The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

9th Edition, June 2012

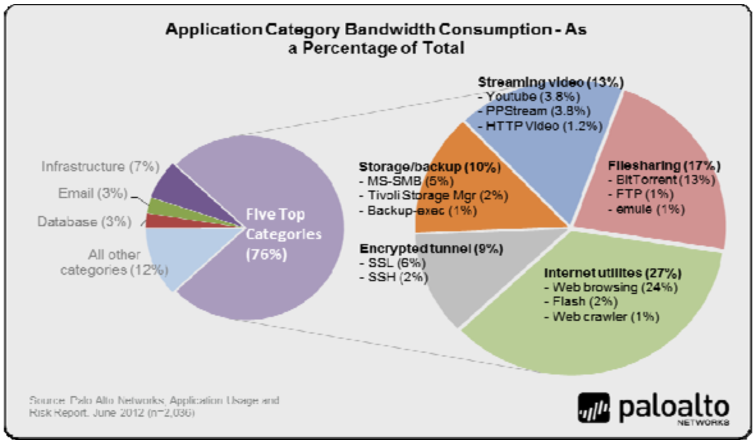
Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 94089
www.paloaltonetworks.com

Table of Contents

Executive Summary

The *Application Usage and Risk Report (9th Edition, June 2012)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing network traffic assessments conducted in 2,036 organizations worldwide between November 2011 and May 2012.

The application usage patterns observed on today's networks showed a significant increase in what could be described as personal application use. Streaming media usage bandwidth consumption crossed into the double digits and in doing so, becomes an even more serious threat to bandwidth sensitive business applications. When combined with double digit bandwidth consumption of filesharing, the amount of bandwidth consumed by these was measured at 30%. Viewed in terms of budget dollars, nearly a third of every dollar spent on bandwidth is for either streaming video or filesharing – a large portion of which is likely to be personal use. Figure 1 shows the top five application categories based on the percentage of total bandwidth consumed and the three top applications within each category.



Source: Palo Alto Networks, Application Usage and Risk Report, June 2012 (n=2,036)

Figure 1: Top five categories and applications based on percentage of bandwidth consumed.

The social networking market continues to define and segment itself as evidenced by the rapid emergence of Pinterest and the relatively sudden uptick in the use of Tumblr, both of which allow users to express themselves in new ways.

Key findings include:

Streaming video bandwidth consumption triples to 13%.

- The bandwidth consumed by streaming video tripled to 13% of total bandwidth consumed and now represents a more significant infrastructure challenge to organizations.

P2P filesharing bandwidth consumption skyrockets 700%.

- P2P filesharing bandwidth consumption jumped to 14% of overall bandwidth observed, crushing all other application categories. Browser-based filesharing held steady at roughly 1% of overall bandwidth.

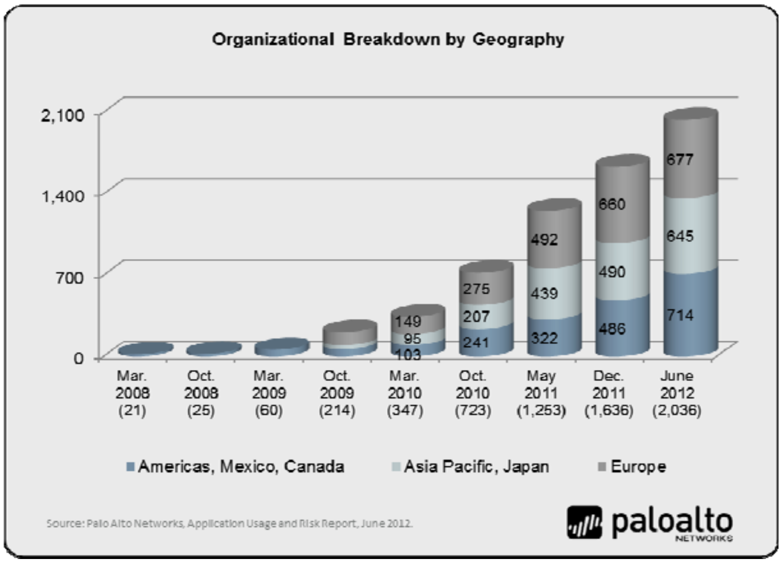
Social networking continues to define itself.

- Two new social networking applications, Tumblr and Pinterest both gained traction in terms of frequency and volume of use despite the dominance that both Facebook and Twitter exhibit. These new applications confirm that social networking, as a category is continuing to define itself.

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 2,036 traffic assessments performed worldwide. The distribution of the participating organizations is distributed fairly equally across three geographic regions: Americas, Mexico, Canada, Asia Pacific/Japan and Europe. The findings within this report will focus solely on the global view of application traffic with any regional specific variations in usage patterns discussed separately.



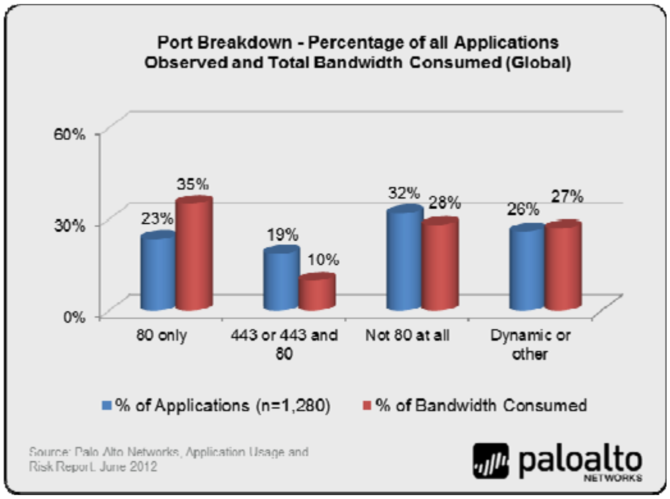
Source: Palo Alto Networks, Application Usage and Risk Report, June 2012.

Figure 2: Geographic distribution of participating organizations.

With browser-based filesharing and social networking dominating the news conversations lately, one would think all the traffic is traversing tcp/80 in the form of web browsing. Nothing could be further from the truth. Traffic traverses all ports, all the time, regardless of whether or not it is browser-based, client-server or peer-to-peer. In the previous Application Usage and Risk report, a discussion of which ports applications use and how much bandwidth is traversing those ports was introduced. The goal was to elevate the discussion to consider more than just port 80. The reason is quite simple – if a security practitioner focuses only on port 80, then they are effectively protecting the front door, while leaving the side and back door unlocked.

The 1,280 applications and associated bandwidth were broken into four groups based on the default port they use:

- Applications that use tcp/80 only.
- Applications that use tcp/443 or tcp/443 and tcp/80.
- Applications that do not use tcp/80 at all
- Applications that are dynamic (hop ports) or use a range of high number/non-standard ports.



Source: Palo Alto Networks, Application Usage and Risk Report. June 2012

Figure 3: Port group analysis by application and bandwidth.

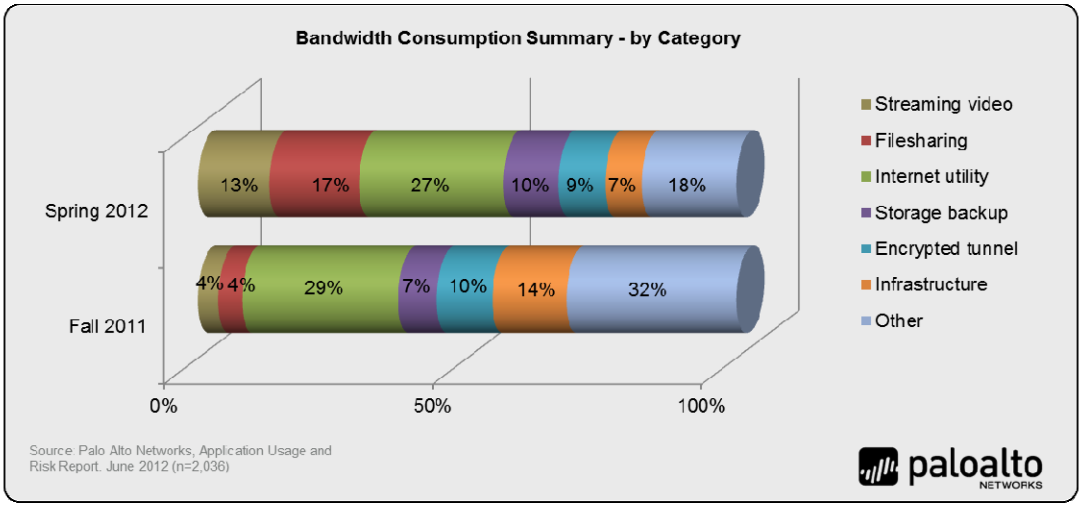
As with the previous report, a significant portion of the applications and the bandwidth are NOT using port 80 and must be included in the security policy discussions. In this report, where appropriate the findings will include a discussion about which port the applications use as a means of re-enforcing the fact that applications have evolved to the point where any application is capable of traversing any port.

Streaming Media Bandwidth Consumption Triples

When asked why the network is slow, one of the most common replies has been to blame congestion due to streaming media and photo applications. Historically, the data has indicated that the bandwidth consumption, relative to other application categories, is insignificant enough to dispute that statement.

Not anymore.

The analysis showed that video streaming application bandwidth consumption more than tripled to 13% of the overall bandwidth observed. For comparison, the previous report published in December 2011 showed that the streaming video bandwidth consumption was only 4% of total – as shown in Figure 4.



Source: Palo Alto Networks, Application Usage and Risk Report. June 2012 (n=2,036)

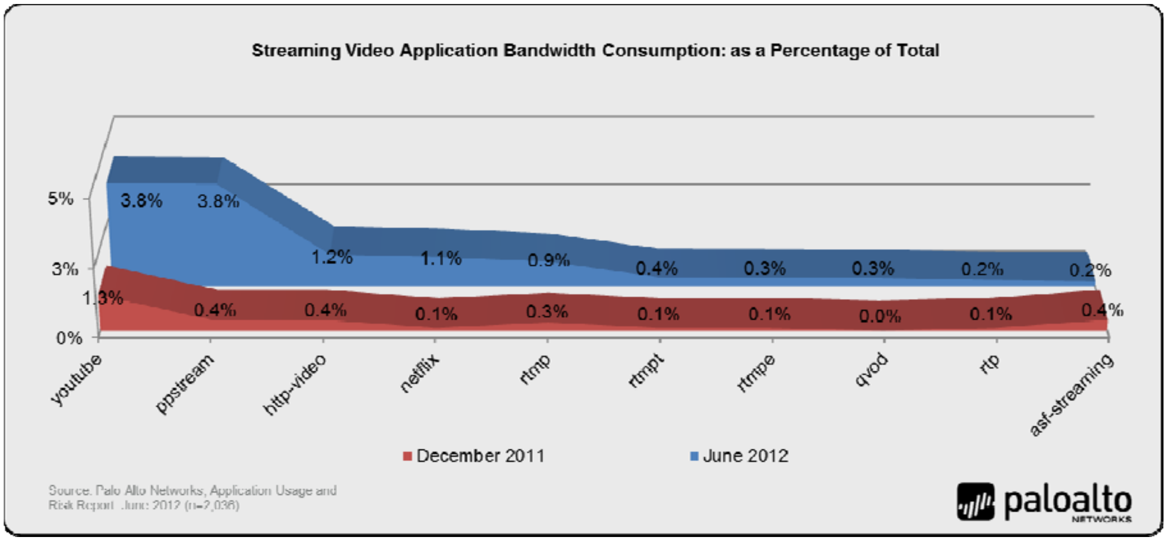
Figure 4: Application category bandwidth consumption summary.

With a 300% increase in bandwidth consumed, the immediate reaction is to look for a significant event of one form or another such as a World Cup Soccer tournament or perhaps the Olympics, but in this time period there were no significant streaming video events (like the upcoming Olympics) that could explain the increase.

Within the applications found across each geographical region, the top 3-5 applications consumed the bulk of the bandwidth with YouTube being the most significant contributor to the bandwidth consumption in two of the four regions.

- Japan: YouTube consumed the most bandwidth with two local streaming applications, Nico Nico Douga (Smile Video) and Yahoo Douga (Yahoo Video) as the next two most heavily used.
- APAC: the most significant consumer of bandwidth is PPStream (PPS) while YouTube and Qvod rounded out the top three video applications.
- In the Americas, YouTube, Netflix and generic HTTP video were the top three consumers of bandwidth.
- In EMEA, YouTube, HTTP Video and RTMP (Real Time Messaging Protocol, used to stream video to Flash Player) were the most heavily used.

Interestingly, the amount of YouTube uploading, identified separately from YouTube, is nearly immeasurable indicating that the usage is indeed "watching". Figure 5 shows the top 10 streaming video applications and the percentage of the total bandwidth they are consuming.



Source: Palo Alto Networks, Application Usage and Risk Report June 2012 (n=2,036)

Figure 5: Streaming video application bandwidth consumption comparison.

While both YouTube and PPS increased in usage, so too did many of the other applications within this group, implying that the increase in bandwidth consumed is primarily the result of an overall increase in use.

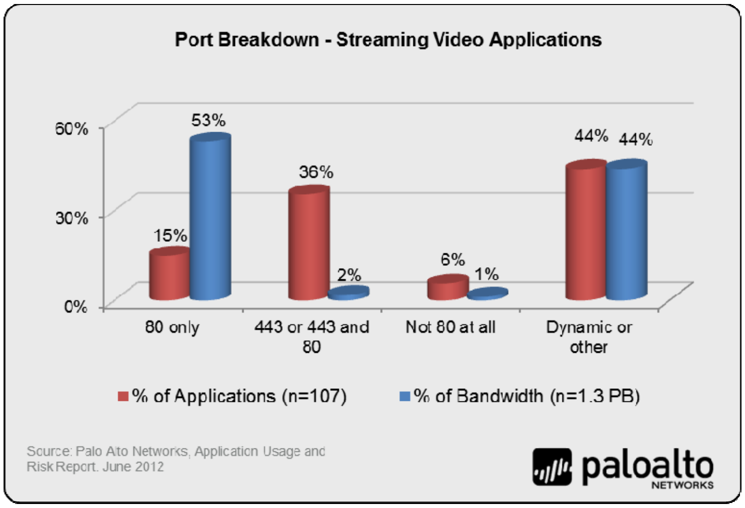
- Out of the 115 different streaming video and photo applications currently identified by Palo Alto Networks, 107 variants were found in use during the six month period, which is the second highest number of applications behind filesharing at 140.
- At least one streaming video or photo application was detected on 97% of the participating organizations.
- An average of 34 different streaming video or photo applications were found on each network, making these applications the most common type found and lending support behind the argument that the majority of the traffic is end-user oriented (personal use).

Regardless of where the increase originated, these applications represent a range of security and business risks for all organizations.

Streaming Video Business Risks

While at work, everyone will take some personal time to take care of daily requirements that life brings; a conference call with the teacher, a follow-up call with the doctor, a comfort-call to an upset child. In most organizations, some level of personal time is tolerated and yes, even the occasional cat video on YouTube is often times tolerated. However, when 13 out of every 100 kilo, mega or gigabyte is being consumed by streaming video – either personal and work-related, the management tolerance level may be exceeded.

- **Business continuity risks:** there are two factors to take into consideration—the first is the impact on specific business applications that may cause unacceptable performance. The second consideration is the overall impact made to the network and the frustration a business application end-user may ultimately experience due to bandwidth starvation imposed by streaming video.
- **Operational costs:** the most obvious impact caused by the increase in streaming video is the need to either buy more bandwidth, or buy a set of tools to exert greater bandwidth control. The less obvious impact is the cost involved in addressing any security risks associated with the use of streaming video applications: (e.g., rebuilding servers or networks following a security incident involving an exploit or virus).
- **Productivity costs:** it is impossible to determine the breakdown of work vs. personal use for this group of applications but with 107 different application found, it is safe to say that there is a significant amount of personal use occurring. For example, PPStream, Hulu Networks and Netflix focus exclusively on entertainment broadcast– not marketing, education, or training. Stated more directly, at 13% of the total bandwidth, there is a significant amount of personal video watching going on that may become a productivity challenge.



Source: Palo Alto Networks, Application Usage and Risk Report. June 2012

Figure 6: Streaming video application and bandwidth summary by port group.

As the image shows, the bulk of the bandwidth is either tcp/80, or tcp80 "plus" meaning an additional range of ports (see page 4 for port group definitions) or the application is dynamic (can hop ports).

Streaming Video Security Risks

The security risks associated with streaming video can be loosely categorized as either indirect and direct. An indirect security risk might be the use of the video as bait to entice the unsuspecting user into clicking to watch the funny cat video but behind the scenes, the user is unknowingly downloading a piece of malware. The risk of videos as bait is more significant than ever before because of the elevated levels of trust that social networking has established. For example, when a good friend forwards a video link, how many users will think twice before clicking to watch? Very few. Cyber criminals know this and take full advantage of it in a process commonly referred to as likejacking.

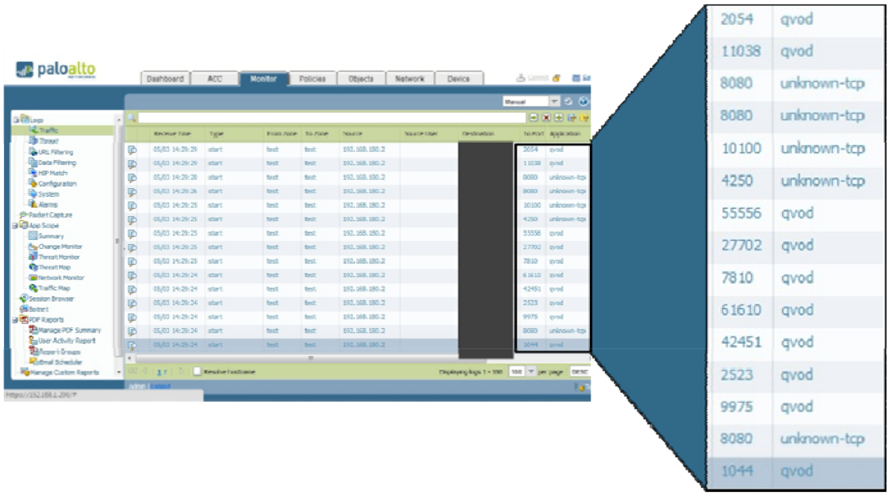
In short, likejacking is a form of social media spam where you are sent a video and encouraged to "Like" it, which in turn posts a notice automatically to your wall saying you "Like" it. Your friends see it, and they too "Like" it and the scam goes viral. In this PCWorld article, by Dan Tynan, one such likejacking scam lead to a request for personal information and potentially, a malware download.

The direct security risks are the specific threats or vulnerabilities associated with the application. In the case of YouTube, it is being delivered by Google over HTTP to the browser. The security risks are going to be associated with the media players, or in downloading the whole video file that may have a virus embedded.

With the browser as the receiver of the video, the risks expand to include XSS attacks and HTML injections over time, but the risks in the players and the browser will exist even if no video is being watched.

P2P Streaming and Unknown Malware

When the underlying technology is P2P-based and used in a less controlled environment, the application and unsuspecting users are more susceptible to infection. The reason for this is that P2P allows a botnet to survive even if its command and control servers are taken down or compromised. Recently, Palo Alto Networks WildFire observed the use of the P2P-based streaming video application Qvod being used to enable malware communications, or as the starting point for new customized P2P protocols.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
	05/03 14:29:29	start	test	test	192.168.180.2		[redacted]	2054	qvod
	05/03 14:29:29	start	test	test	192.168.180.2		[redacted]	11038	qvod
	05/03 14:29:28	start	test	test	192.168.180.2		[redacted]	8080	unknown-tcp
	05/03 14:29:26	start	test	test	192.168.180.2		[redacted]	8080	unknown-tcp
	05/03 14:29:25	start	test	test	192.168.180.2		[redacted]	10100	unknown-tcp
	05/03 14:29:25	start	test	test	192.168.180.2		[redacted]	4250	unknown-tcp
	05/03 14:29:25	start	test	test	192.168.180.2		[redacted]	55556	qvod
	05/03 14:29:25	start	test	test	192.168.180.2		[redacted]	27702	qvod
	05/03 14:29:25	start	test	test	192.168.180.2		[redacted]	7810	qvod
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	61610	qvod
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	42451	qvod
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	2523	qvod
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	9975	qvod
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	8080	unknown-tcp
	05/03 14:29:24	start	test	test	192.168.180.2		[redacted]	1044	qvod

2054	qvod
11038	qvod
8080	unknown-tcp
8080	unknown-tcp
10100	unknown-tcp
4250	unknown-tcp
55556	qvod
27702	qvod
7810	qvod
61610	qvod
42451	qvod
2523	qvod
9975	qvod
8080	unknown-tcp
1044	qvod

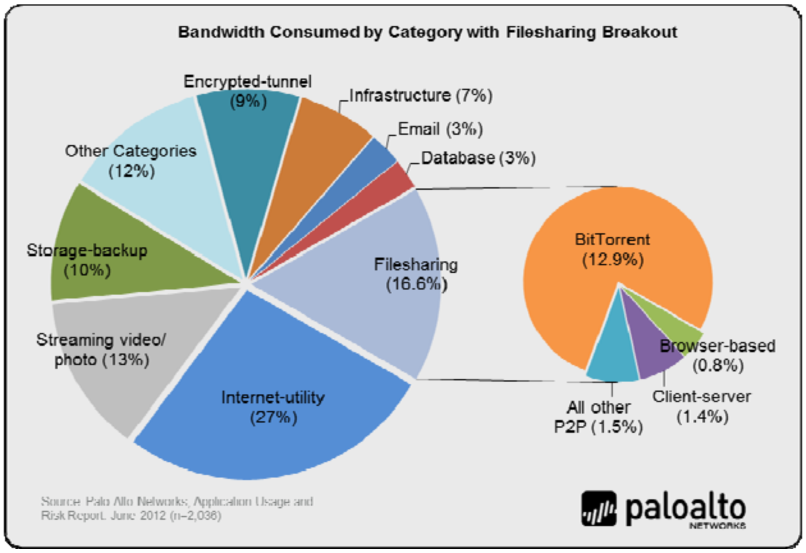
Image 1: Unknown traffic log analysis exposes malware using Qvod to communicate outside of the network.

Image 1 shows how the initially unknown malware was targeting a wide-range of ports as a means of traversing the firewall. The image also highlights the critical requirement for identifying and controlling, in a systematic manner, unknown tcp and udp traffic.

P2P Filesharing Bandwidth Consumption Increases 700%

In recent months, at least three new browser-based filesharing applications were announced. Google Drive was brought to market with significant fanfare; Facebook announced a filesharing feature that would be made available to Facebook groups (initially); and Citrix introduced its ShareFile service. These new applications enter into what is already a very crowded market of at least 70 different filesharing variants, renewing concerns over privacy and security.

While the news and excitement over new browser-based filesharing applications runs its course, P2P filesharing quietly continues to be used across all manner of organizations, despite efforts to control it. The analysis shows that P2P filesharing bandwidth consumption jumped to 14% of overall bandwidth observed, up from 2% in the previous report. For comparison, browser-based filesharing held steady at roughly 1% of overall bandwidth.



Source: Palo Alto Networks, Application Usage and Risk Report, June 2012 (n=2,036)

Figure 7: Filesharing bandwidth consumption summary – by underlying technology.

As with the streaming media figures, the question that immediately comes to mind is “Why the sudden increase in P2P bandwidth consumption?” The volume of application variants (only 38) and the frequency of use (78%) are significantly lower compared to streaming video discussed earlier. The increase in P2P is merely a dramatic spike in usage, not tied to any one particular event or application.

- Out of 38 variants found during the six month period, at least one P2P application was detected on 78% of the participating organizations. On average, 7 different P2P applications were found on each network.

- Geographically, there is less variation than observed in the streaming video category, because the same applications are used heavily in all parts of the world. In all four regions, BitTorrent was the most heavily used worldwide. Table 1 shows the top 3 P2P applications across all regions with the percentage of total bandwidth consumed.

Americas	APAC	EMEA	Japan
BitTorrent (1%)	BitTorrent (10.9%)	BitTorrent (1%)	BitTorrent (0.1%)
eMule (0.4%)	eMule (1.1%)	eMule (0.04%)	Ares (0.01%)
Azureus (0.1%)	Xunlei (0.2%)	Ares (0.01%)	eMule (0.001%)

Table 1: Top P2P applications per geography with percentage of total bandwidth consumed.

Business and Security Risks Both Old and New

P2P filesharing risks are well known. The most well-known risk is the loss of data through improper use. Breaches in the millions of records have occurred in the past and there was the well documented incident where blueprints of MarineOne, United States President Obama's helicopter were found on a P2P network. The risk of data loss remains significant as evidenced by the February 2012 notice sent by the FTC to more 100 organizations of all types informing them that their confidential data was floating around on P2P filesharing networks and that it was their responsibility to exert control over that data. From the warning sent to the violators:

> *"The notices went to both private and public entities, including schools and local governments, and the entities contacted ranged in size from businesses with as few as eight employees to publicly held corporations employing tens of thousands."*

In addition to data loss, copyright infringement risks are ever present with significant fines being levied against violators. Higher education institutions are constantly battling to control P2P, spending countless hours and dollars responding to RIAA warning letters.

In terms of security threats to the network, what's old is new. The distributed nature of P2P is a fundamental part of the technology works, and also underlies what makes it so risky. Because files can be uploaded to a P2P network and distributed to a tracker anonymously, the use of P2P poses significant moral hazard, as it provides a convenient and risk free method to distribute malware to a large user population anonymously.

A newer form of security threat is the use of commercial P2P networks as a means of botnet command and control – the Mariposa botnet was the first example and more recently, the TDL-4 botnet. Two other examples of the use of proprietary P2P include Waledac, and the Zeus/Spyeye botnets. The use of a commercial or proprietary P2P network for botnet command and control makes perfect sense to the cybercriminal. Like the many-headed Hydra from Greek mythology, whose head can never be severed, so too will a P2P network always live.

Browser-based Filesharing Maintains Popularity

P2P filesharing may be the dominant choice for sharing large files, however, browser-based filesharing is significantly more popular in terms of frequency of use and the number of variants found.

- Out of the 140 filesharing applications found, 71 of them are browser-based, 38 are P2P and the remainder are client-server.
- At least one browser-based filesharing application was detected on 89% of the participating networks.
- An average of 13 different browser-based filesharing applications were found on each network.

The business and security risks that surround browser-based filesharing are well known, with new concerns arising as popularity and usage increases. Data loss, purposeful or not, and copyright violations are the most common business risks. As more of these offerings add premium services like autosynch, the risks of data loss will only increase.

With the recent filesharing announcements from Facebook and Google, the terms-of-service and who owns the data have become cause for concern both for individuals and for organizations. The concern arises primarily from two angles. First, the byzantine language used in the terms of service is such that few outside of the legal profession understand what they are reading and second, the fact that both Facebook and Google admittedly analyze the content stored in their services for marketing purposes, making organizations rightfully concerned about employees using these applications.

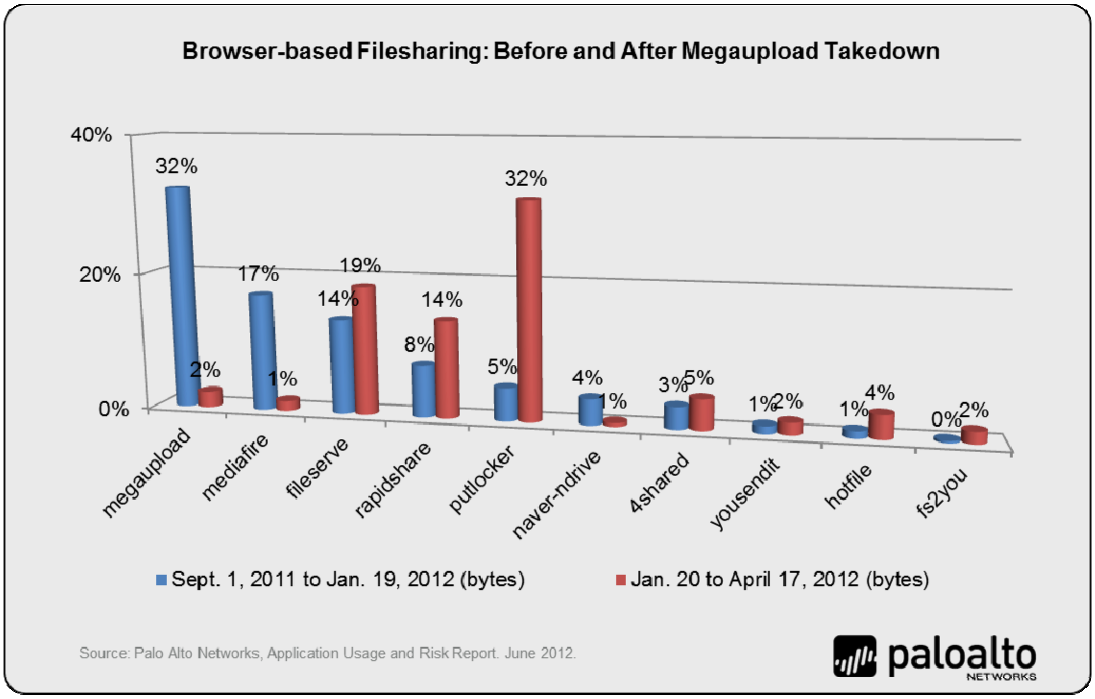
From a security risk perspective, browser-based filesharing applications are rapidly becoming associated with malware and cybercrime, much like FTP and P2P already have. For those browser-based variants that are searchable and accessible by all, and posted anonymously, users can easily be infected – just as they are on P2P networks and on FTP sites. The free and anonymous nature of the application – sign up with an email – make them easy for cybercriminals to use as part of their malware distribution infrastructure.

With Google, Facebook and Citrix all announcing browser-based filesharing alternatives, on top of the other 70 or so existing offerings, this group of applications shows no signs of going away or slowing down. However, with so many variants there will no doubt be some additional segment refinement and use case definition as they all struggle to compete and survive.

Where Did The Megaupload Traffic Go?

On January 19th 2012, Megaupload was shut down by the United States Department of Justice. Until that time, Megaupload was found on around 60% of the participating organizations' networks and it regularly consumed as much as 32% of the browser-based filesharing bandwidth (as opposed to total bandwidth). Megaupload was used primarily as a source for entertainment (movies, games, etc) or software programs (freeware, shareware), as opposed to productivity or work-related use. Once Megaupload was shut down, the question became, where did the Megaupload traffic go?

Based on a shift in bandwidth consumed before and after the Megaupload takedown, it would appear that Putlocker, Rapidshare and Fileserve each benefitted from the demise of Megaupload. Putlocker showed a significant increase in frequency of use, moving from 5% to 32%. The two datasets in Figure 8 represent 80% and 85% of the browser-based filesharing bandwidth respectively. The remaining 61 variants consumed the other 20%



Source: Palo Alto Networks, Application Usage and Risk Report. June 2012.

Figure 8: Browser-based filesharing application bandwidth consumption before and after Megaupload.

Which Ports Do Filesharing Applications Really Use?

All applications within the Palo Alto Networks database include underlying technology (browser-based, peer-to-peer, etc) as well as which ports the applications use. These data points are crucial to helping an administrator learn more about the applications traversing the network as a means of ultimately enabling or blocking them, depending on which is appropriate. The 140 filesharing and file transfer applications were broken down into four port groupings defined as:

- **Applications that use tcp/80 only – no other ports are used.** As expected, the bulk of the applications in this group are browser-based. Putlocker, Depositfiles and Docstoc are three browser-based examples of the applications found in this group.

- **Applications that use tcp/443 or tcp/443 and tcp/80.** Applications within this group use both tcp/80 and/or tcp/443. RapidShare, 4Shared and YouSendIt! are three of the browser-based filesharing application examples while Sugarsync and Microsoft Live Mesh represent two of the client-server based examples.

- **Applications that do not use tcp/80 at all.** All of these applications are either client-server (FTP, TFTP) or peer-to-peer. The peer-to-peer applications in this group are using a range of ports and include Ares, DirectConnect and Kazaa.

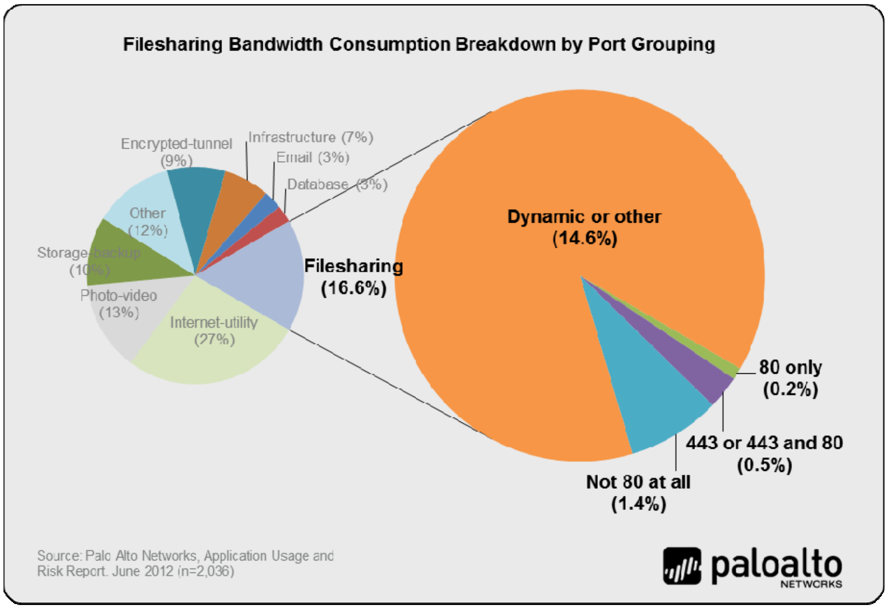
- **Applications that are dynamic (hop ports), or use a range of high numbered ports.** As expected, this group of applications is primarily peer-to-peer and includes BitTorrent, eMule and Xunlei. The browser-based examples within this group include Fileserve, Filesonic, and Mediafire. As a user accessibility and firewall evasion feature, port hopping (aka, dynamic) has historically been used in either client-server or peer-to-peer applications. The use of port hopping in browser-based applications reaffirms how significantly applications have evolved.

	Underlying Application Technology		
Port Group	Browser-based	Client-server	Peer-to-peer
80 only	35	2	0
443 only, or 443 and 80	27	12	3
Not 80 at all	0	5	12
Dynamic or other	9	12	23

Table 2: Underlying technology and default port break down for filesharing applications.

The table above summarizes the port groups while Figure

8 displays the bandwidth consumption based on the ports, as opposed to the underlying technology. The value of looking at the filesharing bandwidth from a port group perspective is that it shows that nearly all of the filesharing bandwidth (14.6%) is capable of evading typical port-based controls by intelligently hopping from port-to-port.



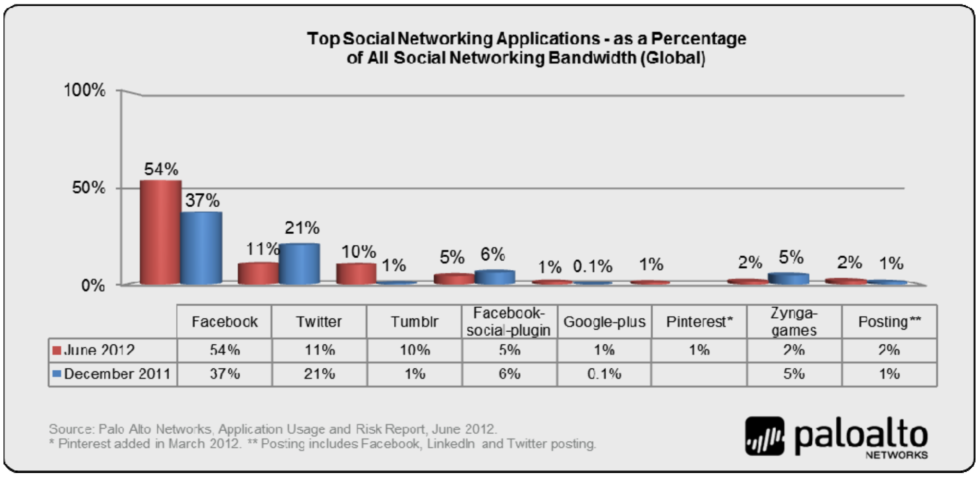
Source: Palo Alto Networks, Application Usage and Risk Report. June 2012 (n=2,036)

Figure 9: Filesharing/file transfer application bandwidth consumption breakdown – by port group.

Social Networking: New Ways to Express Yourself

To use a social networking applications means that a user has to talk about themselves with friends, family and acquaintances – casual or otherwise – at some level. Otherwise, the conversations will be very one-sided. The data shows that Facebook and Twitter, to no ones' surprise, showed consistency in the market lead. Additionally, the data continues to support the assertion that most of the traffic is still voyeuristic – meaning users are doing more browsing than posting – based on the amount of bandwidth consumed.

However, as Facebook executes their public offering, new social networking applications are consuming more social networking bandwidth (as opposed to total) than many other pre-existing social networking applications.



	Facebook	Twitter	Tumblr	Facebook-social-plugin	Google-plus	Pinterest*	Zynga-games	Posting**
🟥 June 2012	54%	11%	10%	5%	1%	1%	2%	2%
🟦 December 2011	37%	21%	1%	6%	0.1%		5%	1%

Source: Palo Alto Networks, Application Usage and Risk Report, June 2012.
* Pinterest added in March 2012. ** Posting includes Facebook, LinkedIn and Twitter posting.

Figure 10: Breakdown of the top social networking bandwidth consumption by application.

The bandwidth consumption distinction is important because the view of social networking as a bandwidth hog is erroneous; the total bandwidth consumed by all social networking applications is a mere 1%. As a category, it is ranked 12th out of 25, far behind other categories such as audio streaming, email, and management.

- Out of the 80 social networking applications identified by Palo Alto Networks, 74 variants were found during the six month period, the sixth highest number of application variants found.
- At least one social networking application was detected on 97% of the participating organizations.
- An average of 29 different social networking applications were found on each of the networks, making these applications the second most common type found behind streaming video applications.

At its young age, it is hard to call Facebook a legacy application, but the speed that the social networking market is evolving means that new participants like Google+, Tumblr and Pinterest, with new features may challenge the existing offerings. Each of these three offerings is relatively new while showing some of the heaviest use in terms of bandwidth consumption.

Tumblr Traffic Increases Ten-fold

Tumblr uses tumblelogging, commonly viewed as a precursor to microblogging (Twitter), to publish stream-of-consciousness using photos, videos, quotes and other multimedia snippets. From the TechCrunch company profile:

> *Tumblr is a re-envisioning of tumblelogging, a subset of blogging that uses quick, mixed-media posts. The service hopes to do for the tumblelog what services like LiveJournal and Blogger did for the blog. The difference is that its extreme simplicity will make luring users a far easier task than acquiring users for traditional weblogging. Anytime a user sees something interesting online, they can click a quick "Share on Tumblr" bookmarklet that then tumbles the snippet directly. The result is varied string of media ranging links and text to pictures and videos that takes very little time and effort to maintain.*

The jump in volume of use for Tumblr is hard to determine but some of the reasons may be found in the many significant differences between Facebook and Tumblr.

- **Tumblr is unfiltered.** You can say and post whatever you want on Tumblr – EVEN IN ALL CAPS – all without fear of big brother-like censorship. For those who are interested in this form of sharing, Tumblr is the ideal solution. But from a business and marketing perspective the unfiltered nature of Tumblr may be one of the key drawbacks. As a warning, a new Tumblr user will want to be very careful what they search for. In contrast, Facebook is very filtered. Inappropriate words are ****ed out, as is some of the imagery.

- **Tumblr is completely customizable.** Users can create their own look and feel, eliminating nearly all of the Tumblr branding. The four screen shots below are a few of the examples found that highlight the customization capabilities (note that the Smarter Planet site is an IBM site). Facebook on the other hand enables a limited amount of customization.

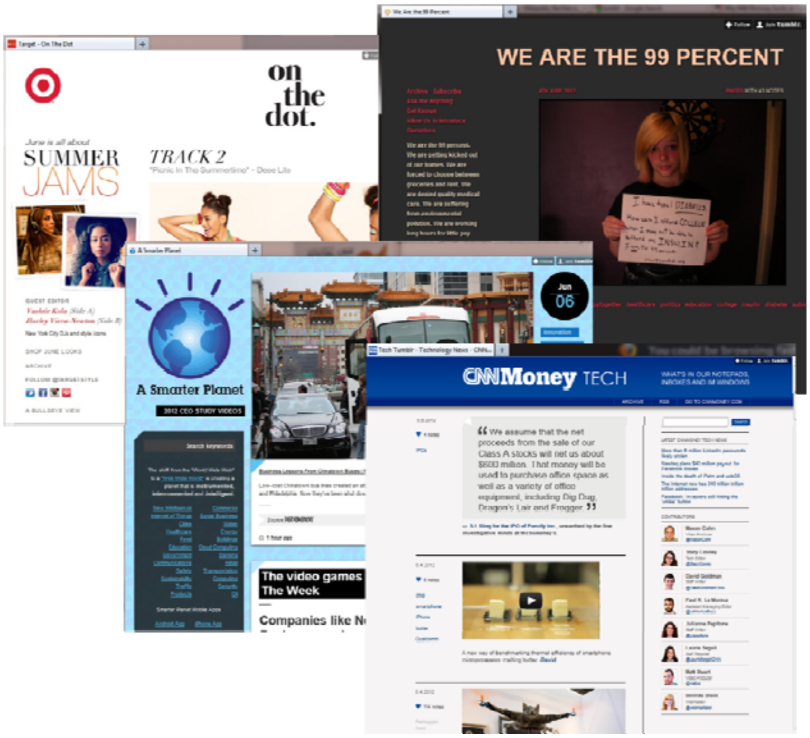


Image 2: Examples of Tumblr customization capabilities.

- **Tumblr ad free – for now.** Tumblr is only now beginning to determine how to monetize their content and their user-base, as evidenced first by the recent announcement of the availability of advertising blocks. The lack of a monetization model and the newness of Tumblr may have limited the number of corporations who are using it as part of their social media initiatives.

  As Jason Keath points out in this Social Fresh article, Tumblr may not work for every brand. Of the 60 companies listed, many are content delivery (websites, publishers, broadcast media) focused, as opposed to hard goods focused.

Going back to the original question of where does the increase in Tumblr usage come from? The exact answer is unclear. However, given the unfiltered nature of Tumblr, its newness and relative low profile in the market, the volume of content delivery focused Tumblr-blogs, it is safe to say that the majority of the increase is from personal use, as opposed to business use.

Pinterest: Look What I Did Today!

Pinterest is a very new application that allows you to "pin" items (pictures, images, links, articles, etc.) that are related to your "interests" (Pin+interests=Pinterest) – users can share and comment on the interests. The Pinterest App-ID was added to the database on March 6th, 2012 and by the end of data collection period (April 30, 2012), Pinterest was found on only 15% of the participating networks – for comparison, Facebook and Twitter are in use on 97% of the participating organizations.

However, Pinterest is consuming 1% of the social networking bandwidth, indicating a fairly heavy amount of use. Much of the excitement around Pinterest is the ability to post photos and images related to the "interest" which may explain the bandwidth consumption.

The next question is whether or not Pinterest is being used for work or for personal purposes within the organizations in this sample. In all likelihood, it is for personal use, given the narrow focus of the solution offering. However, as this Shopify infographic shows, the personal use is not without business benefit; Pinterest is already the third highest shopping referral site behind Facebook and Twitter and the average online order is $80 – double that of Facebook. However the business benefit is to the retailer – not the organization where the user is accessing Pinterest while at work.

Enticement and Trust Bring Elevated Risks

With a captive audience of close to 1 billion users, social networking applications represent a very target rich environment for cybercriminals. If an attack gets a 0.001% return the cybercriminal has just infected 1,000,000 users. One of the most common mechanisms for initiating an attack is to entice a user to click, download or reply to a message. To be clear, enticement to achieve a goal, positive or negative, is not new but social networking has made enticement far easier than ever before. The bait, whether it is a photo of the most recent knitting project on Pinterest, or a link to a gnarly video on Tumblr, is irrelevant. Where trust plays a factor is when the user thinks the update is from a friend, they may be significantly more likely to click on it and in so doing, initiate the next phase of the crime - a background malware download, or a request for account credentials to steal personal information.

As discussed in the streaming video section earlier, one of the latest forms of social networking attack is likejacking where a user "Likes" the criminal's enticement update or post, and in so doing, makes that update available to their friends. There are many other business and security risks associated with social networking – privacy, compliance with internal or government regulations, social engineering – the list goes on. However, many of these risks are initiated through enticement and trust.

Summary: Any Application, Any Port, Any Time.

Online video streaming using P2P on any port; browser-based file sharing hopping ports or using tcp/1723 (PPTP) because it is commonly left open on a firewall. These are just a few examples of how applications have evolved and they add strength to the argument that if you do not have visibility and control over all applications, no matter what port, all the time, then there may be security risks. Port hopping, non-standard ports, using tcp/80 when the traffic is neither web- nor browser-based are all mechanisms to make it easier to use these applications. They are also mechanisms that avoid the traditional port-based firewall, even those which have added application control after the fact. Secure application enablement begins with visibility and control over all applications, on any port, all the time. Armed with that information, security professionals can truly regain control over the applications, users and content traversing the network.

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 1,280 unique applications found across the 2,036 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. ping
4. ssl
5. ntp
6. netbios-ns
7. ms-update
8. linkedin-base
9. icmp
10. flash
11. google-analytics
12. snmp-base
13. ocsp
14. twitter-base
15. soap
16. facebook-base
17. rss
18. google-safebrowsing
19. adobe-update
20. flickr-base
21. facebook-social-plugin
22. smtp
23. webdav
24. http-audio
25. java-update
26. gmail-base
27. http-video
28. sharepoint-base
29. http-proxy
30. youtube-base
31. silverlight
32. google-app-engine
33. ftp
34. rtmpt
35. photobucket
36. hotmail
37. yahoo-mail
38. google-translate-base
39. google-toolbar
40. google-video-base
41. vimeo
42. google-plus-base
43. google-maps
44. ldap
45. facebook-chat
46. apple-update
47. itunes-base
48. stumbleupon
49. google-docs-base
50. ms-ds-smb
51. google-update
52. msn-webmessenger
53. rtmp
54. netbios-dg
55. tumblr-base
56. facebook-posting
57. yahoo-im-base
58. dropbox
59. dailymotion
60. google-translate-manual
61. skype
62. facebook-mail
63. meebo-base
64. google-calendar-base
65. ms-rdp
66. symantec-av-update
67. limelight
68. mobile-me
69. ssh
70. tidaltv
71. t.120
72. facebook-apps (75%)
73. msrpc
74. yahoo-toolbar
75. itunes-appstore
76. twitpic
77. google-picasa
78. babylon
79. ooyala
80. salesforce-base
81. flexnet-installanywhere
82. google-talk-gadget
83. kerberos
84. web-crawler
85. skype-probe
86. office-live
87. asf-streaming
88. netbios-ss
89. teamviewer-base
90. google-talk-base
91. paloalto-updates
92. dhcp
93. pop3
94. myspace-base
95. msn-base
96. google-desktop
97. ms-product-activation
98. zynga-games
99. sip
100. skydrive
101. stun
102. ustream
103. rtmpe
104. google-cache
105. bittorrent
106. snmpv1
107. google-translate-auto
108. dell-update
109. mssql-mon
110. ike
111. google-earth
112. ipsec-esp-udp
113. icloud
114. amazon-cloud-player
115. mail.ru-base
116. 4shared
117. foursquare
118. ms-netlogon
119. syslog
120. active-directory
121. mssql-db
122. teredo
123. linkedin-mail
124. shoutcast
125. rtp
126. mediafire
127. adobe-media-player
128. citrix
129. docstoc
130. logmein
131. boxnet-base
132. telnet
133. ning-base
134. msn-voice
135. hulu-base
136. last.fm
137. clearspace
138. evernote
139. ms-sms
140. rtsp
141. twitter-posting
142. slp
143. rtcp
144. snmp-trap
145. itunes-mediastore
146. aim-express-base
147. vkontakte-base
148. webex-base (50%)
149. megavideo
150. weather-desktop
151. facetime
152. metacafe
153. lpd
154. netflix-base
155. ssdp
156. netlog
157. linkedin-posting
158. filestube
159. time
160. live365
161. aim-mail
162. apple-appstore
163. hp-jetdirect
164. jabber
165. apt-get
166. badoo
167. plaxo
168. sky-player
169. ms-exchange
170. squirrelmail
171. akamai-client
172. yousendit
173. flixster
174. zendesk
175. outlook-web
176. orkut
177. imap
178. napster
179. grooveshark
180. megaupload
181. adobe-flash-socketpolicy-server
182. gmail-enterprise
183. friendfeed
184. yahoo-webmessenger
185. filesonic
186. gotomeeting
187. blog-posting
188. snmpv2
189. yahoo-calendar
190. gmail-chat
191. blogger-blog-posting
192. justin.tv
193. android-market
194. sina-weibo-base
195. scribd-base
196. whatsapp
197. channel4
198. emule
199. blackboard
200. daum
201. myspace-video
202. meetup
203. alisoft
204. livejournal
205. ciscovpn
206. battle.net
207. vnc-base
208. fileserve
209. radius
210. rapidshare
211. ares
212. ms-groove
213. yum
214. eset-update
215. tftp
216. bbc-iplayer
217. odnoklassniki-base
218. upnp
219. brightcove
220. pandora
221. oracle
222. tudou
223. yahoo-voice
224. dotmac
225. apple-push-notifications
226. brighttalk
227. tcp-over-dns
228. lotus-notes-base
229. ipv6
230. shutterfly
231. fotki
232. sharepoint-admin
233. renren-base
234. steam
235. hotfile
236. depositfiles
237. viber-base
238. msn-file-transfer
239. ichat-av
240. quora
241. amazon-instant-video
242. sharepoint-documents
243. portmapper
244. webshots
245. citrix-jedi
246. millenium-ils
247. backweb
248. divshare
249. gre
250. ebuddy
251. good-for-enterprise
252. xunlei
253. cyworld
254. iheartradio
255. live-meeting
256. reuters-data-service
257. playstation-network
258. avira-antivir-update
259. sightspeed
260. paloalto-wildfire-cloud
261. freegate
262. youku
263. zimbra
264. horde
265. coralcdn-user
266. meebome
267. sugarsync
268. sendspace
269. spotify
270. mysql
271. atom
272. mogulus
273. vbulletin-posting
274. yahoo-douga
275. qq-base
276. mixi-base
277. qq-mail
278. aim-base
279. 360-safeguard-update
280. netvmg-traceroute
281. smilebox
282. pptp
283. hyves-base
284. kaspersky
285. netsuite
286. putlocker
287. imesh
288. blackberry
289. twig
290. h.225
291. gnutella
292. irc-base (25%)
293. bet365
294. uploading
295. msn-toolbar
296. xing
297. google-calendar-enterprise
298. xobni
299. me2day
300. pandora-tv

301. adobe-meeting
302. flashget
303. computrace
304. 51.com-base
305. imo
306. imeem
307. esnips
308. concur
309. mail.ru-moimir
310. oovoo
311. trendmicro
312. echo
313. youtube-posting
314. google-docs-enterprise
315. ipsec-esp
316. isatap
317. ppstream
318. qvod
319. open-vpn
320. minecraft
321. teamviewer-sharing
322. tumblr-posting
323. pplive
324. netease-mail
325. trendmicro-officescan
326. dostupest
327. azureus
328. pogo
329. deezer
330. freenet
331. lwapp
332. panda-update
333. h.245
334. roundcube
335. hamachi
336. mediawiki-editing
337. daum-mail
338. live-mesh-base
339. subversion
340. comcast-webmail
341. google-video-enterprise
342. vmware
343. ms-kms
344. sendoid
345. qik-base
346. ebay-desktop
347. kaixin001-base
348. rpc
349. glype-proxy
350. yammer
351. google-music
352. bugzilla
353. phproxy
354. zumodrive
355. stickam
356. capwap
357. funshion
358. activesync
359. friendster
360. logitech-webcam
361. mendeley
362. second-life-base
363. netflow
364. ifolder
365. veohtv
366. badongo
367. mail.ru-agent-base
368. amazon-cloud-drive-uploading
369. qq-download
370. 2ch
371. asus-webstorage
372. myspace-im
373. live-mesh-sync
374. yourminis
375. chrome-remote-desktop
376. netflix-streaming
377. zamzar
378. qqmusic
379. apple-airport
380. yahoo-notepad
381. pando
382. nintendo-wfc
383. ultrasurf
384. norton-av-broadcast
385. live-mesh-remote-desktop
386. webqq
387. easy-share
388. carbonite
389. veetle
390. tor
391. pinterest
392. join-me-base
393. discard
394. socks
395. seesmic
396. gmx-mail
397. itv-player
398. mms
399. wuala
400. instan-t-file-transfer
401. opera-mini
402. google-location-service
403. vnc-encrypted
404. secureserver-mail
405. sharepoint-calendar
406. flumotion
407. pcanywhere
408. stagevu
409. nimbuzz
410. imvu
411. mcafee-update
412. worldofwarcraft
413. rsync
414. battlefield2
415. corba
416. jaspersoft
417. megashares
418. ifile.it
419. mail.ru-webagent
420. niconico-douga
421. ning-posting
422. qq-file-transfer
423. daytime
424. websense
425. web-de-mail
426. hotspot-shield
427. ms-lync-base
428. amazon-unbox
429. renren-chat
430. kakaotalk
431. whois
432. l2tp
433. jira
434. icq
435. wetransfer
436. sina-webuc
437. rip
438. fring
439. evony
440. kazaa
441. netload
442. kugoo
443. send-to-phone
444. garena
445. youtube-safety-mode
446. yahoo-file-transfer
447. ali-wangwang-base
448. google-wave
449. nfs
450. union-procedure-call
451. qq-games
452. source-engine
453. ipp
454. sybase
455. sakai
456. pp-accelerator
457. cgiproxy
458. qqlive
459. gotomypc-base
460. yoono
461. rsvp
462. tvu
463. baofeng
464. dcinside-base
465. bomgar
466. ning-apps
467. sap
468. naver-line
469. renren-music
470. microsoft-dynamics-crm
471. cygnet-scada
472. teachertube
473. youtube-uploading
474. tacacs-plus
475. ntr-support
476. sccp
477. mibbit
478. vnc-clipboard
479. nntp
480. cisco-nac
481. 1und1-mail
482. yandex-mail
483. naver-mail
484. wolfenstein
485. afp
486. ms-lync-video
487. files.to
488. vkontakte-chat
489. chatroulette
490. octoshape
491. mozy
492. gtalk-voice
493. bebo-base
494. qq-audio-video
495. xdmcp
496. runescape
497. rhapsody
498. sopcast
499. gadu-gadu
500. slacker
501. bloomberg-professional
502. league-of-legends
503. hi5
504. endnote
505. git
506. rpc-over-http
507. elluminate
508. snmpv3
509. mail.ru-mail
510. studivz
511. viadeo
512. dcc-antispam
513. flexnet-publisher
514. hangame
515. lineage
516. socialtv
517. vidyo
518. tales-runner
519. xbox-live
520. origin
521. rping
522. msnshell
523. myspace-mail
524. direct-connect
525. netviewer
526. renren-posting
527. open-webmail
528. cloudmark-desktop
529. crashplan
530. adrive
531. yahoo-webcam
532. xunlei-kankan
533. ameba-now-base
534. transferbigfiles
535. all-slots-casino
536. editgrid
537. tikiwiki-editing
538. zango
539. fetion-base
540. fastmail
541. freeetv
542. postgres
543. att-connect
544. magicjack
545. mount
546. daum-cafe-posting
547. nate-mail
548. ospf
549. vsee
550. inforeach
551. clip2net
552. 51.com-games
553. regnum
554. ms-win-dns
555. sina-weibo-posting
556. panos-web-interface
557. ms-scom
558. dameware-mini-remote
559. apple-location-service
560. vmware-view
561. backup-exec
562. svtplay
563. amazon-cloud-drive-base
564. ku6
565. mixi-posting
566. uusee
567. ms-lync-audio
568. dl-free
569. t-online-mail
570. cox-webmail
571. genesys-base
572. lotus-sametime
573. wins
574. megashare
575. baidu-webmessenger
576. nateon-im-base
577. kkbox
578. finger
579. yy-voice-base
580. renren-apps
581. wikispaces-editing
582. taku-file-bin
583. sling
584. tonghuashun
585. popo-im
586. filemaker-pro
587. boxnet-editing
588. naver-ndrive
589. gtalk-file-transfer
590. livelink
591. simplite-msn
592. tivoli-storage-manager
593. altiris
594. gmail-call-phone
595. unassigned-ip-prot
596. flickr-uploading
597. vtunnel
598. warcraft
599. gamespy
600. ms-lync-apps-sharing
601. tudou-speedup
602. spideroak
603. yantra
604. iloveim
605. gogobox
606. paran-mail
607. neonet
608. starcraft
609. checkpoint-cpmi
610. pcoip
611. mydownloader
612. poker-stars
613. tv4play
614. camfrog
615. renren-mail
616. db2
617. fogbugz
618. informix
619. filedropper
620. plugoo-widget
621. scps
622. afreeca
623. x11
624. cvs
625. zoho-sheet
626. igmp
627. miro
628. vnc-http
629. radmin
630. odnoklassniki-apps
631. classmates
632. mgoon
633. manolito
634. ip-messenger-base
635. ncp
636. hopopt
637. linkedin-apps
638. ndmp
639. ea-fifa
640. viber-voice
641. zoho-im
642. ibm-bigfix
643. aol-proxy
644. ironmountain-connected
645. paltalk-base
646. voddler
647. lokalisten
648. streamaudio
649. ezpeer
650. ip-in-ip
651. cups
652. kontiki
653. clubbox
654. palringo
655. hopster
656. odnoklassniki-messaging
657. fuze-meeting-base
658. ameba-blog-posting
659. ammyy-admin
660. orb

661. sbs-netv
662. myspace-posting
663. twtkr
664. boxnet-uploading
665. emc-documentum-webtop
666. earthcam
667. fs2you
668. spark
669. diino
670. feidian
671. dazhihui
672. userplane
673. folding-at-home
674. lotuslive-base
675. paradise-paintball
676. h.323
677. leapfile
678. webex-weboffice
679. eigrp
680. trendmicro-safesync
681. air-video
682. yourfilehost
683. aim-file-transfer
684. hyves-chat
685. readytalk-base
686. draugiem
687. optimum-webmail
688. ibm-websphere-mq
689. mgcp
690. razor
691. isl-light
692. netop-remote-control
693. ilohamail
694. wiiconnect24
695. mcafee-epo-admin
696. acronis-snapdeploy
697. sflow
698. fotoweb
699. gotomypc-printing
700. spark-im
701. zabbix
702. naver-blog-posting
703. call-of-duty
704. zoho-wiki
705. forticlient-update
706. renren-im
707. rsh
708. scribd-uploading
709. neptune
710. google-buzz
711. ms-visual-studio-tfs
712. cpq-wbem
713. sohu-video
714. salesforce-chatter
715. chinaren-base
716. netmeeting
717. groupwise
718. steekr
719. ms-dtc
720. zoho-writer
721. kaixin001-mail
722. mekusharim
723. fc2-blog-posting
724. gds-db
725. innovative
726. hyves-games
727. fortiguard-webfilter
728. ms-ocs
729. symantec-syst-center
730. meinvz
731. ning-mail
732. eve-online
733. yy-voice-games
734. ms-iis
735. ibm-director
736. bacnet
737. filemail
738. qdown
739. autobahn
740. korea-webmail
741. youseemore
742. sina-uc-base
743. ali-wangwang-file-transfer
744. 100bao
745. showmypc
746. rlogin
747. ibackup
748. avaya-phone-ping
749. projectplace
750. xm-radio
751. soribada
752. chinaren-chat
753. winamax
754. aruba-papi
755. nate-video
756. pim
757. mediamax
758. xfire
759. foxy
760. libero-video
761. bebo-posting
762. emc-networker
763. hyves-mail
764. iccp
765. ventrilo
766. webhard
767. ms-isa-fw-client
768. etherip
769. clarizen
770. paltalk-express
771. dealio-toolbar
772. telenet-webmail
773. saba-centra-meeting
774. meabox
775. kproxy
776. rdmplus
777. drivehq
778. 2ch-posting
779. tagoo
780. party-poker
781. pullbbang-video
782. sosbackup
783. yahoo-finance-posting
784. soulseek
785. thinkfree
786. yahoo-blog-posting
787. usermin
788. maplestory
789. bomberclone
790. ms-wins
791. talkbox
792. hp-data-protector
793. gotomypc-file-transfer
794. mail.ru-games
795. ariel
796. babelgum
797. livestation
798. packetix-vpn
799. im-plus
800. cgi-irc
801. big-brother
802. remoteview
803. asterisk-iax
804. nateon-file-transfer
805. mercurial
806. zoho-show
807. crossloop
808. iscsi
809. unreal
810. rift
811. webconnect
812. tvb-video
813. chikka-messenger
814. zelune
815. woome
816. cddb
817. ameba-now-posting
818. storage.to
819. messengerfx
820. ms-ocs-file-transfer
821. mikogo
822. wccp
823. nateon-desktop-sharing
824. apc-powerchute
825. drda
826. fetion-file-transfer
827. magister
828. adnstream
829. daum-blog-posting
830. reserved
831. lotuslive-meeting
832. daum-touch
833. yuuguu
834. siebel-crm
835. shavlik-netchk
836. phonemypc
837. synergy
838. second-life-voice-chat
839. vagaa
840. ypserv
841. trinoo
842. sip-application
843. icq2go
844. diodeo
845. gmail-video-chat
846. gbridge
847. ipsec-ah
848. your-freedom
849. remotecall
850. okurin
851. mobility-xe
852. turboupload
853. hl7
854. writeboard
855. netfolder
856. pna
857. igp
858. winamp-remote
859. zoho-crm
860. sharepoint-blog-posting
861. factset
862. paltalk-superim
863. iso-ip
864. rypple
865. zenbe
866. gigaup
867. pownce
868. zoho-mail
869. eroom-host
870. icap
871. exp
872. nateon-audio-video
873. lotus-notes-admin
874. fasp
875. perfect-dark
876. ovation
877. ibm-clearcase
878. riverbed-rios
879. misslee
880. sophos-update
881. kace
882. esignal
883. jap
884. qik-video-chatting
885. digg-posting
886. totodisk
887. dhcpv6
888. avaya-webalive-base
889. sctp
890. cvsup
891. verizon-wsync
892. drop.io
893. doof
894. arcserve
895. ipv6-icmp
896. adobe-online-office
897. letv
898. keyholetv
899. daap
900. steganos-vpn
901. bigupload
902. trunk-2
903. chinaren-apps
904. fetion-audio-video
905. wikidot-editing
906. noteworthy-base
907. batchbook
908. sugar-crm
909. winny
910. imeet-base
911. vnc-filetransfer
912. egp
913. i2p
914. nakido-flag
915. yahoo-box
916. irc-dcc-file-transfer
917. condor
918. dnp3
919. glide
920. x-font-server
921. cooltalk
922. tistory-blog-posting
923. hyves-music
924. cyberghost-vpn
925. laconica
926. baidu-hi-base
927. lan
928. rusers
929. asproxy
930. yoics
931. distcc
932. koolim
933. beamyourscreen
934. zoho-meeting
935. modbus-read-holding-registers
936. rdt
937. camo-proxy
938. tor2web
939. splashtop-remote
940. idrp
941. secure-access
942. mail.ru-agent-file-transfer
943. perforce
944. argus
945. ms-scheduler
946. idpr-cmtp
947. tokbox
948. filemaker-anouncement
949. callpilot
950. frozenway
951. sina-uc-file-transfer
952. iperf
953. hovrs
954. yugma
955. pup
956. emcon
957. rstatd
958. ibm-clearquest
959. modbus-base
960. move-networks
961. megaproxy
962. dcinside-posting
963. rabbitmq
964. nvp-ii
965. chaos
966. 51.com-bbs
967. swipe
968. baidu-hi-file-transfer
969. war-rock
970. as2
971. vrrp
972. rvd
973. nsfnet-igp
974. mobile
975. bbn-rcc-mon
976. google-docs-uploading
977. wordfast
978. http-tunnel
979. bgp
980. vidsoft
981. egloos-blog-posting
982. bebo-mail
983. seven-email
984. gridftp
985. buddybuddy-base
986. xnet
987. ipcomp
988. host
989. bna
990. 3pc
991. firstclass
992. netvault-backup
993. realtunnel
994. baidu-hi-games
995. ms-frs
996. caihong
997. wsn
998. tlsp
999. sun-nd
1000. srp
1001. private-enc
1002. leaf-1
1003. fire
1004. msn-video
1005. apache-jserv
1006. xns-idp
1007. udplite
1008. trunk-1
1009. sscopmce
1010. prm
1011. netblt
1012. mtp
1013. merit-inp
1014. ipv6-nonxt
1015. dgp
1016. cftp
1017. cbt
1018. estos-procall
1019. zoho-notebook
1020. proxeasy

1021. mcafee
1022. officehard
1023. chinaren-mail
1024. tunnelbear
1025. firephoenix
1026. secure-access-sync
1027. turboshare
1028. qianlong
1029. swapper
1030. doshow
1031. rediffbol-audio-video
1032. netop-on-demand
1033. timbuktu
1034. wb-expak
1035. vmtp
1036. sps
1037. smp
1038. sm
1039. skip
1040. ptp
1041. leaf-2
1042. ipv6-opts
1043. ippc
1044. ipip
1045. il
1046. ggp
1047. dcn-meas
1048. dccp
1049. cpnx
1050. sdrp
1051. emc-smartpackets
1052. wetpaint-editing
1053. motleyfool-posting
1054. hulu-posting
1055. seeqpod
1056. sharebase.to
1057. ip-messenger-file-transfer
1058. peerguardian
1059. paran-u2
1060. gomeetnow
1061. spotnet
1062. xtp
1063. wb-mon
1064. visa
1065. uti
1066. st
1067. sprite-rpc
1068. sat-mon
1069. reliable-data
1070. pnni
1071. pipe
1072. pgm
1073. mfe-nsp
1074. larp
1075. iplt
1076. iatp
1077. gmtp
1078. encap
1079. crudp
1080. compaq-peer
1081. netbotz
1082. thwapr-base
1083. suresome
1084. telex
1085. adobe-meeting-remote-control
1086. sharepoint-wiki
1087. remobo
1088. eatlime
1089. woofiles
1090. subspace
1091. tradestation
1092. radiusim
1093. vyew
1094. fuze-meeting-desktop-sharing
1095. snp
1096. secure-vmtp
1097. pvp
1098. narp
1099. mux
1100. mpls-in-ip
1101. kryptolan
1102. iso-tp4
1103. ipx-in-ip
1104. ipv6-route
1105. ipv6-frag
1106. ipcv
1107. i-nlsp
1108. ifmp
1109. hmp
1110. dfs
1111. ddx
1112. ddp
1113. crtp
1114. cphb
1115. br-sat-mon
1116. aris
1117. activenet
1118. wlccp
1119. modbus-read-input-registers
1120. flixwagon-base
1121. echoware
1122. idpr
1123. ad-selfservice
1124. vkontakte-mail
1125. fluxiom
1126. file-host
1127. knight-online
1128. infront
1129. imhaha
1130. webex-connect
1131. eroom-net
1132. ttp
1133. tcf
1134. sat-expak
1135. qnx
1136. mobilehdr
1137. fibre-channel
1138. track-it
1139. surrogafier
1140. gnu-httptunnel
1141. techinline
1142. isis
1143. dsr
1144. watchdox
1145. 51.com-webdisk
1146. fufox
1147. homepipe
1148. filecatalyst-direct
1149. dynamicintranet
1150. propalms
1151. dnscrypt
1152. vines
1153. stp
1154. irtp
1155. noteworthy-admin
1156. spirent
1157. modbus-write-multiple-registers
1158. modbus-read-coils
1159. bluecoat-auth-agent
1160. maxdb
1161. mail.com
1162. aim-express-file-transfer
1163. meebo-file-transfer
1164. ms-lync-file-transfer
1165. fileguri
1166. blokus
1167. oracle-bi
1168. usejump
1169. swyx-cds
1170. google-docs-editing
1171. gyao
1172. deskshare
1173. jumpdesktop
1174. fastviewer
1175. ms-ocs-audio
1176. ms-ocs-video
1177. paloalto-userid-agent
1178. tacacs
1179. hushmail
1180. tinyvpn
1181. filer.cx
1182. hitachi-spc
1183. dimdim
1184. rwho
1185. Nagios
1186. bosch-rcp-plus
1187. zoho-planner
1188. meeting-maker
1189. fly-proxy
1190. pingfu
1191. r-exec
1192. avamar
1193. socialtext-editing
1194. security-kiss
1195. oracle-crm-ondemand
1196. ants-p2p
1197. winmx
1198. we-dancing-online
1199. quake
1200. jnet
1201. amqp
1202. ms-virtualserver
1203. modbus-read-file-record
1204. meevee
1205. peercast
1206. tvants
1207. blin
1208. desktoptwo
1209. aim-audio
1210. tvtonic
1211. dabbledb
1212. vnn
1213. lawson-m3
1214. foldershare
1215. bonpoo
1216. wixi
1217. gnunet
1218. stealthnet
1219. share-p2p
1220. carefx
1221. stockstar
1222. compass
1223. oracle-ipm
1224. evalesco-sysorb
1225. jxta
1226. msn2go
1227. instan-t-base
1228. avaya-webalive-desktop-sharing
1229. gatherplace-base
1230. iec-60870-5-104
1231. ossec
1232. modbus-write-single-register
1233. zoho-share
1234. kino
1235. graboid-video
1236. cisco-drp
1237. kaixin-base
1238. eyejot
1239. lifecam
1240. nefsis
1241. moinmoin-editing
1242. google-finance-posting
1243. wallcooler-vpn
1244. gtunnel
1245. centriccrm
1246. adobe-meeting-file-transfer
1247. little-fighter
1248. fix
1249. clickview
1250. bluecoat-adn
1251. instan-t-webmessenger
1252. airaim
1253. medium-im
1254. webex-chat
1255. meetro
1256. rediffbol-base
1257. netspoke
1258. adobe-connectnow-base
1259. webex-desktop-sharing
1260. oridus-nettouch
1261. gkrellm
1262. siemens-factorylink
1263. modbus-write-single-coil
1264. modbus-write-multiple-coils
1265. modbus-read-discrete-inputs
1266. qik-uploading
1267. joost
1268. circumventor
1269. guardster
1270. beinsync
1271. pcvisit
1272. sina-uc-remote-control
1273. tuenti
1274. trendmicro-earthagent
1275. access-grid
1276. ali-wangwang-audio-video
1277. gizmo
1278. ragingbull-posting
1279. aol-messageboard-posting