The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

8th Edition, December 2011

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 94089
www.paloaltonetworks.com

Table of Contents

Executive Summary

The *Application Usage and Risk Report (8th Edition, December 2011)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing network traffic assessments conducted in 1,636 organizations worldwide between April 2011 and November 2011. This edition of the report will delve into some shifts in social networking traffic patterns that indicate more active participation than previously viewed. Then, a discussion of how browser-based filesharing applications have evolved into two different usage segments while continuing to grow in popularity. The growth in usage brings personal and professional benefits as well as increased business and security risks. The last section takes a contrarian view of the traffic by highlighting the fact that while tcp/80 is a commonly used port for many applications, the majority of the traffic is traversing ports other than tcp/80 exclusively. The risk of course is that security teams may focus too much effort on tcp/80 and miss significant risks elsewhere.

Key findings include:

Social networking usage is becoming more active.

- Active usage of social networking applications (Facebook-apps, games, social-plugins and posting) more than tripled, going from 9% (October 2010) to 28% (December 2011) when measured as a percentage of total social networking bandwidth.

Browser-based filesharing use cases: work vs. entertainment.

- With 65 different browser-based filesharing variants found with an average of 13 being used in each of the participating organizations, two clear use cases are emerging within the browser-based filesharing market: work and entertainment. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 does not equate to securing the network.

- Conventional wisdom suggests that most of an organization's network traffic is going through tcp/80. The analysis shows that 51% of the bandwidth consumed by 35% of the applications is not using tcp/80. In contrast, the 297 applications that use only tcp/80, and no other port by default, represent a mere 25% of the applications and 32% of the bandwidth observed.

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 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 the semi-annual Application Usage and Risk Report.

Demographics

The latest edition of the Application Usage and Risk Report summarizes 1,636 traffic assessments performed worldwide. The distribution of the participating organizations remains relatively even with 30% being performed in the U.S., Canada, Mexico and Asia Pacific/Japan while the remaining 40% of the participating organizations were in Europe. The findings within this report will focus solely on the global view of application traffic with any country or region specific variations in usage patterns discussed separately.

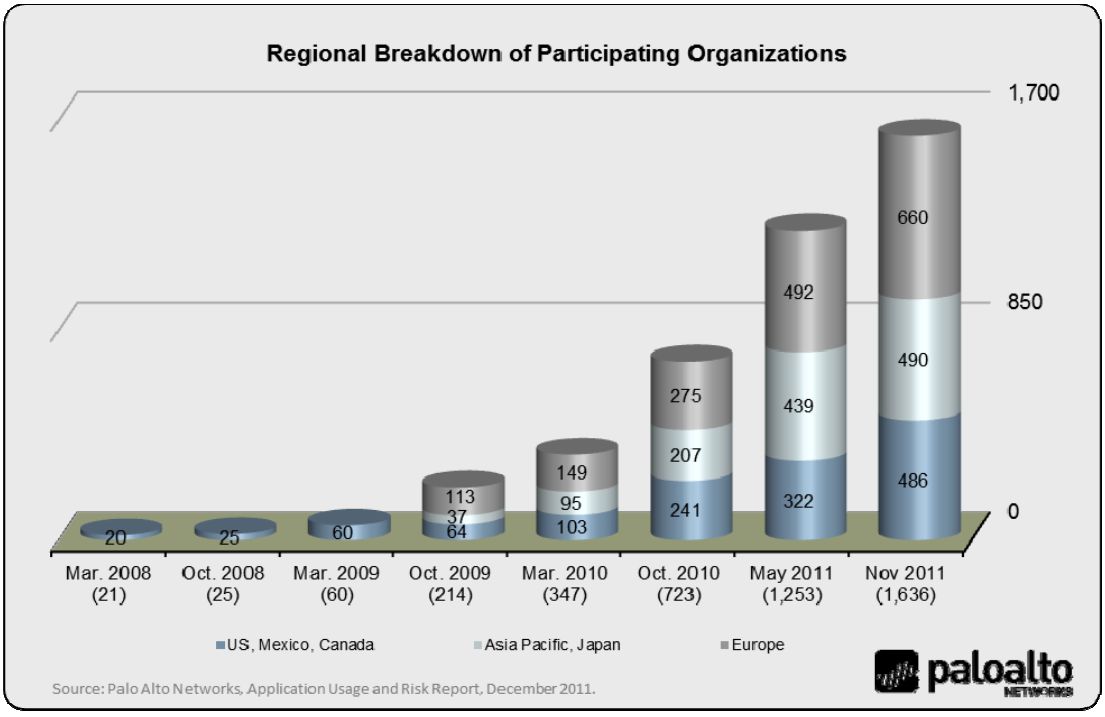

Figure 1: Geographic distribution of participating organizations.

Social Networking Use Becomes More Active

In previous reports, the analysis showed that the use of social networking was voyeuristic in nature; meaning that users would watch their Facebook Wall or Timeline while at work much like how instant messaging has been used and is used today. Social networking applications are open on their desktop, but users are not actively posting, using plugins or social networking applications. The latest analysis shows some fairly significant shifts in traffic when compared to the analysis from October 2010.

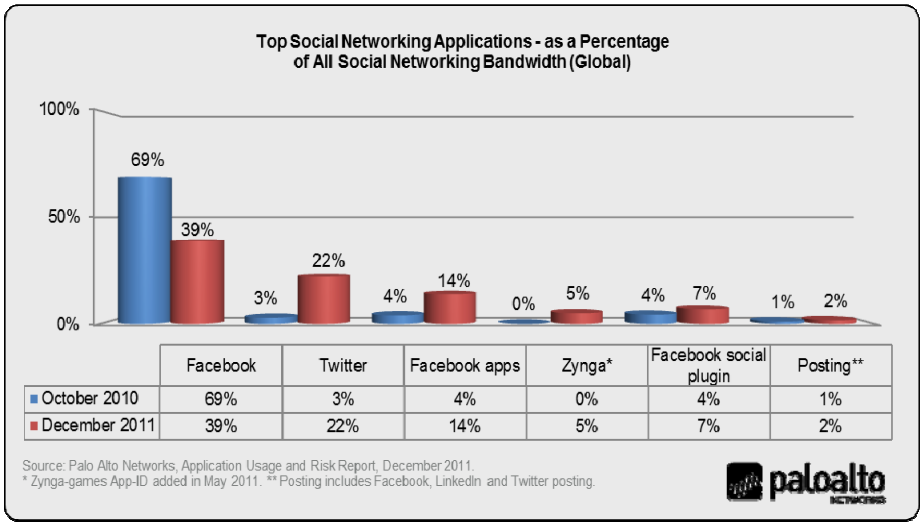

Figure 2: Changes in social networking bandwidth consumption between Oct. 2010 and Dec. 2011.

Facebook Applications Bandwidth Consumption Triples

The year-over-year comparison shows that the percentage of social networking bandwidth consumed by Facebook applications more than tripled, growing from 4% to 13%. Social networking detractors will immediately jump to the conclusion that employees are wasting time playing games. While this may be true in some cases, many businesses have developed Facebook applications as an extension of their marketing and services offerings. Facebook applications and social plugins are becoming a mechanism to reach new markets, support existing customers and strengthen relationships. Some Facebook examples are described below.

- **CareFirstDance:** CareFirstDance uses Facebook to encourage and help policyholders track their dance activity. CareFirstDance is a means of capturing the growth of dance as a means of staying fit that began in May 2010 with National Dance Day. This is an instance where a company is using social media for both marketing and cost savings purposes. By encouraging members to dance, exercise, and pay attention to their health, CareFirst has a public health effort that helps the brand, and by having ultimately healthier members who need less care or at least less expensive care, and thus lower costs – giving the company a bottom line benefit. Like the Nike+ Challenge application, should a quick update on how long an employee danced be blocked? http://www.carefirst.com/membsvcs/facebook/socialmedia.html

- **Ford: Ford Social and Mustang Battle applications**: Ford uses a classic business-to-consumer (B2C) approach – attract and retain customers with image-building and brand-building games and social media activities. Customers are invited to share the passion they have for Ford's products – and they do, often, and with great detail. The use of this application improves Ford's top line revenue by attracting new customers, but more importantly, cements the relationship with existing customers, ensuring they buy again. https://www.facebook.com/fordmustang

- **Caterpillar:** Caterpillar (Cat) is a classic, blue collar, blue chip, business-to-business (B2B) company. Cat uses social media very successfully to engage with its customers – deeply. While B2B, rather than B2C, Cat recognizes that the lines between work and personal life have blurred to the point of becoming indistinct, and uses social media to tap into their customers' professional/personal interests. For example, Cat talks about big jobs/projects, big new gear, and engineering feats of brilliance. Rather than simply pushing their products, Cat appeals to their buyers' love of their jobs, and their successful use of Cat products to complete a big project via social media (Facebook, Twitter, and blogging), effectively doing much of the same top-line revenue influence that Ford does in a B2C context, and also with much higher price tags. https://www.facebook.com/catproducts and http://twitter.com/#!/caterpillarinc

- **Zynga-games:** This set of Facebook applications was broken out as its own App-ID in May 2011, and since its release, Zynga-games were found in 53% of the participating organizations and consumed roughly 5% of the total social networking bandwidth. Unlike the other applications observed, these games are entertainment-focused, and as such may warrant more scrutiny and control from an application usage policy perspective.

- **Nike: Nike+ Challenge:** Nike+ Challenge is a Facebook application that helps runners break out of a training rut, reach new goals and stay motivated through a group challenge. Users agree upon a running related challenge then use the application to track progress, post updates and encourage (or talk smack) to the others who are participating in the challenge. With the Nike+ Challenge application, Nike is building a relationship with users who may not be Nike customers. By participating in a Nike+ Challenge with their friends, the non-Nike customers will be more likely to switch. An employee that takes a few minutes to use the Nike+ Challenge application at work to post their fitness progress is clearly not performing their daily tasks, but studies have shown that fit employees are more productive. Should the use of the Nike+ Challenge application be blocked? http://nikerunning.nike.com/nikeos/p/nikeplus/en_US/index_vapor

Twitter Bandwidth Consumption Increases 7-Fold

In a comparison with the October 2010 data, Twitter-browsing measured as a percentage of social networking bandwidth, increased from 3% (October 2010) to 21% (December 2011). Adding to the enormity of this increase is the fact that Twitter-posting, which was flat year-over-year, is identified and measured separately. The explanations for this increase are varied. One explanation is the changes Twitter made to the application itself, allowing users to attach files and pictures to their 140 character missives. Another more meaningful reason, outside of its use as a social networking application for individuals, is that businesses are using it as a public relations, recruiting, and marketing tool.

Another reason is that Twitter has become a powerful tool that enables organizations, grass-roots or otherwise, to deliver their message to the masses quickly, effectively and repeatedly. There were examples where Twitter and other social networking applications significantly influenced the volume of news about, and visibility of, a particular world-news event. Unrest in the Middle East, economic turmoil and associated demonstrations in Europe, disasters in APAC and the Occupy movement in the U.S. all experienced significant activity on social networking applications such as Twitter. In this case, the usage is, in most cases, of a personal nature, raising the question of how organizations should treat the tracking of world news, in near real-time: allow it, block it, or manage it? This is a critical challenge that organizations face today.

Some Perspective On Bandwidth Consumption

At first glance, the shifts in usage patterns may imply that there is a significant drain on productivity and a strain on the networking infrastructure, possibly jeopardizing other, more business critical, bandwidth sensitive applications. Clearly social networking applications are being used for both business and personal purposes, but the overall impact to the bandwidth infrastructure is small, when compared to the total bandwidth observed. All 71 social networking applications combined, consumed only 1% of the total bandwidth. This volume of bandwidth consumption is small considering it is the sum of all 1,587 organizations where social networking was in use and the time period is over a five day span.

Social networking usage patterns are changing and will continue to change as more and more organizations develop and refine their social networking strategies and usage policies. In many cases, blindly blocking the use of these applications will encourage the use of proxies, other circumvention tools, or in some cases, exceptions for some groups which will be difficult to manage and scale. Blindly allowing all without security measures represents additional challenges and risks. Organizations must evaluate social networking usage and set an appropriate and manageable enablement policy for all users.

Managing the Risks

The use of social networking applications, for whatever purpose, represents a wide range of business and security risks that all organizations must take into consideration.

- **Trust:** Social networking applications have trained users to be too trusting by encouraging everyone to share the story of their lives. When users receive links, pictures, videos, and executables from their social network and presumably their "friends, they are more inclined to click first and think later. The elevated trust level has many ramifications, including social engineering, malware propagation and botnet command/control channels.

- **Social engineering:** Old-school social engineering had criminals calling users on the phone; convincing them they were the IT department. The conversation would result in divulging a user name and password. Now, social networking sites are rich with information about users that can easily be used to for social engineering purposes. A user's social networking activity is monitored for names of pets or kids, activities, hobbies, vacations, holiday activities, and other commonly shared information that can be used to reset a password.

  With those data points, the cybercriminal is able to entice a user to click on a link forwarded from a supposed friend. The Aurora attack of a few years ago and the recent TDL4 outbreak both show connections to this type of social engineering. When used in this manner, the cyber criminals' goal is to remain hidden, looking for very specific information, often times remaining silent for long periods of time.

- **Malware propagation:** By taking advantage of the "automatic" elevated levels of trust, it has become very easy for cyber criminals to rapidly propagate their payload using social networking applications. As an example, a variant of the Zeus Trojan, known in the past to steal financial information, recently infected thousands of Facebook users who had viewed photos supposedly sent to them by a friend. In reality, the friend's account had been hijacked and the photos being sent were a booby-trapped screensaver file with a .jpg file extension.

- **Botnet command and control:** There are numerous examples of how social networking applications can act as a command and control channel for botnets. A very detailed description of this use case is included in the July 2010 Shadowserver Foundation report, Shadows in the Cloud: Investigating Cyber Espionage 2.0. The report highlights how social networking (and other applications) applications such as Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail were used to extract their payload from the targeted individuals.

The list of risks above is by no means the complete list, but for organizations that are struggling to find the appropriate balance between blocking and enabling social networking applications, these four must be addressed via extensive user education along with appropriate security and content scanning policies.

Browser-based Filesharing: Work vs. Entertainment

Since 2008, the Palo Alto Networks *Application Usage and Risk Report* has monitored browser-based filesharing as an application category. It has steadily increased to the point where it is now found in 92% of all participating organizations while P2P filesharing has slowed to where it is used in 82% of the participating organizations. Only client/server related file transfer applications (FTP, etc.) are more commonly found.

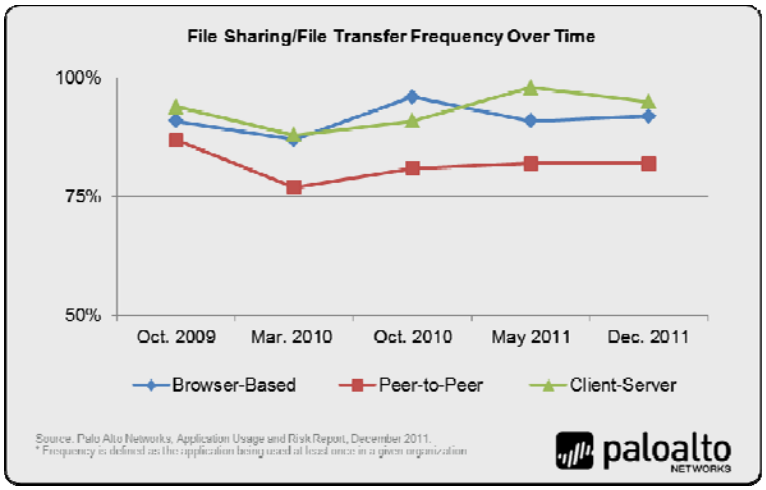

Figure 3: Frequency that filesharing/file transfer applications are being used.

Since 2008, the number of browser-based filesharing applications has more than tripled, growing from 22 to 71 now identified in Applipedia. The growth is attributed to two factors; new applications being released to the market and new App-IDs being added to the database. Regardless of the reasons for the growth, there are many variants. In the April 2011 to November 2011 timeframe that this analysis covers, 65 different browser-based filesharing applications were found. On average, 13 variants were found across 1,506 (92%) of the participating organizations. For some perspective on the number of application variants found, an average of 13 variants per organization is considered to be high; only two other application categories. photo-video (29 variants) and social networking (16 variants) had more application variants.

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. Whereas P2P and FTP both require some technical acumen to use, these new applications were point and click easy. With YouSendit! the file is uploaded and a URL for the download is sent to the intended recipient. With so many variants, segmentation into different use cases has occurred with two clear cases emerging: infrastructure- and/or productivity-oriented or entertainment-oriented. The other significant change is that many no longer use the browser as their sole user interface.

Infrastructure- or Productivity-Oriented Browser-based Filesharing

The browser-based filesharing applications that fall into this group are those that are used by organizations as part of their cloud-based infrastructure or are used by employees themselves to get their jobs done. This use case is loosely 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 including 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.

Based on the number of variants found in nearly all of the organizations, it is safe to say that these applications are providing both business and personal benefits, but the question is, how heavily are they used?

Application (Ports Used)	Organizations using the application (n=1,636)	Bytes consumed in Gigabytes (GB)	High definition movie downloads per organization*
Dropbox (tcp/80, 443)	1,251 (76%)	17,573	5
Mediafire (tcp/dynamic)	988 (60%)	12,280	4
Yousendit (tcp/80, 443)	834 (51%)	423	0
Boxnet (tcp/80, 443)	941 (57%)	86	0
Skydrive (tcp/80, 443)	1,065 (65%)	31	0
Docstoc (tcp/80)	969 (59%)	23	0
Total Bandwidth: All BBFS Applications (n=65)	1,506 (96%)	76,225	17
Total Bandwidth: All Applications (n=1,195)	1,636 (100%)	10,872,110	2,215
*Average size of a 2 hour high definition movie is 3 GB.			

Table 1: Browser-based filesharing application bandwidth consumption in terms of file downloads.

The statistics in Table 1 show that these applications are used with relatively high frequency (column 2). Browser-based filesharing applications that fulfill the infrastructure or productivity definition were found as frequently as 76% of the time. The highest bandwidth consumed in this group is Dropbox, at five high definition movies downloaded across all users within a given organization across a 5-day period.

Entertainment Oriented Browser-based Filesharing

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 positions and markets the application and the application user experience. For many of these applications, a registered user can browse a library of downloads as well as upload their own files.

- **Megaupload:** This application is very community based, with a top-100 download list that is derived from user activity. Once registered, a user can 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 has a tiered-based service model, with a free version as well as several pay or premium service offerings. The premium service offerings provide users with a client to simplify the management of the users file uploads. In addition to the tiered services, Megaupload also provides an API that allows users to embed an upload "folder" in their website. In addition to the API, users can 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 will allow users to more easily bypass network security controls.

- **FilesTube:** This application lets users search for shared files from various file hosting sites including FileServe, FileSonic, Megaupload, 4shared, Rapidshare, Hotfile, Mediafire, Netload and many others. Once registered, a user can browse video, games, software and lyrics categories or they can subscribe to groups or create their own. 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.

Application (Ports Used)	Organizations using the application (n=1,636)	Bytes consumed in Gigabytes (GB)	High definition movie downloads per organization*
Megaupload (tcp/80,800, 1723)	931 (57%)	20,405	7
Filesonic (tcp/80, 20, 21, dynamic)	857 (52%)	4,058	3
4shared (tcp/80, 443)	1,025 (63%)	2,041	1
Filestube (tcp/80)	826 (50%)	176	0
Total Bandwidth: All BBFS Applications (n=65)	1,506 (96%)	76,225	17
Total Bandwidth: All Applications (n=1,195)	1,636 (100%)	10,872,110	2,215
*Average size of a 2 hour high definition movie is 3 GB.			

Table 2: Browser-based filesharing application bandwidth consumption in terms of file downloads.

The statistics in Table 2 show that these applications are used with less frequency than those listed in Table 1, with entertainment-oriented variants found as frequently as 60% of the time. However, the volume of use, measured in terms of bandwidth consumed, is significantly higher.

Comparing Frequency and Volume of Use

An average of 13 different browser-based filesharing applications found in 92% of the 1,636 participating organizations means that these applications are used commonly and are delivering (work or personal) related benefits. The use case definitions and the discussion from above, and the frequency of use along with the bandwidth consumed shown in figure 4, provide some added clarity on how the application is being used.

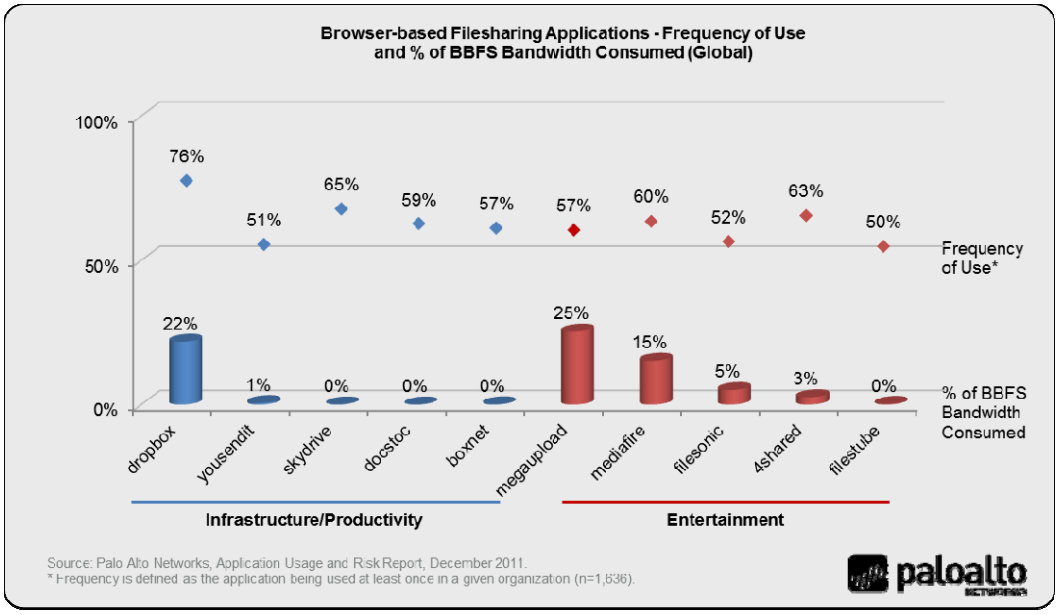

Figure 4: Most frequently detected browser-based filesharing applications and their bandwidth consumption.

Megaupload was found in 57% of the participating organizations yet it consumed the highest amount of browser-based filesharing bandwidth, indicating that the file sizes are large. Given the community-based emphasis along with the types of files being exchanged (video, games, software), it would not be inaccurate to say that Megeaupload, in most of the participating organizations, is non-work related. 4shared and FilesTube would also fall into this category. FileSonic is also an entertainment-oriented application that has established distribution agreements with a wide range of artists, thereby minimizing possible copyright infringement violations.

In contrast, both Docstoc and YouSendit! were used in more than 50% of the organizations 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, indicating a higher likely hood that the usage is for work-related purposes, as opposed to entertainment.

Dropbox presents a bit of a contradiction in that it is used most frequently and 2nd highest percentage of bandwidth consumed. Dropbox, as defined above, is focused on being part of the business infrastructure, which would imply that the file types and sizes are work-related and smaller than media files. Yet at 22% of the browser-based filesharing bandwidth, the strength of the work-related theory is lessened. The most likely explanation for the 22% bandwidth consumption would be the popularity (76% of the organizations) and a high volume of (possibly work related) files.

The fact that browser-based applications are in use, with high frequency and in some cases, a high volume of use, they are only one of three different ways in which large files can be moved from user-to-user: P2P and client-server are the other missing two mechanisms.

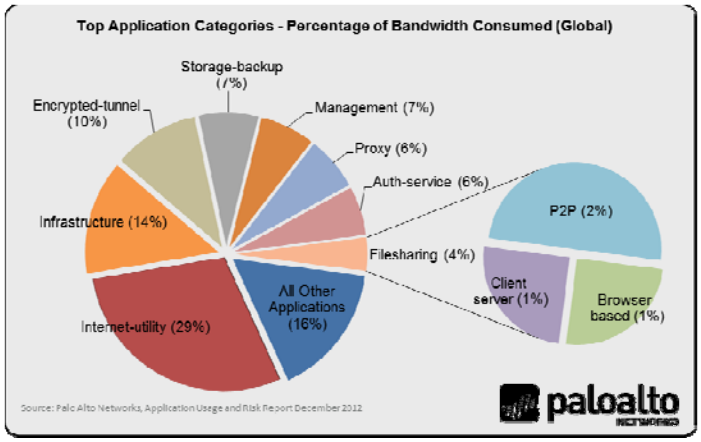

Figure 5: Bandwidth consumption breakdown for heaviest used application categories.

When all three mechanism are analyzed (Figure 4), P2P consumed 2% of the total bandwidth, while client server uses 1%. These applications are in use, and they carry certain business and security risks.

Browser-based filesharing: What are the Risks?

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 applications and 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.

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, or have been accused of, copyright violations.

- **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 bonafide ones. 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 bonafide application.

Browser-based filesharing applications are clearly used for both business and personal purposes. The same can be said for social networking applications as shown in Table 3. In fact, the analysis shows that the usage similarities at the organizational level are very similar. The one element that is not shown, but is relatively clear, is the number of actual users. Without question, the number of social networking users will far outweigh the number of browser-based filesharing users.

	Browser-based Filesharing	Social Networking
Applications found	65	71
Frequency of use (n=1,636)	92% (1,506)	96% (1,587)
Number of application variants found (total)	64	71
Number of application variants found (per organization)	13	16
Bandwidth consumed in GBs	76,225 GB	80,987 GB
Bandwidth consumed (high definition movies ~3 GB)	25,408	26,996
Bandwidth consumed as a percentage of total	0.70%	0.74%

Table 3: Browser-based filesharing and social networking statistical comparison.

However, the business and security risks are also remarkable similar. Yet the volume of concern expressed in the media is far more significant for social networking applications then it is for browser-based filesharing. The question arises; are the risks for social networking overblown? Or are the risks for browser-based filesharing underreported?

If Port 80 is Secure, Then my Network is Safe, 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 easily justified 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. The 1,195 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, contrary to popular belief, 413 of the 1,195 applications found (35%) are not using tcp/80. These applications consumed 51% 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 the bulk of the traffic and the associated security incidents.

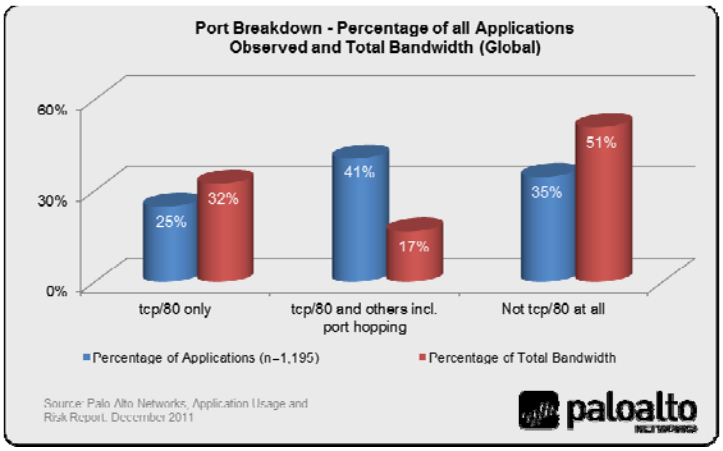

Figure 5: Applications observed based on port groupings.

Applications Using tcp/80 Only

This set of 297 applications uses only 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 and include social networking, webmail, browser-based filesharing, Internet utilities (tool bars, etc.) and web posting. Five of the heaviest bandwidth consuming applications in this group are shown in Table 4.

Application	Bandwidth consumed (GBs)	Organizations using the application	High definition movie downloads per organization*	Technology	Ports used
web-browsing	2,932,744	1,636	598	browser-based	tcp/80
youtube	143,142	1,517	31	browser-based	tcp/80
flash	112,373	1,596	23	browser-based	tcp/80
adobe-update	57,580	1,566	12	client-server	tcp/80
http-video	48,906	1,529	11	browser-based	tcp/80
*Average size of a 2-hour high definition movie is 3 GB.					

Table 4: Sample of applications that use tcp/80 only.

The applications within this sample are to be expected, with some exceptions such as Adobe-update; a client-server application that uses tcp/80 to ensure that the application is kept up-to-date. The business risks associated with this set of applications include possible productivity drain (YouTube and HTTP video) as well as bandwidth consumption. The security threats are the to-be-expected viruses, spyware and other types of malware associated with these applications.

Applications Using tcp/80 or Other Ports

This set of 485 applications 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.

Application	Bandwidth consumed (GBs)	Organizations using the application	High definition movie downloads per organization*	Technology	Ports used
http-proxy	699,270	1532	152	browser-based	tcp/80, 443, 1080, 3128, 8000, 8080
msrpc	209,028	1278	55	network-protocol	tcp/dynamic, udp/dynamic
bittorrent	177,513	1086	54	peer-to-peer	tcp/dynamic, udp/dynamic
ms-update	82,674	1606	17	client-server	tcp/80, tcp/443
ppstream	46,972	474	33	peer-to-peer	tcp/dynamic, udp/dynamic
*Average size of a 2-hour high definition movie is 3 GB.					

Table 5: Applications that use tcp/80 plus others, including port hopping.

A view into five of the highest bandwidth consumers shown in Table 5 highlights several data points. 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 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. 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 Not Using tcp/80

These applications do not use tcp/80 at all, nor are they dynamic (hop ports). Examples of the applications within this group are skewed more towards the traditional business applications and include database, authentication services, management, storage/backup, remote access, gaming and Internet utilities.

Application	Bandwidth consumed (GBs)	Organizations using the application	High definition movie downloads per organization*	Technology	Ports used
ssl	962,714	1632	197	browser-based	tcp/443
ms-ds-smb	547,735	1387	132	client-server	tcp/445,139 udp/445
snmp	484,727	1590	102	client-server	tcp/161, udp/161
ldap	337,241	1427	79	client-server	tcp/389, 3268 udp/389, 3268
mssql-db	193,637	940	69	client-server	tcp/1433, udp/1433
*Average size of a 2-hour high definition movie is 3 GB.					

Table 6: Sample of applications that do not use tcp/80 at all.

Five of the highest bandwidth consuming applications out of the 413 found, are shown in Table 7 include three very popular targets for cyber criminals – SMB, RPC 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 instead of tcp/80.

Applications Not Using tcp/80: Remote Access Control

Hidden within this group of applications are 51 different remote access control applications. 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.

Table 9. Types of remote access by percent of breaches within Hacking and percent of records

Local remote screen sharing (e.g., RDP, PCAnywhere)	64%	24%
Online session screen sharing (e.g., Go2Assist, LogMeIn, NetViewer)	5%	13%
Remote Shell (e.g., ssh, telnet, rsh)	2%	1%
Web-based terminal services (e.g., Citrix, MS Terminal Services)	2%	12%
VPN	1%	<1%

Source: 2011 Verizon Databreach Report

The most recent Verizon Databreach report that analyzed 900 incidents worldwide showed that 320 of the initial penetrations could be tracked back to remote access errors. The report implies that the common use (or misuse) of these tools is such that attackers have built it into their development efforts. From the report:

"As soon as an intruder discovers a particular [remote access] vendor's authentication method and schema (be it for TCP port 3389 for RDP; or TCP port 5631 and UDP port 5632 for pcAnywhere), he will be able to exploit it across a multitude of that vendor's partners and customers. Oftentimes, in lieu of conducting a full port scan for these remote service applications, attackers will customize their scripts to exclusively look for these ports and search a broad swath of the Internet."

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. During the analysis period for this report, an average of eight remote-access applications were found in 96% of the participating organizations. When viewed across the past two years of data collected and analyzed in the Application Usage and Risk Reports, the top five remote access tools have remained consistent in terms of the frequency of usage.

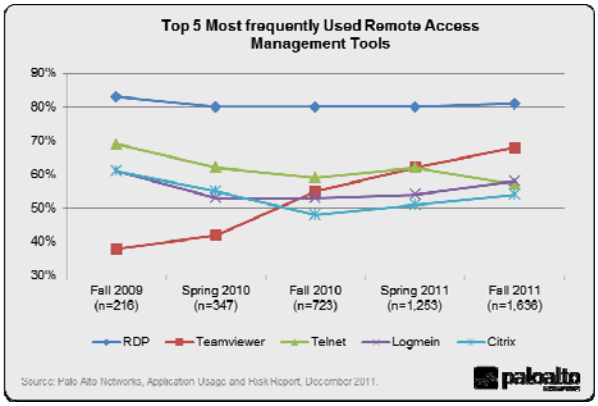

Figure 6: Most frequently used remote access management tools.

The interesting trend seen is the growth in popularity of Teamviewer, an open source tool that, according to Wikipedia, supports nearly every client known to exist. So using Teamviewer, a support representative could conceivably help a customer using their Android-based phone. A very powerful business proposition. And therein lies the downfall, at least from a security perspective.

Application	Bandwidth Consumed (GBs)	Organizations using the application	Ports Used
ms-rdp	7,356	1,318 (81%)	tcp/3389
teamviewer	853	1,105 (68%)	tcp/dynamic udp/dynamic
logmein	593	942 (57%)	tcp/80,tcp/443
telnet	424	934 (58%)	tcp/23
citrix	9,930	885 (54%)	tcp/443,2512,2513,2598,1494 udp/2512,2513

Table 7: Sample of applications that do not use tcp/80 at all.

The tech-savvy user who thinks it's cool can do the same thing from their desk but possibly leave the application up and running and in so doing, punch an unnecessary hole (on a non-standard port) in the firewall, exposing the organization to business and security risks.

Summary: Striking the Appropriate Balance

An argument could be made that never before have traffic patterns on enterprise networks evolved so rapidly. Employees use whatever application they want, often times to get their job done; other times the use is for personal purposes. Yet the application is one in the same. This dual-purpose usage presents IT organizations with the difficult challenge of striking the appropriate balance between enabling usage and protecting the network. Contrary to popular belief, the balancing act must expand beyond web-centric traffic to include all enabling applications traversing all ports, not just the popular or commonly used ones. Otherwise, the organizations security posture will be significantly compromised.

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its next-generation firewalls enable unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 20Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. Enterprises can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. Most recently, Palo Alto Networks has enabled enterprises to extend this same network security to remote users with the release of GlobalProtect™ and to combat targeted malware with its WildFire™ service. For more information, visit www.paloaltonetworks.com.

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 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, usually up to seven days, an Application Visibility and Risk Report is generated 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 The Application Usage and Risk Report.

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: Classifying All Applications, All Ports, All the Time.** App-ID addresses the traffic classification visibility limitations that plague traditional firewalls by applying multiple classification mechanisms to the traffic stream, as soon as the firewall sees it, to determine the exact identity of applications traversing the network. Unlike add-on offerings that rely solely on IPS-style signatures, implemented after port-based classification, every App-ID automatically uses up to four different traffic classification mechanisms to identify the application. App-ID continually monitors the application state, re-classifying the traffic and identifying the different functions that are being used. The security policy determines how to treat the application: block, allow, or securely enable (scan for, and block embedded threats, inspect for unauthorized file transfer and data patterns, or shape using QoS).

- **User-ID: Enabling Applications by Users and Groups.** Traditionally, security policies were applied based on IP addresses, but the increasingly dynamic nature of users and computing means that IP addresses alone have become ineffective as a mechanism for monitoring and controlling user activity. User-ID allows organizations to extend user- or group-based application enablement polices across Microsoft Windows, Apple Mac OS X, Apple iOS, and Linux users. User information can be harvested from enterprise directories (Microsoft Active Directory, eDirectory, and Open LDAP) and terminal services offerings (Citrix and Microsoft Terminal Services) while integration with Microsoft Exchange, a Captive Portal, and an XML API enable organizations to extend policy to Apple Mac OS X, Apple iOS, and UNIX users that typically reside outside of the domain.

- **Content-ID: Protecting Allowed Traffic.** Many of today's applications provide significant benefit, but are also being used as a delivery tool for modern malware and threats. Content-ID, in conjunction with App-ID, provides administrators with a two-pronged solution to protecting the network. After App-ID is used to identify and block unwanted applications, administrators can then securely enable allowed applications by blocking vulnerability exploits, modern malware, viruses, botnets, and other malware from propagating across the network, all regardless of port, protocol, or method of evasion. Rounding out the control elements that Content-ID offers is a comprehensive URL database to control web surfing and data filtering features.

- **Purpose-Built Platform: Predictable performance with services enabled.** 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 Applipedia, the Palo Alto Networks encyclopedia of applications.

Appendix 2: Applications Found

The complete list of the 1,195 unique applications found across the 1,636 participating organizations, ranked in terms of frequency are listed below. The frequency is based on the number of organizations where the application was being used. 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. web-browsing
3. ssl
4. ping
5. ntp
6. ms-update
7. netbios-ns
8. flash
9. google-analytics
10. icmp
11. snmp
12. rss
13. soap
14. twitter-base
15. facebook-base
16. adobe-update
17. ocsp
18. google-translate-base
19. gmail-base
20. google-safebrowsing
21. http-audio
22. facebook-social-plugin
23. smtp
24. sharepoint-base
25. http-proxy
26. webdav
27. flickr
28. http-video
29. hotmail
30. silverlight
31. youtube-base
32. photobucket
33. ftp
34. linkedin-base
35. google-app-engine
36. google-toolbar
37. rtmpt
38. google-video-base
39. yahoo-mail
40. google-docs-base
41. msn-webmessenger
42. ldap
43. itunes
44. vimeo
45. yahoo-im-base
46. facebook-chat
47. stumbleupon
48. apple-update
49. ms-ds-smb
50. rtmp
51. facebook-posting
52. google-calendar-base
53. facebook-mail
54. netbios-dg
55. mobile-me
56. skype
57. limelight
58. ms-rdp
59. symantec-av-update
60. meebo-base
61. google-picasa
62. facebook-apps
63. msrpc
64. google-talk-gadget
65. ssh
66. office-live
67. t.120
68. google-cache
69. yahoo-toolbar
70. dropbox
71. flexnet-installanywhere
72. atom
73. asf-streaming
74. msn-base (75%)
75. dailymotion
76. babylon
77. netbios-ss
78. google-desktop
79. skype-probe
80. myspace-base
81. kerberos
82. salesforce
83. twitpic
84. java-update
85. pop3
86. web-crawler
87. paloalto-updates
88. dhcp
89. ooyala
90. teamviewer
91. stun
92. bittorrent
93. skydrive
94. google-earth
95. ipsec-esp-udp
96. 4shared
97. ustream
98. tidaltv
99. google-talk-base
100. rtmpe
101. sip
102. yahoo-webmessenger
103. ike
104. mediafire
105. apple-appstore
106. msn-voice
107. active-directory
108. docstoc
109. ms-netlogon
110. syslog
111. mail.ru-base
112. shoutcast
113. logmein
114. boxnet-base
115. mssql-db
116. telnet
117. megaupload
118. rtp
119. adobe-media-player
120. gmail-chat
121. mssql-mon
122. last.fm
123. zynga-games
124. megavideo
125. netlog
126. time
127. metacafe
128. citrix
129. linkedin-mail
130. slp
131. teredo
132. aim-express-base
133. rtsp
134. filesonic
135. badoo
136. twitter-posting
137. gmail-enterprise
138. yousendit
139. hulu
140. filestube (50%)
141. ms-sms
142. lpd
143. clearspace
144. squirrelmail
145. linkedin-posting
146. vkontakte-base
147. plaxo
148. live365
149. sky-player
150. aim-mail
151. rtcp
152. outlook-web
153. orkut
154. friendfeed
155. myspace-video
156. flixster
157. hp-jetdirect
158. amazon-cloud-player
159. weather-desktop
160. channel4
161. ssdp
162. napster
163. snmp-trap
164. evernote
165. bbc-iplayer
166. fileserve
167. ms-exchange
168. rapidshare
169. akamai-client
170. justin.tv
171. grooveshark
172. hotfile
173. blackboard
174. imap
175. emule
176. facetime
177. foursquare
178. blogger-blog-posting
179. eset-update
180. jabber
181. tudou
182. webex-base
183. dotmac
184. msn-file-transfer
185. webshots
186. daum
187. livejournal
188. gotomeeting
189. yahoo-voice
190. sina-weibo-base
191. blog-posting
192. ebuddy
193. fotki
194. lotus-notes-base
195. radius
196. netflix-base
197. shutterfly
198. ares
199. brighttalk
200. sharepoint-admin
201. avira-antivir-update
202. divshare
203. backweb
204. xunlei
205. oracle
206. depositfiles
207. ipv6
208. coralcdn-user
209. tftp
210. pandora
211. yum
212. ciscovpn
213. friendster
214. meetup
215. upnp
216. horde
217. odnoklassniki-base
218. ms-groove
219. sightspeed
220. steam
221. twig
222. millenium-ils
223. meebome
224. portmapper
225. msn-toolbar
226. reuters-data-service
227. 360-safeguard-update
228. imeem
229. ppstream
230. sharepoint-documents
231. mogulus
232. gre
233. youku
234. zimbra
235. iheartradio
236. alisoft
237. sendspace
238. yahoo-douga
239. gnutella
240. pandora-tv
241. tumblr-base
242. aim-base
243. vbulletin-posting
244. cyworld
245. seesmic
246. google-plus-base
247. imesh
248. mysql
249. flashget
250. adobe-meeting
251. esnips
252. azureus
253. google-docs-enterprise
254. xobni
255. hyves-base
256. kaspersky (25%)
257. ichat-av
258. apt-get
259. trendmicro
260. xing
261. playstation-network
262. qq-mail
263. netvmg-traceroute
264. tcp-over-dns
265. blackberry
266. viber
267. yahoo-calendar
268. netsuite
269. pptp
270. live-meeting
271. google-translate-manual
272. trendmicro-officescan
273. quora
274. avaya-webalive-base
275. myspace-im
276. sugarsync
277. computrace
278. badongo
279. deezer
280. imo
281. phproxy
282. qq-base
283. stickam
284. qvod
285. citrix-jedi
286. netease-mail
287. ms-product-activation
288. renren-base
289. imvu
290. freegate
291. vnc-base
292. kaixin001-base
293. ipsec-esp
294. isatap
295. pogo
296. easy-share
297. youtube-uploading
298. oovoo
299. yourminis
300. daum-mail
301. bet365
302. norton-av-broadcast
303. freenet
304. panda-update
305. itunes-appstore
306. glype-proxy
307. mediawiki-editing
308. roundcube
309. subversion
310. send-to-phone
311. logitech-webcam
312. echo
313. comcast-webmail
314. hamachi
315. live-mesh-base
316. h.323
317. lwapp
318. secureserver-mail
319. hi5
320. pplive
321. rpc
322. dcc-antispam
323. google-calendar-enterprise
324. google-translate-auto
325. yammer
326. open-vpn
327. bugzilla
328. ifolder
329. activesync
330. socks
331. qqmusic
332. veohtv
333. h.245
334. dostupest
335. vmware
336. nintendo-wfc
337. spotify
338. me2day
339. snmpv1
340. gmx-mail
341. mms
342. ebay-desktop
343. google-video-enterprise
344. irc
345. amazon-cloud-drive-uploading
346. capwap
347. carbonite
348. stagevu
349. qqlive
350. google-location-service
351. qq-download
352. pcanywhere
353. itv-player
354. second-life
355. source-engine
356. vnc
357. netflow
358. live-mesh-sync
359. live-mesh-remote-desktop
360. classmates
361. h.225
362. webqq
363. flumotion
364. qq-file-transfer
365. ifile.it
366. kazaa
367. 2ch
368. apple-airport

369. corba
370. icq
371. tikiwiki-editing
372. sharepoint-calendar
373. websense
374. garena
375. funshion
376. itunes-mediastore
377. mail.ru-moimir
378. nimbuzz
379. veetle
380. yoono
381. worldofwarcraft
382. irc-base
383. tor
384. whois
385. wuala
386. kugoo
387. gotomypc-base
388. rsvp
389. yahoo-file-transfer
390. qq-games
391. sina-webuc
392. zamzar
393. google-buzz
394. google-wave
395. jira
396. nfs
397. octoshape
398. concur
399. gtalk-voice
400. baofeng
401. ipp
402. megashares
403. filemaker-pro
404. mail.ru-agent-base
405. cgiproxy
406. pando
407. rip
408. rsync
409. instan-t-file-transfer
410. pp-accelerator
411. amazon-instant-video
412. mixi-base
413. tvu
414. web-de-mail
415. odnoklassniki-messaging
416. hotspot-shield
417. ali-wangwang-base
418. mibbit
419. dcinside-base
420. sap
421. bebo-base
422. discard
423. tacacs-plus
424. files.to
425. ultrasurf
426. daytime
427. iloveim
428. jaspersoft
429. mail.ru-webagent
430. battle.net
431. evony
432. niconico-douga
433. 51.com-base
434. l2tp
435. nntp
436. rhapsody
437. sybase
438. vnc-clipboard
439. fastmail
440. netload
441. ntr-support
442. qik-base
443. yahoo-notepad
444. xdmcp
445. zango
446. mcafee-update
447. zendesk
448. yandex-mail
449. runescape
450. baidu-webmessenger
451. open-webmail
452. lineage
453. minecraft
454. teachertube
455. viadeo
456. msnshell
457. qq-audio-video
458. sopcast
459. microsoft-dynamics-crm
460. renren-chat
461. rpc-over-http
462. snmpv2
463. kkbox
464. simplite-msn
465. google-update
466. cisco-nac
467. cygnet-scada
468. socialtv
469. hangame
470. gadu-gadu
471. sakai
472. all-slots-casino
473. myspace-mail
474. vnc-encrypted
475. yahoo-webcam
476. ms-scom
477. naver-mail
478. editgrid
479. battlefield2
480. chatroulette
481. mail.ru-mail
482. kakaotalk
483. xbox-live
484. bomgar
485. gogobox
486. mount
487. netviewer
488. sccp
489. wins
490. youtube-safety-mode
491. boxnet-editing
492. dameware-mini-remote
493. mozy
494. afp
495. fetion-base
496. uusee
497. cloudmark-desktop
498. adrive
499. tudou-speedup
500. dl-free
501. camfrog
502. ezpeer
503. mgoon
504. tales-runner
505. endnote
506. panos-web-interface
507. gmail-call-phone
508. union-procedure-call
509. vtunnel
510. join-me-base
511. hyves-chat
512. rping
513. ospf
514. sina-weibo-posting
515. studivz
516. whatsapp
517. lotus-sametime
518. yy-voice-base
519. backup-exec
520. flexnet-publisher
521. woome
522. yantra
523. gmail-video-chat
524. svtplay
525. asus-webstorage
526. genesys
527. git
528. ms-win-dns
529. nate-mail
530. ncp
531. warcraft
532. lokalisten
533. clip2net
534. cox-webmail
535. vsee
536. db2
537. regnum
538. radmin
539. smilebox
540. poker-stars
541. renren-music
542. scps
543. direct-connect
544. estos-procall
545. popo-im
546. daum-cafe-posting
547. nateon-im-base
548. plugoo-widget
549. diino
550. filedropper
551. mydownloader
552. t-online-mail
553. freeetv
554. zoho-im
555. transferbigfiles
556. autobahn
557. elluminate
558. informix
559. libero-video
560. checkpoint-cpmi
561. hopster
562. mixi-posting
563. palringo
564. tonghuashun
565. tv4play
566. megashare
567. odnoklassniki-apps
568. renren-posting
569. finger
570. neonet
571. tumblr-posting
572. ameba-now-base
573. gtalk-file-transfer
574. symantec-syst-center
575. zoho-sheet
576. netflix-streaming
577. tivoli-storage-manager
578. vkontakte-chat
579. crashplan
580. gamespy
581. hyves-mail
582. magicjack
583. clubbox
584. cups
585. sflow
586. streamaudio
587. x11
588. yourfilehost
589. inforeach
590. orb
591. att-connect
592. unassigned-ip-prot
593. foxy
594. fs2you
595. spark
596. myspace-posting
597. rsh
598. xunlei-kankan
599. zoho-writer
600. nate-video
601. postgres
602. sling
603. cvs
604. twtkr
605. renren-apps
606. wikispaces-editing
607. wolfenstein
608. kaixin001-mail
609. kontiki
610. sbs-netv
611. aim-file-transfer
612. apple-location-service
613. ndmp
614. neptune
615. soribada
616. vnc-http
617. aol-proxy
618. hyves-games
619. leapfile
620. ms-iis
621. taku-file-bin
622. folding-at-home
623. google-maps
624. soulseek
625. feidian
626. ibm-websphere-mq
627. ip-messenger-base
628. optimum-webmail
629. showmypc
630. forticlient-update
631. gds-db
632. ibm-bigfix
633. brightcove
634. dealio-toolbar
635. yy-voice-games
636. eigrp
637. eve-online
638. move-networks
639. boxnet-uploading
640. igmp
641. messengerfx
642. ms-dtc
643. mcafee-epo-admin
644. steekr
645. call-of-duty
646. earthcam
647. livelink
648. hopopt
649. ms-wins
650. razor
651. emc-documentum-webtop
652. acronis-snapdeploy
653. ali-wangwang-file-transfer
654. ameba-blog-posting
655. im-plus
656. meinvz
657. amazon-cloud-drive-base
658. cpq-wbem
659. ironmountain-connected
660. manolito
661. netmeeting
662. renren-im
663. afreeca
664. air-video
665. babelgum
666. emc-networker
667. maplestory
668. mediamax
669. qdown
670. sophos-update
671. voddler
672. ibm-director
673. ip-in-ip
674. miro
675. naver-blog-posting
676. telenet-webmail
677. mgcp
678. nateon-file-transfer
679. dazhihui
680. fortiguard-webfilter
681. meabox
682. webex-weboffice
683. 51.com-games
684. ammyy-admin
685. filemail
686. fotoweb
687. groupwise
688. korea-webmail
689. naver-ndrive
690. tagoo
691. zoho-wiki
692. google-music
693. ilohamail
694. rift
695. winamax
696. amazon-unbox
697. iccp
698. usermin
699. yahoo-finance-posting
700. fogbugz
701. google-docs-editing
702. ms-lync-video
703. packetix-vpn
704. pim
705. ms-isa-fw-client
706. renren-mail
707. kproxy
708. mail.ru-games
709. mikogo
710. projectplace
711. rlogin
712. avaya-phone-ping
713. cgi-irc
714. drivehq
715. zumodrive
716. hp-data-protector
717. kino
718. userplane
719. bacnet
720. mekusharim
721. pullbbang-video
722. storage.to
723. youseemore
724. 100bao
725. webhard
726. ariel
727. paradise-paintball
728. proxeasy
729. fetion-file-transfer
730. innovative
731. ms-ocs
732. fc2-blog-posting
733. ibackup
734. nateon-desktop-sharing
735. trendmicro-safesync
736. party-poker
737. putlocker
738. wiiconnect24
739. zoho-mail
740. ms-lync-base
741. wccp
742. apc-powerchute
743. bebo-posting
744. livestation
745. netop-remote-control
746. winamp-remote
747. zabbix
748. adnstream
749. seeqpod
750. xfire
751. big-brother
752. yuuguu
753. etherip
754. hyves-music
755. icq2go
756. kaixin-base
757. keyholetv
758. thinkfree
759. vnc-filetransfer
760. daum-blog-posting
761. drda
762. mercurial
763. cddb
764. diodeo
765. drop.io
766. fring
767. magister
768. ms-ocs-file-transfer
769. your-freedom
770. 2ch-posting
771. ameba-now-posting
772. bomberclone
773. vkontakte-mail
774. ypserv
775. igp
776. ovation
777. unreal
778. zoho-crm
779. glide
780. koolim
781. rypple
782. yahoo-blog-posting
783. clarizen
784. daum-touch
785. dcinside-posting
786. ms-lync-audio
787. rdmplus
788. ventrilo
789. nateon-audio-video
790. synergy
791. trinoo
792. zoho-show
793. iscsi
794. ms-lync-apps-sharing
795. rdt
796. snmpv3
797. totodisk
798. aruba-papi
799. cvsup
800. gigaup
801. ibm-clearcase
802. isl-light
803. reserved
804. webconnect
805. cooltalk
806. jap
807. msn-video
808. okurin
809. siebel-crm
810. sugar-crm
811. crossloop
812. doof

813. eroom-host
814. google-docs-uploading
815. hovrs
816. ipsec-ah
817. mobility-xe
818. sina-uc-base
819. zelune
820. asterisk-iax
821. icap
822. lotus-notes-admin
823. megaproxy
824. saba-centra-meeting
825. xm-radio
826. 1und1-mail
827. dabbledb
828. dell-update
829. egloos-blog-posting
830. fasp
831. filemaker-anouncement
832. homepipe
833. vidyo
834. zenbe
835. baidu-hi-games
836. nakido-flag
837. netfolder
838. perfect-dark
839. pna
840. turboupload
841. egp
842. hl7
843. meebo-file-transfer
844. ms-scheduler
845. starcraft
846. vagaa
847. verizon-wsync
848. dhcpv6
849. gbridge
850. ipv6-icmp
851. secure-access
852. adobe-online-office
853. camo-proxy
854. emcon
855. http-tunnel
856. mail.ru-agent-file-transfer
857. splashtop-remote
858. zoho-meeting
859. baidu-hi-base
860. beamyourscreen
861. buddybuddy-base
862. hushmail
863. pup
864. sina-uc-file-transfer
865. sosbackup
866. spotnet
867. tistory-blog-posting
868. argus
869. bgp
870. bigupload
871. exp
872. sctp
873. steganos-vpn
874. vrrp
875. chaos
876. fetion-audio-video
877. fileguri
878. iso-ip
879. laconica
880. netvault-backup
881. perforce
882. secure-access-sync
883. sharebase.to
884. tokbox
885. writeboard
886. yugma
887. aim-express-file-transfer
888. arcserve
889. dnp3
890. eatlime
891. esignal
892. peerguardian
893. prm
894. skip
895. usejump
896. zoho-notebook
897. iperf
898. mail.com
899. paltalk-base
900. pownce
901. qik-video-chatting
902. rwho
903. suresome
904. swapper
905. timbuktu
906. vyew
907. war-rock
908. xns-idp
909. dcn-meas
910. idpr-cmtp
911. idrp
912. ipcomp
913. leaf-1
914. netbotz
915. nvp-ii
916. rvd
917. udplite
918. wlccp
919. 3pc
920. bbn-rcc-mon
921. blin
922. caihong
923. emc-smartpackets
924. good-for-enterprise
925. ippc
926. mobile
927. noteworthy-admin
928. noteworthy-base
929. paran-mail
930. rusers
931. sat-expak
932. sun-nd
933. x-font-server
934. cbt
935. dccp
936. eroom-net
937. fire
938. fluxiom
939. ipv6-nonxt
940. ipv6-opts
941. iso-tp4
942. lan
943. mcafee
944. narp
945. pgm
946. ptp
947. realtunnel
948. reliable-data
949. rstatd
950. sm
951. trunk-2
952. uti
953. xtp
954. yoics
955. baidu-hi-file-transfer
956. bna
957. daap
958. ggp
959. gotomypc-printing
960. graboid-video
961. gyao
962. hitachi-spc
963. kryptolan
964. modbus-base
965. mpls-in-ip
966. mux
967. radiusim
968. remobo
969. seven-email
970. srp
971. sscopmce
972. swipe
973. techinline
974. tinyvpn
975. tlsp
976. visa
977. woofiles
978. xnet
979. 51.com-bbs
980. aris
981. bebo-mail
982. bluecoat-auth-agent
983. callpilot
984. chinaren-base
985. compaq-peer
986. cphb
987. cpnx
988. dfs
989. dgp
990. dsr
991. echoware
992. encap
993. fufox
994. gnu-httptunnel
995. gridftp
996. hmp
997. host
998. iatp
999. idpr
1000. il
1001. i-nlsp
1002. ipv6-frag
1003. irtp
1004. knight-online
1005. larp
1006. leaf-2
1007. mfe-nsp
1008. mobilehdr
1009. netblt
1010. paltalk-express
1011. pnni
1012. sdrp
1013. secure-vmtp
1014. sip-application
1015. stp
1016. subspace
1017. ttp
1018. turboshare
1019. tvants
1020. vines
1021. wetpaint-editing
1022. 51.com-webdisk
1023. activenet
1024. asproxy
1025. br-sat-mon
1026. ddx
1027. fibre-channel
1028. file-host
1029. gmtp
1030. gotomypc-file-transfer
1031. ifmp
1032. instan-t-webmessenger
1033. ipcv
1034. iplt
1035. ip-messenger-file-transfer
1036. ipv6-route
1037. ipx-in-ip
1038. isis
1039. jumpdesktop
1040. meevee
1041. merit-inp
1042. moinmoin-editing
1043. nsfnet-igp
1044. pipe
1045. private-enc
1046. pvp
1047. qnx
1048. sat-mon
1049. smp
1050. snp
1051. sprite-rpc
1052. sps
1053. st
1054. tcf
1055. tradestation
1056. unyte
1057. vidsoft
1058. vmtp
1059. wb-expak
1060. wb-mon
1061. wsn
1062. cftp
1063. crtp
1064. crudp
1065. ddp
1066. dimdim
1067. distcc
1068. i2p
1069. ipip
1070. jxta
1071. mtp
1072. netop-on-demand
1073. officehard
1074. oracle-bi
1075. paltalk-superim
1076. pcvisit
1077. phonemypc
1078. phpwiki-editing
1079. rediffbol-audio-video
1080. share-p2p
1081. trunk-1
1082. wallcooler-vpn
1083. wikidot-editing
1084. altiris
1085. bluecoat-adn
1086. frozenway
1087. gizmo
1088. gomeetnow
1089. imhaha
1090. joost
1091. modbus-read-holding-registers
1092. ms-frs
1093. ms-virtualserver
1094. nagios
1095. netspoke
1096. pingfu
1097. schmedley
1098. sharepoint-blog-posting
1099. sharepoint-wiki
1100. tuenti
1101. zoho-share
1102. ad-selfservice
1103. airaim
1104. ants-p2p
1105. buddybuddy-file-transfer
1106. chinaren-chat
1107. desktoptwo
1108. dynamicintranet
1109. fastviewer
1110. firephoenix
1111. fuze-meeting-base
1112. jango
1113. maxdb
1114. qik-viewing
1115. ragingbull-posting
1116. rediffbol-base
1117. r-exec
1118. spirent
1119. surrogafier
1120. vnn
1121. winny
1122. ali-wangwang-audio-video
1123. avaya-webalive-desktop-sharing
1124. beinsync
1125. bonpoo
1126. chinaren-apps
1127. dclink
1128. doshow
1129. fly-proxy
1130. google-finance-posting
1131. instan-t-base
1132. medium-im
1133. modbus-read-coils
1134. modbus-read-input-registers
1135. motleyfool-posting
1136. ossec
1137. pichat
1138. propalms
1139. sina-uc-remote-control
1140. socks2http
1141. spark-im
1142. stealthnet
1143. tvtonic
1144. vakaka
1145. we-dancing-online
1146. winmx
1147. wixi
1148. yosemite-backup
1149. zwiki-editing
1150. 51.com-music
1151. 51.com-posting
1152. aim-audio
1153. aim-video
1154. ali-wangwang-remote-control
1155. baidu-hi-audio-video
1156. batchbook
1157. bypassthat
1158. chargen
1159. chinaren-mail
1160. circumventor
1161. evalesco-sysorb
1162. eyejot
1163. filer.cx
1164. fuze-meeting-desktop-sharing
1165. generic-p2p
1166. gnunet
1167. google-lively
1168. groupmax
1169. jnet
1170. kaixin-mail
1171. lifecam
1172. little-fighter
1173. meeting-maker
1174. meetro
1175. modbus-write-single-register
1176. msn2go
1177. ms-ocs-video
1178. oridus-nettouch
1179. outblaze-mail
1180. paloalto-userid-agent
1181. paran-u2
1182. peercast
1183. peerenabler
1184. qik-sharing
1185. ruckus
1186. simple-im
1187. sina-uc-web-disk
1188. track-it
1189. warez-p2p
1190. webex-desktop-sharing
1191. webot
1192. webrdp
1193. zoho-db
1194. zoho-peoplezoho-planner