of "why are you using these applications" was asked, then the answer might be "because I can."

Today's university student must be more computer-savvy than ever before; in fact the successful completion of a university education is dependent upon knowledge of how to use technology and in many cases, requires outright ownership of a PC, laptop or other device. The technical acumen that students have, combined with the breadth of applications, and the premise that university networks are "open" places extraordinary pressures on university security teams who are asked to enable openness, while protecting the network and the corresponding data.

In analyzing 619 university networks around the world, Palo Alto Networks found the expected range of applications that included social, entertainment, infrastructure and educational use. As with the previous two versions of this paper, filesharing and streaming media consumes the majority of the bandwidth. The use of applications that enable circumvention such as external proxies, encrypted tunneling, and remote desktop access remains high.

The consistent use of circumvention applications means that the question posed previously remains; if the network is open, then why use applications that can mask user activities? This is the key question to be answered. Secondarily, are control efforts implemented in such a way that users are being driven to use these applications? Whichever the reason, the statistics show that students are using whatever application they want and security administrators are struggling to keep pace.

CIRCUMVENTION TOOLS: STEADY OR INCREASING IN USE

One of the more interesting finding uncovered during the analysis is how frequently the use of encrypted tunnel, remote access, and external proxy applications were being used. This finding is somewhat contradictory to the assumption that university networks are "open". The theory being that if the networks are open, then why would there be a need to use applications that can bypass security? Are the students being overly cautious? Or are the universities exerting stricter traffic controls? Regardless of the underlying reasons, the frequency that these applications were seen was quite surprising.

ENCRYPTED TUNNELS: SECURITY OR EVASION?

There are two types of encrypted tunnel applications: those that are endorsed by the university and used for secure communications (e.g., SSH, SSL, IPSec, IKE, ESP, Secure Access) and those that may not be endorsed (e.g., Hamachi, Tor, UltraSurf, FreeNet). These applications were found with similar or increased frequency when compared to previous versions of this report.

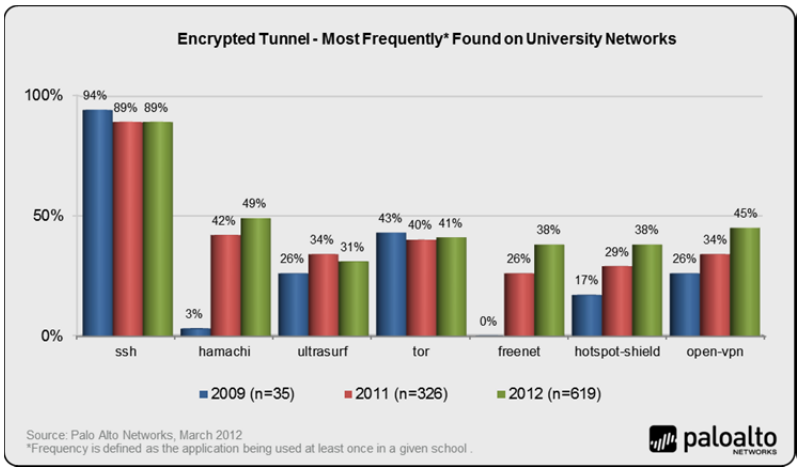


Figure 1: The most commonly detected encrypted tunnels found across the participating universities.

When looking only at UltraSurf, Hamachi, Tor, Gpass and Gbridge, at least one of these applications was found on 67% of the university networks. Comparatively speaking, in non-university environments, these applications are found on 42% of the networks (n=5,515). This set of applications warrant some added discussion around their target users and use cases. These applications describe themselves and their use-cases in one of two ways.

- OpenVPN, HotSpot Shield, and Hamachi describe themselves more aggressively as VPN security tools, with privacy from censorship a secondary message. They each have free-to-registered user versions with pay options also available. On a university network, a student using these services may be taking the correct approach to their online activity, which is to stay protected. They may also be trying to mask their activity.

- Tor, UltraSurf, and FreeNet all place a much greater emphasis on protecting the user from censorship, with privacy and security as the byproduct. The users of these applications, in most cases, are making a more concerted attempt to stay anonymous by masking their activity.

An additional data point to consider when evaluating the use case for these applications on a university network is the default port they use as shown in Table 1. The generally accepted port breakdown is as follows; well-known ports (0-1023), registered ports (1024-49151), dynamic/private (49152-65535). Three of the VPN offerings use the default port for SSL (tcp/443) and only one of them, Tor, uses it exclusively. The applications that use a non-standard or private port make it harder for the port-based security infrastructure used by most universities to know which applications are traversing the network and that lack of knowledge introduces risks.

Target Use is Security/VPN Focused		Target Use is Anti-Censorship	
Application	**Default Port**	**Application**	**Default Port**
OpenVPN	tcp/udp/1194, tcp/443	Tor	tcp/443
HotSpot Shield	tcp/443, 80, dynamic	FreeNet	tcp/dynamic
Hamachi	tcp/12975, 10080, udp 17771	UltraSurf	tcp/dynamic

Table 1: Default port breakdown for encrypted tunnel applications found on university networks.

To be clear on what this data indicates – these applications are in use on university networks, in some cases, with increasing frequency and collectively, their bandwidth consumption relatively small at 0.2%. (SSL and SSH combined consumer 4.2%). It is impossible to determine, from the data collected, which use case is most common – security or masking of activities. The purpose for the discussion is to return to the question posed earlier – if universities are "open" then why are students using applications that are clearly designed to mask activity?

REMOTE DESKTOP APPLICATIONS: TEAMVIEWER GAINS POPULARITY

Overall, 53 different remote access tools were found, with an average of seven variants in 96% of the participating universities. A few subtle changes occurred in this group of applications when compared to the previous reports. First, the growth in popularity of TeamViewer slowed a bit, gaining 7% over the previous report. The second change observed is a shift in the bandwidth consumption (not shown). MS-RDP supplanted TeamViewer in the 1% (of the total bandwidth) club. TeamViewer dropped in bandwidth consumption to 0.2%

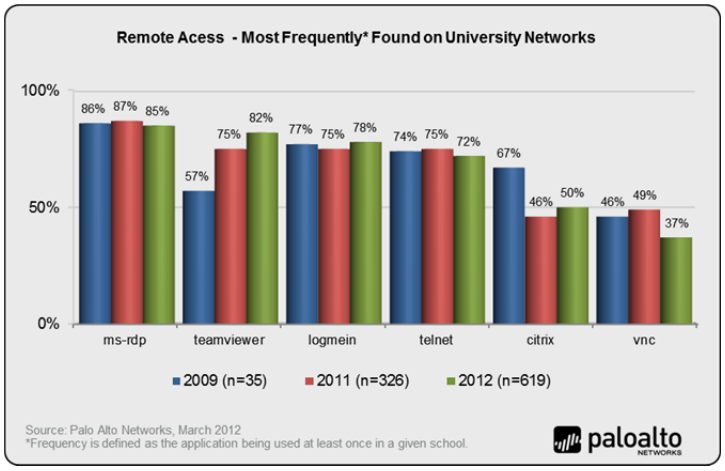


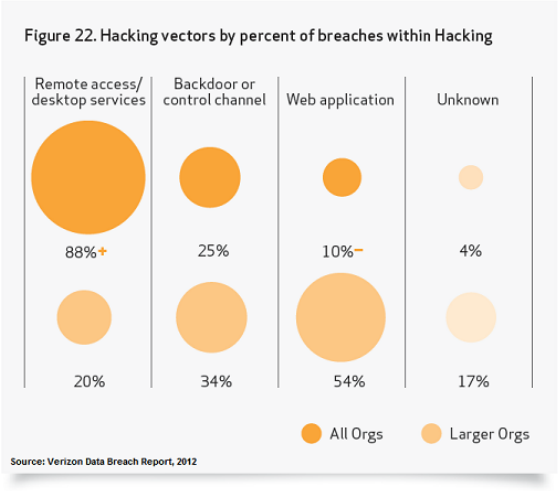
Figure 2: Most commonly detected remote desktop access applications found across the participating universities.

The target users for these tools are normally IT- and support-oriented, but the sophistication of end users has advanced to the point where the user-base is significantly broader, and at times, less diligent about security best-practices. Many IT professional are not aware of TeamViewer, a freely available remote access tool (for personal use) that is supported on a wide range of operating systems (Windows, Mac OS X, iOS, Android and Linux). To simplify remote access, TeamViewer supports browser-based control over the remote desktop.

Remote Desktop Protocol (RDP) is a well-known tool included as a utility in Microsoft Windows. RDP is a client/server application that uses port 3389 by default, but is also capable of hopping from port-to-port. Once connected, the user has full mouse and keyboard control over the managed computer while displaying everything that's happening on the screen. This means users can leave their computer at the office without losing access to files, applications, and e-mail that are on their home machines. With RDP, a student can easily configure their PC to connect to an external PC and from there can run any application they desire – swap files, run a P2P application, listen to music, surf the web – all while appearing to look like RDP traffic, a commonly allowed application on any network, university or otherwise.

The fact that most of these remote desktop control tools are readily available as part of a tool kit or an operating system lowers the barrier to entry to a point where, given some time and intelligence, a user can figure out how to use them. Most of the applications shown in Figure 2 are similar to SSH in that they can be used by IT or support to help rectify PC or server problems remotely. Without question, these applications are invaluable tools, but they can also be used by students to login to a remote machine and mask their network activity and they have become common cybercriminal targets as shown in the Verizon Data Breach Report released in March of 2012. The report shows that the list of hacking-related pathways in 2012 tells a very similar story to years past. Here is an excerpt from the report:

> *"Remote access services (e.g., VNC, RDP) continue their rise in prevalence, accounting for 88% of all breaches leveraging hacking techniques—more than any other vector. Remote services accessible from the entire Internet, combined with default, weak, or stolen credentials continue to plague smaller retail and hospitality organizations. Often these victims share the same support and/or software vendor. Scripted attacks seeking victims with known remote access ports (TCP 3389, RDP or VNC), followed with issuance of known default vendor credentials, allow for targets of opportunity to be discovered and compromised in an automated and efficient manner."*



Translating the percentage breakdown into real numbers, there were 855 breaches analyzed, 812 (95%) were attributed to hacking of some type and 715 (88%) of those 812 were remote access tool related. More simply translated, 84% of the 855 breaches were attributable to remote access tool exploitation.

More recently, $3 million USD was stolen from unsuspecting Subway customers by cyber criminals who gained access to the credit card data by performing a port scan for remote access tools and then cracking the associated passwords.

The tech-savvy student who thinks it's ok to access their home PC from the school lab or library is bypassing the school firewall, possibly on a non-standard port, and exposing the school and all the users to unnecessary business and security risks.

EXTERNAL PROXIES: USAGE REMAINS HIGH BUT FLAT

There are two types of proxies that can be used for the purposes of bypassing security controls. The first is a private proxy, which the student will install on a machine at home, or somewhere outside of the university network. The student will then browse to the external proxy as an unmonitored means to browse the web, bypassing any network controls.

- The analysis found 34 different private proxy variants (up from 30), not including HTTP proxy, which is typically deployed and endorsed by the school.
- Excluding HTTP proxy from the discussion, external proxies were detected in 85% of the networks. An average of five proxy variants were found on each network.

The primary use case for an external private proxy is to bypass filtering controls, which are commonplace in universities. The analysis shows that the most popular private proxies were detected at nearly double the rate that they were detected on enterprise networks. This indicates that students are making a more concerted effort to bypass controls than enterprise employees.

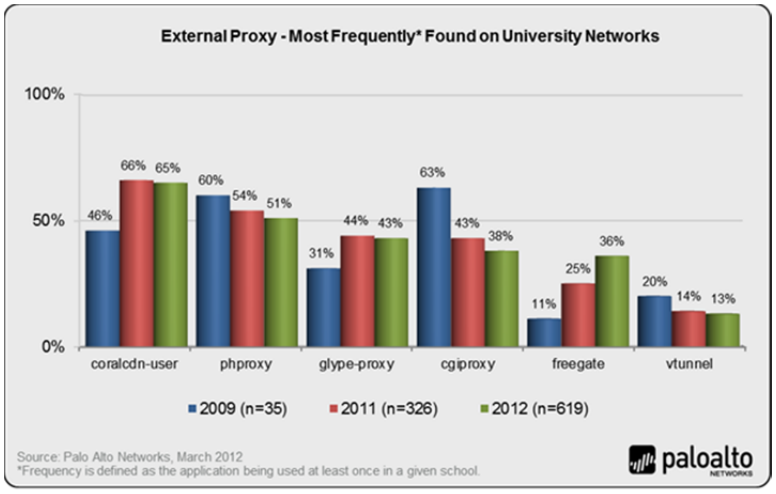


Figure 3: The most commonly detected proxies found across the participating universities.

The second proxy variant is a public proxy or a proxy service. These are merely implementations of proxy software applications (PHproxy, CGIproxy, Glype-Proxy) discussed above, but their URL has been made public for others to use on websites such as www.proxy.org. Currently, there are several thousand public proxies listed and users can sign up for an email update that notifies them of new proxy sites made available on a daily basis.

In either of these two cases, the traffic looks like normal web browsing to most security products and this type of traffic is typically allowed. The result is that students are bypassing control efforts, including threat inspection, which is exposing the school to unnecessary security and compliance risks.

P2P FILESHARING: SOLUTION OF CHOICE FOR MOVING LARGE FILES

Peer-to-peer technology by itself is a very powerful tool, leveraging shared computing resources for efficiency. The negative reputation that P2P technology has received is due to the end result of the use-case that emerged for P2P filesharing applications, not the technology itself. Viewed another way, most animal trainers will say there are no bad dogs, only bad owners; the same can be said about P2P technology, it is not bad, it is the users and the developers. The data that can be found on P2P networks is there because someone has put it there, or in the case of the inadvertent breaches, the application was not configured correctly.

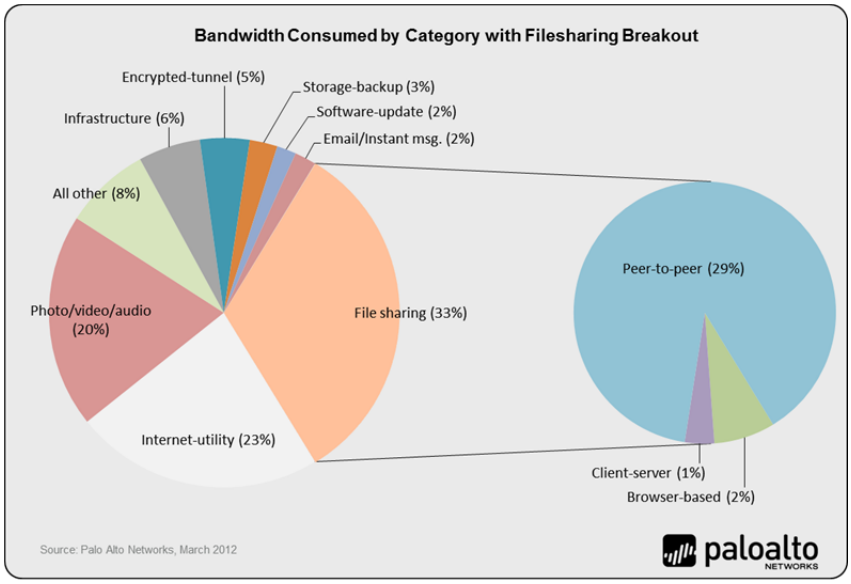


Figure 4: Filesharing bandwidth comparison breakout as a percentage of total.

A total of 34 P2P filesharing applications were found with an average of 10 of them being used on 94% of the participating university networks. While the frequency of use remained unchanged at 94%, the bandwidth consumed increased from 22% to 29%. For perspective, 29% of the bandwidth is equal to 982 two-hour HD movie downloads (3GB in size) for *each* of the 583 universities where P2P was found in use. The risks that P2P applications represent have not changed.

- Copyright infringement violation tracking, response and litigation are costly for universities that have increasingly constrained budgets.
- Inadvertent loss of personal or private data through a misconfigured P2P client.
- Commonly used for threat propagation and/or command/control. Previous versions of this report highlighted the now defunct Mariposa botnet as an example of a threat using P2P as its propagation mechanism. Newer examples include TDL-4 which uses the KAD P2P network as a means of command and control.

Educational freedom proponents will often use access to Linux binaries and efficiency in moving large research files as arguments against P2P control. The hole in that argument is that the binaries can be found easily elsewhere and there are other tools that can move large research files, and in both cases, those tools present lower risks to the network, the school, and the individual.

BROWSER-BASED FILESHARING: POPULARITY DRIVES SEGMENTATION

Browser-based filesharing applications have made moving large files a very simple task for the masses. Large graphics files that cannot be sent via email due to size restrictions can now be transmitted using YouSendIt! or drop.box. These applications are easier to use than both FTP and P2P – everyone has access to a browser, allowing the sender to upload a file, grab the URL and send it to the recipient. The dark side of these applications is that they make it very easy to illegally share copyrighted information, and are difficult to detect and control.

The analysis of showed that a total of 70 browser-based filesharing applications were found (compared to 34 P2P), with an average of 18 variants found on 97% of the university networks. The most commonly detected are shown in Figure 6.

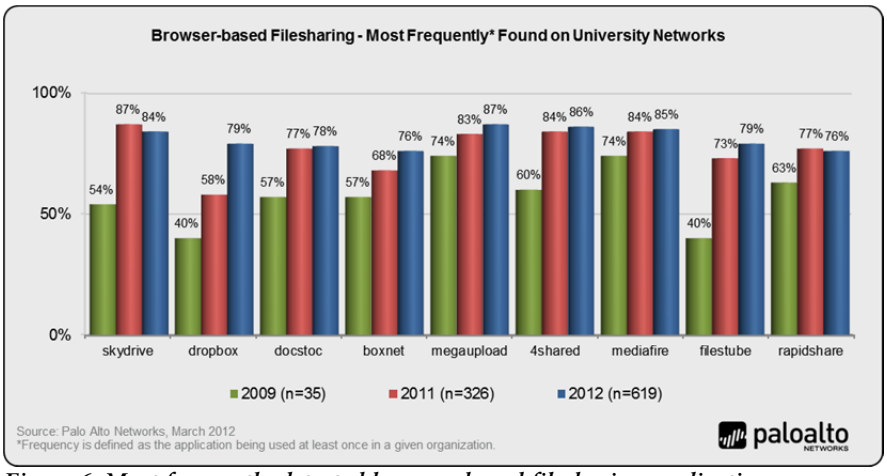


Figure 6: Most frequently detected browser-based filesharing applications.

The initial use case for browser-based filesharing was to bypass the file size limitations in email with a mechanism that was as easy as email file attachments. Previously, FTP may have been used, but it requires some technical acumen to use, and these new browser-based filesharing applications are point and click easy. YouSendit! allows a user to upload a file and a URL for the download is sent to the intended recipient. With at least 70 application variants, segmentation into different use cases has occurred with two clear cases emerging: productivity (education)-oriented or entertainment-oriented.

BROWSER-BASED FILESHARING USE CASE: PRODUCTIVITY

The browser-based filesharing applications that fall into this use case are those that are used by students and/or staff to further their education or get their jobs done. This use case is defined based upon how the application vendor positions and markets the application and the application user experience.

- **Box.net:** This application is clearly focused on being part of an organization's IT infrastructure with a range of solution offerings that include managed file transfer, cloud-based file server, FTP replacement and document/content management. The content management solution integrates with a wide range of collaborative tools including SharePoint, EMC Documentum and Lotus Notes. Like most of the other offerings, Box.net has a free service offering and a fee-based upgrade option that provides better performance, more flexibility, and integration options.

- **Dropbox:** Dropbox has evolved from browser-based only to the point where a new user is "encouraged" to install the Dropbox client. Once registered, the browser-based version of Dropbox becomes available. Once a user is registered and the client is installed, a folder is accessible on the user's desktop that synchronizes with the web-based folder. Files can be dropped into the folder for transfer using either the client version or the browser-based version. In addition to the file transfer functions, users have access to several advanced features: bandwidth control, automatic folder synchronization (defaults to yes), and configuration of proxy and port. For application developers, Dropbox has an API that can be used to deliver version or feature updates to their applications.

- **Yousendit!:** This application is commonly used to help users bypass the email file attachment limitations with a very simple and straightforward process: login, select send, pick the files to send, enter email address(es) and go. Other features include receipt confirmation and folders that allow users to store their files in the cloud. To more firmly encourage this action, users decline this option every time that a file is uploaded. A premium fee-based service includes more storage and a client to enhance the file management and upload process.

BROWSER-BASED FILESHARING USE CASE: ENTERTAINMENT

Several of the browser-based filesharing applications are clearly focused on the entertainment segment (music, movies, games and software applications). This use case definition is derived from how the application vendor markets the application, the application user experience, and the volume of bandwidth used when compared to others in the same category. For many of these applications, a registered user can browse a library of downloads as well as upload their own files.

- **FilesTube:** This application allows users to search for shared files from various file hosting sites, including FileServe, FileSonic, Megaupload (now defunct), 4shared, Rapidshare, Hotfile, Mediafire, Netload and many others. Once registered, a user can browse videos, games, software and lyrics categories, or they can subscribe to groups or create their own groups. A brief scan of the files available for download shows that they range from homemade movies to production-class movies – some of which appear to be only in theaters at the current time. Note that the low volume of bandwidth for FilesTube is somewhat misleading because the links and related downloads will come from the hosting site (listed above) and not FilesTube.

- **4Shared:** Allows users to store files privately or share them for all users. A quick view of the files displayed here http://search.4shared.com/q/1 supports the media centric use case. Like the now defunct MegaUpload, 4shared is community-based, although private online storage and file synchronization is fully supported. By default, the user files posted and the user's profile is shared with everyone.

- **Megaupload:** Prior to being taken down by the U.S. government, this application was very community based with a top-100 download list that is derived from user activity. Once registered, a user could build "credits" which may be used to improve download performance, a model that closely follows P2P filesharing. Of the top-20 file downloads found on December 5th 2011, six of the files were software applications, eight were games or game demos, and six were movie trailers.

  Like many of the applications within this category, Megaupload had a tier-based service model, with a free version as well as several pay or premium service offerings. The premium service offerings provided users with a client to simplify the management of the users file uploads. In addition to the tiered services, Megaupload also provided an API that allows users to embed an upload "folder" on their website. In addition to the API, users could use either tcp/800 (mdbs_daemon or remote control) or tcp/1723 (PPTP) as their download port (instead of tcp/80). Using the port configuration option allowed users to more easily bypass network security controls.

An average of 18 different browser-based filesharing applications were found in 97% of the 619 participating schools. The use case definitions and the discussion from above, and the frequency of usage along with the bandwidth consumed shown in Figure 7, provides some added clarity on how the application is being used.

The now defunct MegaUpload, was found in 87% of the networks consuming 37% of the category bandwidth while MediaFire was found in 85% of the participating schools and consumed 22% of the browser-based filesharing bandwidth. Comparing these applications and the frequency of use to the productivity set of applications; the differences in bandwidth consumption are significant and act as another datapoint supporting the market segmentation.

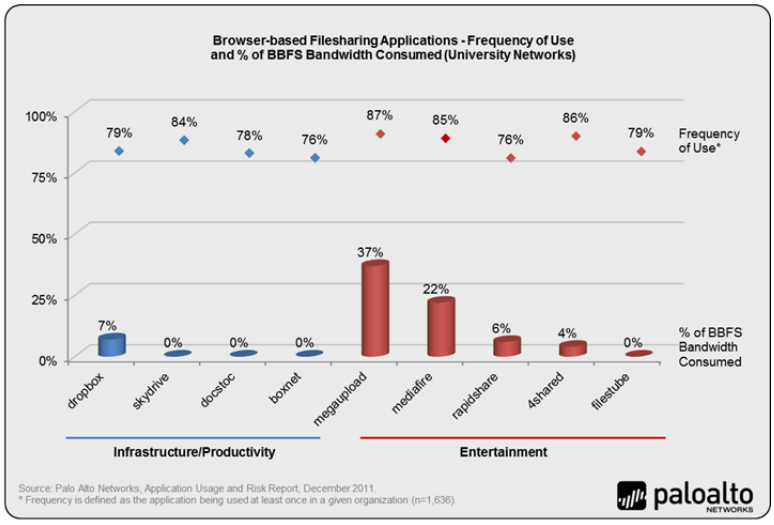


Figure 7: Frequency of use and percentage of browser-based filesharing bandwidth consumed.

In contrast, SkyDrive, Docstoc and YouSendit! were used in more than 76% of the schools, yet their bandwidth consumed was nearly immeasurable as a percentage of the category bandwidth, which strongly implies that the files are smaller in size, perhaps similar to large PowerPoint files, Illustrator graphics files or PDFs. This indicates a higher likelihood that the usage is for educational-related purposes, as opposed to entertainment.

BROWSER-BASED FILESHARING: WHAT ARE THE RISKS?

As browser-based filesharing applications segment into distinct use cases, and they add end-point clients as a form of premium service, comparisons to P2P applications will be drawn. Table 2 shows how similar the two groups of applications are from the standpoint of their use case and the ports they use. Moving away from the comparisons to P2P for the moment, all applications, business or personal, carry some level of business and security risk that may include network downtime, compliance violations, and increased operational expenses. Browser-based filesharing applications are no different than any other popular application which has a direct impact on an organization's overall risk and exposure to threats. As discussed previously, the ability to transfer files of virtually any size quickly and easily makes these applications attractive to users both for business and personal reasons. The ease of file transfer along with the ubiquity, then anonymity and the low cost (free), make these applications attractive to cybercriminals as well.

Characteristic	Browser-based Filesharing	P2P Filesharing
Frequency of use?	Found in 97% of the 619 university networks analyzed	Found in 95% of the 619 university networks analyzed
Enable efficient distribution of large files?	Yes	Yes
Legitimate uses?	FTP or email attachment alternative for sending large files	Known source of Linux binaries and large files within research communities
Known illicit uses?	• Distribution of copyrighted information such as movies, TV shows, and music • Malware delivery via infected media or image files	• Distribution of copyrighted information such as movies, TV shows, and music • Malware delivery via infected media or image files • Bot propagation (Mariposa)
Sharing methodology	1 to 1, or 1 to a few	1 to many
Risk of "inadvertently" sharing private data?	Low – although increasing as they add clients as premium services	Medium to high
Number of variants found	70	40
Use port 80 exclusively?	35 (50%)	3 (8%)
Use port 443 exclusively?	5 (7%)	None
Use port 80 or port 443?	22 (31%)	None
Hop ports?	5 (7%)	19 (48%)
Use non-standard ports?	3 (7%)	18 (45%)

Table 1: Behavioral characteristics comparison between browser-based and P2P filesharing applications.

BUSINESS RISKS

- **Potential copyright violations:** The same application that is useful to the user for sending large PowerPoint files is also potentially just as valuable for moving illegal music, movies, or even large amounts of sensitive enterprise data. Several of the media focused browser-based filesharing applications discussed above have been found to be in violation of copyright laws, or have been accused of copyright violations. Managing responses to the RIAA is a very costly and time consuming process.

- **Inadvertent data loss/sharing:** Some of the most highly publicized P2P-related data breaches were inadvertent, traced to either a misconfigured P2P client or other user errors. Initially, browser-based filesharing applications dramatically reduced the risk of inadvertent sharing because their initial focus was on one-to-one distribution or one-to-a few. As many of these offerings added clients and premium services, the risks increased. For example, the Dropbox client creates a folder on the Windows desktop that, by default, automatically synchronizes desktop folder to the cloud-based folder. If a proprietary file is dropped into the folder accidently, it is automatically shared with those who have folder permissions. The risks, while still lower than those associated with P2P, have increased in conjunction with the usage and should be addressed.

SECURITY RISKS

In addition to the compliance risks introduced, these applications present an ideal infrastructure for cybercriminals and their malware. File transfer applications have long been associated with malware. Peer-to-peer file transfer applications, for example, have been notorious in this respect for years (Mariposa most recently), and malware has been using FTP for communication for an even longer period of time. Put another way, whatever mechanism is used to electronically transfer files, is also commonly used to move malware, and browser-based file transfer applications are the latest front in this evolution. Browser-based filesharing applications have unique characteristics that make them uniquely suited for cybercriminals.

- **Free and anonymous:** Since these applications are typically free (or at least offer free versions), a cybercriminal can easily upload malware anonymously. Most only require an email address in order to use the service, so the cybercriminal can remain virtually untraceable simply by using a disposable email address and a network anonymizer, a proxy or circumventor. Furthermore, the ease with which attackers can upload files means that they can easily and continually update and refresh their malware in order to stay ahead of traditional antivirus signatures.

- **Simple and trusted:** A key reason for the popularity of browser-based filesharing applications is the fact that they make file transfers very easy. They are easily built into the browser or even the application tray of the operating system. This means that file transfers are almost as simple as clicking on a link, which vastly increases the opportunities for a target user to be lured into a dangerous spear-phishing click. Several of the offerings provide an option that enables folders and shared files to be embedded into web site while other application offerings include a developer API.

- **Ongoing control:** A common, though not universal feature of browser-based filesharing applications is the ability to regularly sync files or entire directories. This sort of capability is already being marketed as a method for delivering and updating applications. This functionality could easily benefit malicious applications just as much as legitimate applications. A key requirement for modern malware is to establish a method of command and control in which the attacker can direct the malware, update the program and extract data. An attacker could use this syncing ability to perform all of these functions under the cover of a legitimate application.

When compared to non-university environments, both types of filesharing applications are used frequently, exposing the university to unnecessary risks. The challenge that universities face is the academic freedom argument, which at times, makes security policy enforcement difficult. Network administrators will need to pay closer attention to the use of these applications as a means of protecting the school from copyright infringement and minimizing the propagation of threats.

STREAMING MEDIA: ENTERTAINMENT, EDUCATION OR BOTH?

As the cost of bandwidth continues to drop, universities are able to increase the size of their Internet connection to deploy more online offerings, and provide their students with an improved end-user experience. High-speed connectivity, combined with increased amounts of content that may not be educational in nature, means that university networks are saturated to the point where university business and research applications may suffer.

The analysis found that roughly 31% of the applications found (382 of 1,248), were consuming 77% of the total bandwidth observed. For comparison, the same categories within non-university networks represent roughly the same number of applications 30% (402 of 1,338) of the applications but they consumed 58% of the total – nearly a 39% differential. The most striking element in the bandwidth comparison is not so much the total bandwidth itself, but the significant variances at the categorical level.

Application Category	Non-University Networks		University Networks	
	# of Applications (n=1,338)	% of Total Bandwidth	# of Applications (n=1,248)	% of Total Bandwidth
File-sharing	150 (11%)	9%	141 (11%)	33%
Photo-video	108 (8%)	1%	105 (8%)	19%
Audio-streaming	37 (3%)	0.2%	35 (3%)	1%
VoIP-video conferencing	55 (4%)	2%	50 (4%)	1%
Internet-utility	52 (4%)	46%	51 (4%)	23%
Totals	**402 (30%)**	**58.2%**	**382 (31%)**	**77%**

Table 1: Category breakdown including number of applications and percentage of total bandwidth consumed.

On university networks, filesharing of all types and photo/video applications are consuming up to more than five times the amount of bandwidth than on non-university networks. As shown earlier, the bulk of the filesharing traffic is across a range of P2P networks. In terms of photo/video applications, YouTube, PPStream and HTTP video were the top consumers of bandwidth, indicating that there may be a valid mix of educational (YouTube, HTTP video) and entertainment (PPStream) oriented content.

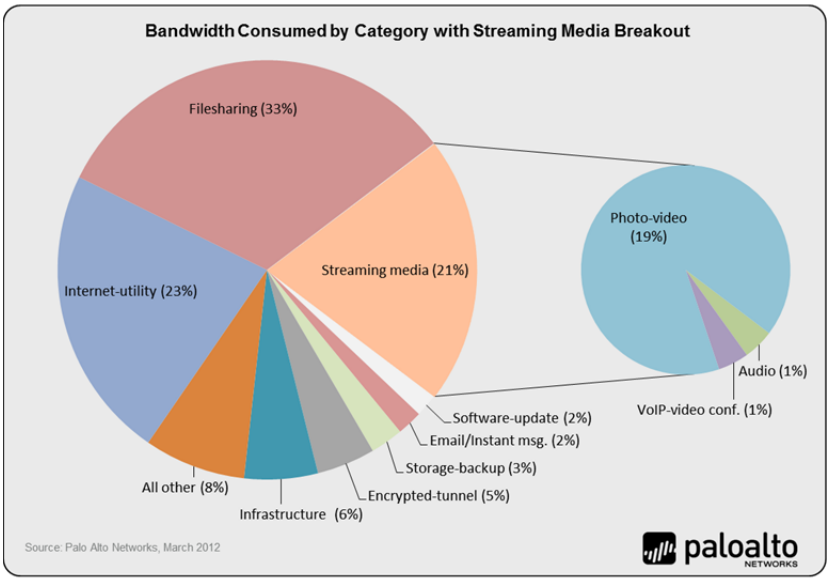


Figure 4: Streaming media bandwidth consumption comparison as a percentage of total.

On non-university networks, Internet utilities are consuming nearly double the bandwidth when compared to university networks. Examples of internet utility applications include web-browsing, a wide range of toolbars, and several Google tools. The usage of these applications in both environments indicates heavy use of the web to accomplish daily tasks.

IF PORT 80 IS SECURE, THEN STUDENTS ARE PROTECTED, RIGHT?

There is a prevailing belief that the majority of the application traffic and related security issues are a result of applications traversing tcp/80. This belief is based not only on the previous discussions around social networking and browser-based filesharing, but also on the highly publicized security incidents that have been propagated across web-based applications. As shown in Figure 9, the 1,248 applications and associated bandwidth were broken into three groups based on the default port they use:

- Applications that use tcp/80 only.
- Applications that use tcp/80 as well as others including tcp/443 or port hopping.
- Applications that do not use tcp/80 at all.

The analysis showed that 941 of the 1,248 applications found (75%) can use ports other than tcp/80 or do not use tcp/80 at all. These applications collectively consumed 68% (49% + 19%) of the bandwidth observed. This means that if an organization chooses to take the path of fortifying and protecting only tcp/80, then they risk missing a significant portion of the traffic and the associated security risks.

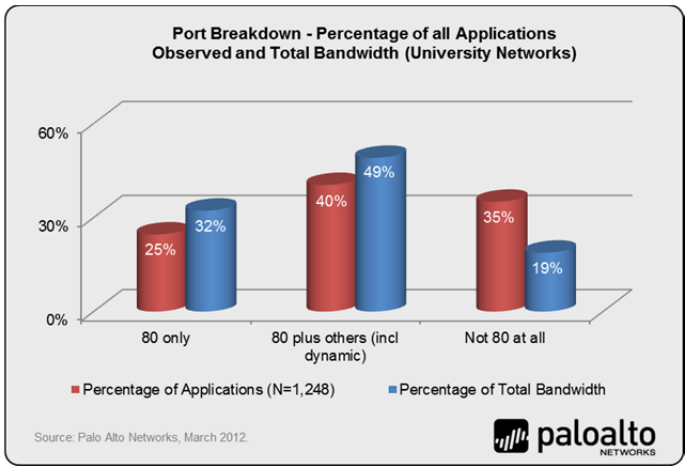


Figure 9: Applications observed based on port groupings.

APPLICATIONS USING TCP/80 ONLY

This set of 307 applications only uses tcp/80 - no other port is used by default. Applications in this group are primarily browser-based with a small percentage using either P2P or client-server technology. Examples include social networking, webmail, browser-based filesharing, Internet utilities (tool bars, etc.), and web posting. The applications within this sample are to be expected, with some exceptions such as software updates for Adobe, Google, Apple, and TrendMicro; all of these are client-server applications that use tcp/80 to ensure that the application is kept up-to-date.

The risks to students are content-filtering related; if nearly 50% of the bandwidth is consumed by tcp/80 only applications, then the question of whether or not the content is educationally oriented arises. The security threats are the to-be-expected viruses, spyware, and other types of malware associated with these applications; how will a resource-starved IT department protect the network from the deluge of malware?

APPLICATIONS USING TCP/80 OR OTHER PORTS

This set of 504 applications (40%) may use tcp/80, but may also use other ports such as tcp/443, a range of ports or may hop ports (tcp/ or udp/dynamic). The applications within this group include webmail and instant messaging, filesharing, audio streaming, gaming, encrypted tunnels, business systems, proxies, and a few remote access clients.

As applications expand beyond tcp/80, the underlying technology becomes more varied, emphasizing the fact that application developers ignore the traditional port-based development methodology. Developing an application that is "dynamic" helps ensure that the application is accessible by nearly any user no matter what controls are in place. Nearly all P2P filesharing applications are in this group, which exposes organizations to business risks that include possible copyright violations and data loss – inadvertent or otherwise. Instant messaging applications are also commonly found within this group of applications. In the case of RPC, the dynamic nature of the application is how it has been designed to operate; yet RPC is a regular target for cybercriminals. The security risks associated with this group of applications include propagation of malware, extraction of data, and targeted threats.

APPLICATIONS THAT NEVER USE TCP/80

The 437 applications (35%) in this group do not use tcp/80 at all, nor are they dynamic (hop ports) in their method of communications. The applications in this group are skewed more towards the traditional "business" applications and include database, authentication services, management, storage/backup, remote access, and gaming and Internet utilities. This group includes three very popular targets for cyber criminals – SMB, FTP and SQL. It is not uncommon for SQL developers to establish SQL instances on non-standard ports, thereby further increasing both the business and security risks and despite their "age", SQL injection attacks remain one of the most common attacks that cybercriminals will execute.

Another example of an application that falls into this category is PPTP, which uses tcp/1723, a port that is commonly used and left open on traditional firewalls. In an example of how application developers ignore port and protocol methodologies, Megaupload, discussed in the browser-based filesharing section later in this paper, can be configured to use tcp/1723 (or tcp/89) instead of tcp/80.

Hidden within the group of applications that never use tcp/80 are 29 (out of a total of 53) remote access control applications. As discussed earlier in this paper, these applications are powerful business tools that enable IT and support personnel to rectify computer and networking issues remotely. They have also become commonplace for IT savvy employees to use as a means of bypassing security controls and cybercriminals are taking full advantage of this pattern.

SUMMARY

University networks are commonly viewed as open environments that can foster education and research. The findings support this view with the wide spread use of non-education related applications. However, students are using applications that enable them to mask their activities and these applications are invisible to port-based security solutions.

Earlier in the paper, we postulated that the question of "why are you using these applications" might be answered with "because I can," or "because it is cool." These applications introduce business and security risks to the network and may best be answered with "just because you can, does not mean you should." In order to regain visibility into what students are doing, universities need to deploy solutions that provide visibility into the applications (not ports or protocols) on the network and then control them where appropriate.

APPENDIX 1: METHODOLOGY

The data in this report is generated via the Palo Alto Networks Application Visibility and Risk assessment process where a Palo Alto Networks next-generation firewall is deployed within the university network, in either tap mode or virtual wire mode, where it monitors traffic traversing the Internet gateway. At the end of the data collection period (up to seven days) the data is extracted (with permission from the university) and used to generate an Application Visibility and Risk Report that presents the findings along with the associated business risks, and a more accurate picture of how the network is being used. The data from each of the AVR Reports is then aggregated and analyzed, resulting in *Academic Freedom or Application Chaos*.

Delivered as a purpose-built platform, Palo Alto Networks next-generation firewalls bring visibility and control over applications, users and content back to the IT department using three identification technologies: App-ID, Content-ID, and User-ID.

- **App-ID:** Using as many as four different traffic classification mechanisms, App-ID™ accurately identifies exactly which applications are running on networks – irrespective of port, protocol, SSL encryption or evasive tactic employed. App-ID gives administrators increased visibility into the actual identity of the application, allowing them to deploy comprehensive application usage control policies for both inbound and outbound network traffic.

- **Content-ID:** A stream-based scanning engine that uses a uniform threat signature format detects and blocks a wide range of threats and limits unauthorized transfer of files and sensitive data (CC# and SSN), while a comprehensive URL database controls non-work related web surfing. The application visibility and control delivered by App-ID, combined with the comprehensive threat prevention enabled by Content-ID, means that IT departments can regain control over application and related threat traffic.

- **User-ID:** Seamless integration with Microsoft Active Directory links the IP address to specific user and group information, enabling IT organizations to monitor applications and content based on the employee information stored within Active Directory. User-ID allows administrators to leverage user and group data for application visibility, policy creation, logging and reporting.

Purpose-Built Platform: Designed specifically to manage enterprise traffic flows using function-specific processing for networking, security, threat prevention and management, all of which are connected by a 20 Gbps data plane to eliminate potential bottlenecks. The physical separation of control and data plane ensures that management access is always available, irrespective of the traffic load.

To view details on more than 1,400 applications currently identified by Palo Alto Networks, including their characteristics and the underlying technology in use, please visit the Applipedia (encyclopedia of applications) at the following URL: http://ww2.paloaltonetworks.com/applipedia/

APPENDIX 1: APPLICATIONS FOUND

The following table lists the applications that were found on the university networks and are ranked in terms of frequency. To view details on the entire list of 1,400+ applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications at http://ww2.paloaltonetworks.com/applipedia/

1. **dns (100%)**
2. ssl
3. web-browsing
4. ntp
5. icmp
6. flash
7. ms-update
8. facebook-base
9. netbios-ns
10. twitter-base
11. google-analytics
12. gmail-base
13. http-audio
14. ping
15. rss
16. google-safebrowsing
17. webdav
18. youtube-base
19. http-proxy
20. google-video-base
21. soap
22. smtp
23. http-video
24. ftp
25. adobe-update
26. google-docs-base
27. flickr
28. rtmpt
29. yahoo-im-base
30. hotmail
31. sharepoint-base
32. yahoo-mail
33. photobucket
34. google-toolbar
35. facebook-chat
36. apple-update
37. silverlight
38. rtmp
39. linkedin-base
40. stumbleupon
41. msn-base
42. google-desktop
43. ldap
44. facebook-mail
45. skype
46. bittorrent
47. yahoo-toolbar
48. dailymotion
49. myspace-base
50. skype-probe
51. symantec-av-update
52. limelight
53. google-app-engine
54. facebook-apps
55. google-picasa
56. office-live
57. asf-streaming
58. google-talk-gadget
59. ssh
60. mobile-me
61. babylon
62. stun
63. web-crawler
64. flexnet-installanywhere
65. pop3
66. msn-webmessenger
67. megaupload
68. google-earth
69. 4shared
70. twitpic
71. google-talk-base
72. mediafire
73. msn-voice
74. netbios-dg
75. snmp
76. megavideo
77. ms-ds-smb
78. ms-rdp
79. skydrive
80. rtmpe
81. teredo
82. facebook-social-plugin
83. shoutcast
84. rtsp
85. ooyala
86. metacafe
87. sip
88. salesforce
89. ustream
90. atom
91. mail.ru-base
92. teamviewer
93. last.fm
94. itunes
95. rtp
96. gmail-chat
97. dhcp
98. ike
99. ipsec-esp-udp
100. msrpc
101. dropbox
102. facebook-posting
103. filestube
104. myspace-video
105. yahoo-webmessenger
106. docstoc
107. google-cache
108. time
109. logmein
110. twitter-posting
111. emule
112. t.120
113. friendfeed
114. meebo-base
115. boxnet-base
116. rapidshare
117. slp
118. yahoo-voice
119. **google-translate (75%)**
120. vimeo
121. orkut
122. jabber
123. adobe-media-player
124. msn-file-transfer
125. hulu
126. steam
127. plaxo
128. squirrelmail
129. sky-player
130. ocsp
131. justin.tv
132. tidaltv
133. tudou
134. syslog
135. ssdp
136. blogger-blog-posting
137. flixster
138. imap
139. telnet
140. rtcp
141. ares
142. bbc-iplayer
143. livejournal
144. aim-mail
145. eset-update
146. gnutella
147. depositfiles
148. grooveshark
149. google-calendar
150. mssql-mon
151. sightspeed
152. youku
153. aim-express-base
154. kerberos
155. azureus
156. xunlei
157. ipv6
158. live365
159. ebuddy
160. meebome
161. gmail-enterprise
162. blog-posting
163. backweb
164. qq-base
165. napster
166. netbios-ss
167. coralcdn-user
168. webshots
169. blackboard
170. ppstream
171. trendmicro
172. evernote
173. outlook-web
174. netlog
175. qvod
176. vkontakte-base
177. facetime
178. akamai-client
179. msn-toolbar
180. qq-mail
181. pandora-tv
182. playstation-network
183. mssql-db
184. daum
185. ms-groove
186. yum
187. clearspace
188. yousendit
189. ichat-av
190. channel4
191. hotfile
192. esnips
193. friendster
194. imesh
195. sendspace
196. worldofwarcraft
197. aim-base
198. fotki
199. millenium-ils
200. upnp
201. flashget
202. hp-jetdirect
203. imvu
204. lpd
205. veohtv
206. divshare
207. nintendo-wfc
208. imeem
209. radius
210. myspace-im
211. twig
212. yahoo-douga
213. mogulus
214. source-engine
215. irc
216. mysql
217. pandora
218. sina-weibo-base
219. netease-mail
220. stickam
221. oovoo
222. netvmg-traceroute
223. 360-safeguard-update
224. pplive
225. computrace
226. kaspersky
227. logitech-webcam
228. ms-sms
229. dotmac
230. gre
231. qqmusic
232. shutterfly
233. snmp-trap
234. cyworld
235. qqlive
236. phproxy
237. reuters-data-service
238. **filesonic (50%)**
239. citrix
240. hi5
241. horde
242. pptp
243. alisoft
244. qq-download
245. hamachi
246. fileserve
247. badongo
248. seesmic
249. vbulletin-posting
250. brighttalk
251. kaixin001-base
252. linkedin-mail
253. paloalto-updates
254. pando
255. bet365
256. pogo
257. second-life
258. mediawiki-editing
259. yourminis
260. mms
261. ciscovpn
262. echo
263. portmapper
264. hyves-base
265. lwapp
266. stagevu
267. ms-netlogon
268. zimbra
269. active-directory
270. google-docs-enterprise
271. open-vpn
272. gotomeeting
273. iheartradio
274. xobni
275. zango
276. ifile.it
277. kugoo
278. socks
279. java-update
280. avira-antivir-update
281. imo
282. apple-appstore
283. glype-proxy
284. icq
285. lotus-notes-base
286. yahoo-file-transfer
287. instan-t-file-transfer
288. webex-base
289. daytime
290. deezer
291. tvu
292. zynga-games
293. oracle
294. tftp
295. odnoklassniki-base
296. linkedin-posting
297. adobe-meeting
298. garena
299. mixi-base
300. veetle
301. 2ch
302. tor
303. qq-games
304. battlefield2
305. sopcast
306. nntp
307. qq-file-transfer
308. badoo
309. baofeng
310. evony
311. xing
312. bebo-base
313. gtalk-voice
314. sharepoint-admin
315. ebay-desktop
316. cgiproxy

317. me2day
318. hotspot-shield
319. niconico-douga
320. amazon-cloud-player
321. viber
322. freenet
323. myspace-mail
324. weather-desktop
325. whois
326. yandex-mail
327. bugzilla
328. panda-update
329. vnc
330. funshion
331. megashares
332. foursquare
333. uusee
334. freegate
335. subversion
336. roundcube
337. tales-runner
338. tikiwiki-editing
339. yahoo-webcam
340. capwap
341. isatap
342. kazaa
343. mibbit
344. carbonite
345. netload
346. discard
347. google-wave
348. live-mesh-base
349. nimbuzz
350. xbox-live
351. daum-mail
352. chatroulette
353. ms-exchange
354. netsuite
355. dcinside-base
356. ipsec-esp
357. qq-audio-video
358. gmx-mail
359. webqq
360. sugarsync
361. tcp-over-dns
362. netflix
363. quora
364. rsvp
365. youtube-uploading
366. rping
367. rsync
368. ultrasurf
369. yoono
370. dcc-antispam
371. lineage
372. norton-av-broadcast
373. rhapsody
374. sharepoint-documents
375. gamespy
376. hangame
377. sina-webuc
378. flumotion
379. baidu-webmessenger
380. nate-mail
381. secureserver-mail
382. wolfenstein
383. citrix-jedi
384. meetup
385. nateon-im-base
386. spotify
387. yourfilehost
388. apple-airport
389. avaya-webalive-base
390. neonet
391. warcraft
392. adrive
393. files.to
394. iloveim
395. live-mesh-remote-desktop
396. send-to-phone
397. fs2you
398. live-mesh-sync
399. ipp
400. trendmicro-officescan
401. finger
402. open-webmail
403. cisco-nac
404. msn-video
405. web-de-mail
406. h.245
407. youtube-safety-mode
408. easy-share
409. octoshape
410. poker-stars
411. **naver-mail (25%)**
412. teachertube
413. comcast-webmail
414. endnote
415. orb
416. clubbox
417. cygnet-scada
418. tudou-speedup
419. ali-wangwang-base
420. mozy
421. pp-accelerator
422. camfrog
423. activesync
424. git
425. mail.ru-moimir
426. union-procedure-call
427. kaixin-base
428. fastmail
429. filemaker-pro
430. live-meeting
431. palringo
432. feidian
433. itv-player
434. l2tp
435. dostupest
436. google-location-service
437. sflow
438. google-buzz
439. sakai
440. afp
441. mixi-posting
442. myspace-posting
443. runescape
444. filedropper
445. netflow
446. yy-voice-base
447. lokalisten
448. gadu-gadu
449. all-slots-casino
450. freeetv
451. ifolder
452. woome
453. cups
454. h.323
455. miro
456. socialtv
457. studivz
458. timbuktu
459. gmail-call-phone
460. h.225
461. gotomypc
462. folding-at-home
463. maplestory
464. kakaotalk
465. rpc
466. autobahn
467. manolito
468. direct-connect
469. mail.ru-webagent
470. elluminate
471. fetion-base
472. pcanywhere
473. clip2net
474. renren-im
475. yammer
476. jaspersoft
477. xunlei-kankan
478. classmates
479. google-video-enterprise
480. spark
481. ameba-now-base
482. wuala
483. amazon-cloud-drive-uploading
484. diino
485. gogobox
486. mgoon
487. babelgum
488. foxy
489. kaixin001-mail
490. mydownloader
491. unassigned-ip-prot
492. drop.io
493. editgrid
494. aim-file-transfer
495. soulseek
496. boxnet-editing
497. gmail-video-chat
498. tonghuashun
499. zamzar
500. gtalk-file-transfer
501. kkbox
502. sybase
503. jango
504. rdt
505. soribada
506. daum-cafe-posting
507. corba
508. zoho-writer
509. eve-online
510. apple-location-service
511. twtkr
512. vmware
513. vsee
514. yy-voice-games
515. msnshell
516. aol-proxy
517. cloudmark-desktop
518. dealio-toolbar
519. move-networks
520. sina-weibo-posting
521. mediamax
522. sling
523. vkontakte-chat
524. xfire
525. call-of-duty
526. google-plus
527. popo-im
528. blackberry
529. libero-video
530. nateon-file-transfer
531. cgi-irc
532. innovative
533. livestation
534. messengerfx
535. tumblr
536. userplane
537. afreeca
538. megashare
539. boxnet-uploading
540. google-maps
541. itunes-appstore
542. zoho-im
543. ameba-blog-posting
544. crashplan
545. mail.ru-mail
546. google-translate-manual
547. google-update
548. medium-im
549. wiiconnect24
550. ms-product-activation
551. nate-video
552. ncp
553. qdown
554. razor
555. ariel
556. ezpeer
557. magicjack
558. sharepoint-calendar
559. igmp
560. sbs-netv
561. hopopt
562. icloud
563. meabox
564. wikispaces-editing
565. hopster
566. rip
567. bomgar
568. google-translate-auto
569. radmin
570. simplite-msn
571. nfs
572. odnoklassniki-messaging
573. plugoo-widget
574. vtunnel
575. apt-get
576. flexnet-publisher
577. mail.ru-agent-base
578. ntr-support
579. xdmcp
580. ip-in-ip
581. air-video
582. android-market
583. fc2-blog-posting
584. itunes-mediastore
585. kino
586. storage.to
587. svtplay
588. dell-update
589. jira
590. ning
591. party-poker
592. regnum
593. streamaudio
594. unreal
595. dl-free
596. bomberclone
597. ospf
598. postgres
599. transferbigfiles
600. naver-blog-posting
601. naver-ndrive
602. battle.net
603. renren
604. yahoo-calendar
605. keyholetv
606. snmpv1
607. whatsapp
608. zoho-sheet
609. tv4play
610. viadeo
611. zendesk
612. websense
613. winamp-remote
614. microsoft-dynamics-crm
615. nateon-audio-video
616. vkontakte-mail
617. blin
618. pim
619. dazhihui
620. putlocker
621. google-docs-editing
622. paradise-paintball
623. t-online-mail
624. kontiki
625. tumblr-posting
626. cox-webmail
627. cvs
628. hyves-chat
629. join-me-base
630. minecraft
631. vnc-http
632. zoho-wiki
633. zumodrive
634. bebo-posting
635. concur
636. good-for-enterprise
637. asus-webstorage
638. mount
639. packetix-vpn
640. proxeasy
641. meinvz
642. mekusharim
643. thinkfree
644. brightcove
645. 2ch-posting
646. adobe-connect
647. ali-wangwang-file-transfer
648. ilohamail
649. inforeach
650. kproxy
651. pullbbang-video
652. uploading
653. netviewer
654. smilebox
655. tagoo
656. youseemore
657. ameba-now-posting
658. seeqpod
659. fortiguard-webfilter
660. snmpv2
661. amazon-instant-video
662. ip-messenger-base
663. renren-chat
664. sosbackup
665. taku-file-bin
666. groupwise
667. ibm-bigfix
668. odnoklassniki-apps
669. peerguardian
670. forticlient-update
671. ventrilo
672. your-freedom
673. cpq-wbem
674. tacacs-plus
675. dcinside-posting
676. google-calendar-enterprise
677. sap
678. sophos-update
679. x11
680. zoho-show

681. mcafee-update
682. nateon-desktop-sharing
683. renren-music
684. tokbox
685. vagaa
686. bacnet
687. fetion-file-transfer
688. ibackup
689. optimum-webmail
690. qik
691. yuuguu
692. 51.com
693. mail.com
694. mendeley
695. ms-win-dns
696. renren-posting
697. korea-webmail
698. neptune
699. verizon-wsync
700. chrome-remote-desktop
701. drda
702. filemail
703. fogbugz
704. hyves-mail
705. amazon-cloud-drive-base
706. igp
707. mercurial
708. showmypc
709. adobe-flash-socketpolicy-server
710. bebo-mail
711. cddb
712. cvsup
713. google-music
714. outblaze-mail
715. backup-exec
716. cooltalk
717. doof
718. pna
719. rift
720. rpc-over-http
721. usermin
722. yahoo-blog-posting
723. diodeo
724. earthcam
725. glide
726. livelink
727. scribd
728. eatlime
729. koolim
730. ms-scom
731. reserved
732. tivoli-storage-manager
733. webex-weboffice
734. netop-remote-control
735. panos-web-interface
736. scps
737. totodisk
738. voddler
739. asterisk-iax
740. crossloop
741. google-docs-uploading
742. pownce
743. secure-access
744. sina-uc-base
745. fring
746. hushmail
747. icq2go
748. lotus-sametime
749. sccp
750. egloos-blog-posting
751. ms-kms
752. renren-apps
753. tvants
754. acronis-snapdeploy
755. adnstream
756. etherip
757. gbridge
758. iso-ip
759. opera-mini
760. turboupload
761. writeboard
762. yahoo-notepad
763. zelune
764. zoho-crm
765. baidu-hi-base
766. graboid-video
767. hyves-games
768. jap
769. netflix-streaming
770. ovation
771. rdmplus
772. gds-db
773. ning-apps
774. symantec-syst-center
775. wins
776. baidu-hi-games
777. dimdim
778. emc-documentum-webtop
779. emc-networker
780. ning-posting
781. winamax
782. daum-blog-posting
783. informix
784. meebo-file-transfer
785. mikogo
786. starcraft
787. yantra
788. 100bao
789. egp
790. gigaup
791. trendmicro-safesync
792. vidyo
793. ammyy-admin
794. emcon
795. ku6
796. paloalto-wildfire-cloud
797. renren-mail
798. zoho-mail
799. apple-push-notifications
800. bigupload
801. genesys
802. imhaha
803. wikidot-editing
804. yahoo-finance-posting
805. zoho-notebook
806. 51.com-games
807. ms-lync-video
808. dabbledb
809. fotoweb
810. laconica
811. vnc-encrypted
812. adobe-online-office
813. amazon-unbox
814. apc-powerchute
815. chaos
816. daum-touch
817. eigrp
818. ipv6-icmp
819. mgcp
820. ndmp
821. netspoke
822. pup
823. sendoid
824. steekr
825. tistory-blog-posting
826. webconnect
827. xm-radio
828. drivehq
829. exp
830. naver-line
831. perfect-dark
832. spideroak
833. splashtop-remote
834. subspace
835. teamviewer-sharing
836. wetpaint-editing
837. zenbe
838. cbt
839. fetion-audio-video
840. gizmo
841. http-tunnel
842. ibm-director
843. ms-wins
844. nakido-flag
845. netmeeting
846. prm
847. spark-im
848. turboshare
849. webhard
850. ypserv
851. clarizen
852. fileguri
853. im-plus
854. isl-light
855. sharebase.to
856. simplify
857. skip
858. vmtp
859. war-rock
860. xns-idp
861. bloomberg-professional
862. camo-proxy
863. filemaker-anouncement
864. ironmountain-connected
865. iscsi
866. megaproxy
867. sina-uc-file-transfer
868. swapper
869. 1und1-mail
870. aruba-papi
871. baidu-hi-file-transfer
872. dnp3
873. mail.ru-games
874. ms-dtc
875. ms-lync
876. paltalk
877. sctp
878. share-p2p
879. sugar-crm
880. udplite
881. usejump
882. vrrp
883. 3pc
884. caihong
885. dhcpv6
886. fasp
887. google-lively
888. leapfile
889. mux
890. trinoo
891. tuenti
892. altiris
893. att-connect
894. lan
895. ms-ocs
896. nsfnet-igp
897. nvp-ii
898. rwho
899. seven-email
900. tinyvpn
901. viber-voice
902. wixi
903. argus
904. bbn-rcc-mon
905. bna
906. daap
907. dccp
908. hmp
909. leaf-1
910. mcafee-epo-admin
911. pnni
912. slacker
913. vyew
914. yugma
915. checkpoint-cpmi
916. chinaren
917. dameware-mini-remote
918. filer.cx
919. gridftp
920. homepipe
921. idpr-cmtp
922. ippc
923. ipsec-ah
924. isis
925. joost
926. knight-online
927. kryptolan
928. larp
929. ms-iis
930. okurin
931. paran-mail
932. pgm
933. sat-expak
934. steganos-vpn
935. synergy
936. tlsp
937. xnet
938. zabbix
939. buddybuddy-base
940. chinaren-chat
941. dfs
942. dsr
943. esignal
944. estos-procall
945. ggp
946. hovrs
947. hyves-music
948. iatp
949. idrp
950. ipv6-frag
951. ipv6-nonxt
952. leaf-2
953. merit-inp
954. mobilehdr
955. narp
956. omnidrive
957. pcoip
958. private-enc
959. projectplace
960. ptp
961. radiusim
962. reliable-data
963. rlogin
964. rypple
965. sdrp
966. snp
967. sscopmce
968. telenet-webmail
969. trunk-1
970. trunk-2
971. zoho-meeting
972. beamyourscreen
973. crtp
974. dcn-meas
975. gpass
976. host
977. ipv6-opts
978. lotus-notes-admin
979. modbus-base
980. ospfigp
981. pipe
982. qnx
983. rediffbol-audio-video
984. remobo
985. rsh
986. rvd
987. secure-vmtp
988. sm
989. snmpv3
990. srp
991. st
992. ttp
993. uti
994. visa
995. wb-expak
996. wetransfer
997. wsn
998. x-font-server
999. zoho-planner
1000. aim-express-file-transfer
1001. aris
1002. big-brother
1003. cpnx
1004. db2
1005. dgp
1006. encap
1007. evalesco-sysorb
1008. fibre-channel
1009. foldershare
1010. frozenway
1011. fuze-meeting
1012. generic-p2p
1013. idpr
1014. il
1015. ipcomp
1016. ipip
1017. mcafee
1018. msn2go
1019. phonemypc
1020. smp
1021. vmware-view
1022. avaya-phone-ping
1023. cftp
1024. compaq-peer
1025. cphb
1026. eroom-host
1027. fluxiom
1028. hp-data-protector
1029. ifmp
1030. i-nlsp
1031. iso-tp4
1032. mail.ru-agent-file-transfer
1033. paltalk-express
1034. scribd-uploading
1035. sip-application
1036. tradestation
1037. vines
1038. wb-mon
1039. woofiles
1040. xtp
1041. br-sat-mon
1042. ddx
1043. distcc
1044. fire

1045. fufox
1046. gmtp
1047. i2p
1048. ibm-websphere-mq
1049. iperf
1050. iplt
1051. irtp
1052. jxta
1053. mfe-nsp
1054. mobile
1055. modbus-read-holding-registers
1056. mpls-in-ip
1057. ms-frs
1058. ms-scheduler
1059. netblt
1060. netbotz
1061. ning-mail
1062. origin
1063. paltalk-superim
1064. pvp
1065. realtunnel
1066. sat-mon
1067. second-life-voice-chat
1068. spotnet
1069. sprite-rpc
1070. sps
1071. suresome
1072. vnc-clipboard
1073. activenet
1074. aim-audio
1075. bgp
1076. crudp
1077. ea-fifa
1078. firephoenix
1079. gotomypc-file-transfer
1080. gyao
1081. ipcv
1082. ipx-in-ip
1083. magister
1084. meeting-maker
1085. moinmoin-editing
1086. ms-lync-apps-sharing
1087. ms-lync-audio
1088. mtp
1089. pingfu
1090. stp
1091. sun-nd
1092. swipe
1093. tcf
1094. we-dancing-online
1095. wlccp
1096. yoics
1097. zoho-share
1098. ants-p2p
1099. chinaren-apps
1100. condor
1101. ddp
1102. draugiem
1103. gnu-httptunnel
1104. google-finance-posting
1105. ms-ocs-file-transfer
1106. perforce
1107. privax
1108. propalms
1109. readytalk
1110. techinline
1111. tvtonic
1112. wccp
1113. aim-video
1114. bonpoo
1115. cyberghost-vpn
1116. desktoptwo
1117. file-host
1118. flickr-uploading
1119. flixwagon
1120. gotomypc-printing
1121. hitachi-spc
1122. iccp
1123. irc-dcc-file-transfer
1124. jumpdesktop
1125. meevee
1126. modbus-read-input-registers
1127. modbus-write-multiple-registers
1128. netfolder
1129. noteworthy-admin
1130. noteworthy-base
1131. qik-video-chatting
1132. rediffbol-base
1133. rstatd
1134. siebel-crm
1135. sina-uc-remote-control
1136. tunnelbear
1137. vidsoft
1138. vnn
1139. arcserve
1140. asproxy
1141. buddybuddy-file-transfer
1142. callpilot
1143. circumventor
1144. doshow
1145. dropboks
1146. dynamicintranet
1147. hl7
1148. ipv6-route
1149. little-fighter
1150. lotuslive
1151. modbus-read-coils
1152. modbus-write-single-register
1153. netop-on-demand
1154. officehard
1155. peercast
1156. phpwiki-editing
1157. rabbitmq
1158. rusers
1159. schmedley
1160. sharepoint-blog-posting
1161. sharepoint-wiki
1162. spirent
1163. surrogafier
1164. tacacs
1165. tor2web
1166. vakaka
1167. winny
1168. airaim
1169. ali-wangwang-audio-video
1170. avaya-webalive-desktop-sharing
1171. blokus
1172. bypassthat
1173. centriccrm
1174. chinaren-mail
1175. emc-smartpackets
1176. fastviewer
1177. fly-proxy
1178. g.ho.st
1179. gmail-drive
1180. gnunet
1181. ibm-clearcase
1182. kace
1183. kaixin-chat
1184. kaixin-mail
1185. meetro
1186. misslee
1187. mobility-xe
1188. msn-money-posting
1189. ms-visual-studio-tfs
1190. netvault-backup
1191. openft
1192. oracle-crm-ondemand
1193. pcvisit
1194. ruckus
1195. saba-centra-meeting
1196. socks2http
1197. unyte
1198. vnc-filetransfer
1199. zwiki-editing
1200. 51.com-bbs
1201. ad-selfservice
1202. aol-messageboard-posting
1203. avoidr
1204. backpack-editing
1205. batchbook
1206. beinsync
1207. chikka-messenger
1208. echoware
1209. eyejot
1210. factset
1211. ghostsurf
1212. gkrellm
1213. gomeetnow
1214. gopher
1215. gtunnel
1216. howardforums-posting
1217. ibm-clearquest
1218. infront
1219. instan-t-webmessenger
1220. ip-messenger-file-transfer
1221. league-of-legends
1222. lifecam
1223. lotuslive-meeting
1224. motleyfool-posting
1225. ms-isa-fw-client
1226. ms-virtualserver
1227. orsiso
1228. ossec
1229. paran-u2
1230. pbwiki-editing
1231. peerenabler
1232. pichat
1233. psiphon
1234. qianlong
1235. remotecall
1236. r-exec
1237. salesforce-chatter
1238. shavlik-netchk
1239. sina-uc-web-disk
1240. stockstar
1241. thwapr
1242. track-it
1243. tvb-video
1244. webot
1245. winmx
1246. wordfast
1247. yosemite-backup
1248. zoho-people