The Application Usage and Threat Report

An Analysis of Application Usage and Related Threats – Regional Findings

- *Americas and Canada (Latin and South America, Canada, U.S.A.)*
- *Europe, Africa, Middle East*
- *Asia Pacific*
- *Japan*

March 2013

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

Table of Contents

Executive Summary

Since 2008, Palo Alto Networks has published trends and analysis in application usage across enterprise networks in its bi-annual *Application Usage and Risk Report*. This version of the report marks an evolution of sorts – it now includes threat activity, specifically malware and exploits, across the applications observed and therefore, the name of the report has been changed.

The *Application Usage and Threat Report (10th Edition, January 2013)* from Palo Alto Networks provides a global view into enterprise application usage and the associated threats by summarizing network traffic assessments conducted in 3,056 organizations worldwide between May 2012 and December 2012. This report edition will be the first report of its kind to discuss application usage patterns and the specific type of threat they may or may not introduce. The application and threat patterns discussed within this report dispel the position that social networking, filesharing and video applications are the most common threat vectors, while reaffirming that internal applications are highly prized targets. Rather than use more obvious, commercially available applications, attackers are masking their activities through custom or encrypted applications.

A summary of the global and regional findings are outlined below. To view additional details and interactively browse the global and regional findings, visit www.paloaltonetworks.com/autr.

Key global findings include:

Applications commonly viewed as top threat sources are, in fact, not.

- 339 social networking, video, and filesharing applications represent 20% of the bandwidth but displayed only 0.4% of the threat logs.
- Exploits observed in Facebook applications (3rd party applications and widgets) were 228 times greater in number than in other social networking applications.

Exploits continue to target enterprises' most valued assets.

- Out of 1,395 applications found, 10 were responsible for 97% of all exploit logs observed.
- Of the 10 applications, 9 are internal applications and they represented 82% of the exploit logs.

Malware relies heavily on custom applications.

- Custom or unknown traffic was the #1 type of traffic associated with malware communications, as leading malware families continue to customize their command-and-control traffic.
- Control of unknown and custom traffic provided an intriguing option for controlling botnet communications.

The use of SSL – both a security mechanism and a masking agent.

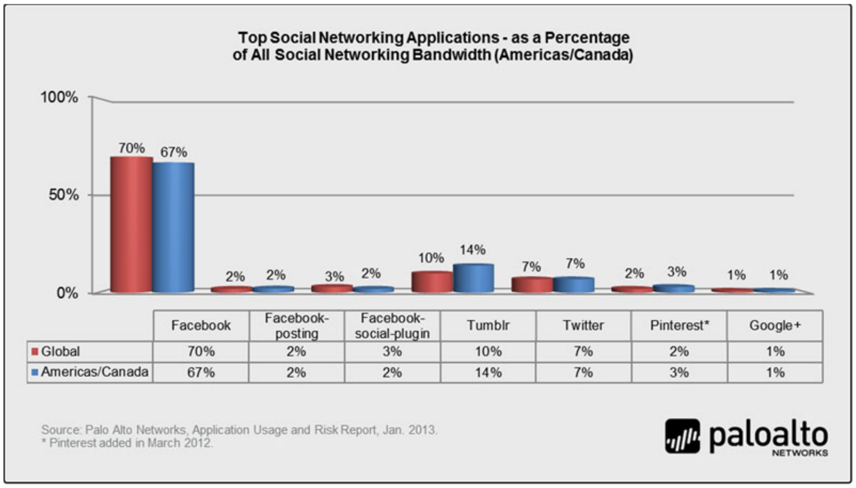
- 356 applications used SSL in some way, shape or form - 85 of them did not use standard SSL ports.
- SSL by itself represented 5% of all bandwidth and the sixth highest volume of malware logs within known applications.
- HTTP proxy, used both as a security component and to evade controls, exhibited the seventh highest volume of malware logs.

The analysis and related findings in this report are generated via live network traffic observed in several thousand organizations worldwide. In that respect the report is unique in that it is not based on a survey – it is real data collected from live traffic. The threat logs analyzed and discussed within the report are broken out into vulnerability exploits (e.g., SQL injection, overflow and code execution) and malware (e.g., botnets, spyware and keyloggers).

Key Findings: The Americas and Canada

The Americas and Canada dataset represents more 1,124 organizations distributed across 11 countries with USA, Brazil and Canada (in order) representing 84% of the participating organizations. A total of 1,316 applications were detected along with 1,700 unique threats that had generated 164 million threat logs.

Common sharing applications are pervasive, but they display a lower than expected percentage of overall threats when compared to the other categories. Social networking, filesharing and photo-video applications collectively represent 24% of the applications (319), 23% of the bandwidth yet only 0.2% of the threat logs. This is not to say these applications are low risk – the data shows that a greater percentage of the threats (exploits and malware) were found in other applications. Facebook continues to dominate the social networking landscape – four Facebook functions (Facebook-base, -apps, -posting, and social-plugins) consume 71% of all social networking bandwidth - leaving only 29% of the bandwidth for the other 69 variants found.


Top Social Networking Applications - as a Percentage of All Social Networking Bandwidth (Americas/Canada)

	Facebook	Facebook-posting	Facebook-social-plugin	Tumblr	Twitter	Pinterest*	Google+
🟥 Global	70%	2%	3%	10%	7%	2%	1%
🟦 Americas/Canada	67%	2%	2%	14%	7%	3%	1%

Source: Palo Alto Networks, Application Usage and Risk Report, Jan. 2013.
* Pinterest added in March 2012.

Figure 1: Top social networking applications, as a percentage of total social networking bandwidth.

Tumblr in the Americas/Canada had higher bandwidth consumption than all other geographic regions while Google + was used found in 91% of the participating 1,124 organizations (Americas/Canada). Google + posting was found in only 1 organization. Myspace continues to survive - found in 74% of the organizations; Myspace posting was highest byte/session at 2.6MB (Facebook positing only 111KB).

Filesharing usage diversifies somewhat but BitTorrent and FTP still consume the most bandwidth. There were 137 different filesharing applications found with an average of 22 found on 99% of the 1,124 networks analyzed (6 client/server, 11 browser-based, 5 P2P). Within the 137 filesharing applications, the bulk of the threat logs, primarily exploits were targeted at FTP and WebDAV.

Despite control efforts, BitTorrent continues to be used heavily, both in terms of frequency of use (68%) and volume of use (3% of TOTAL bandwidth). It is much like a weed that continues to return, despite repeated control efforts. It raises the question of whether or not it can ever be controlled.

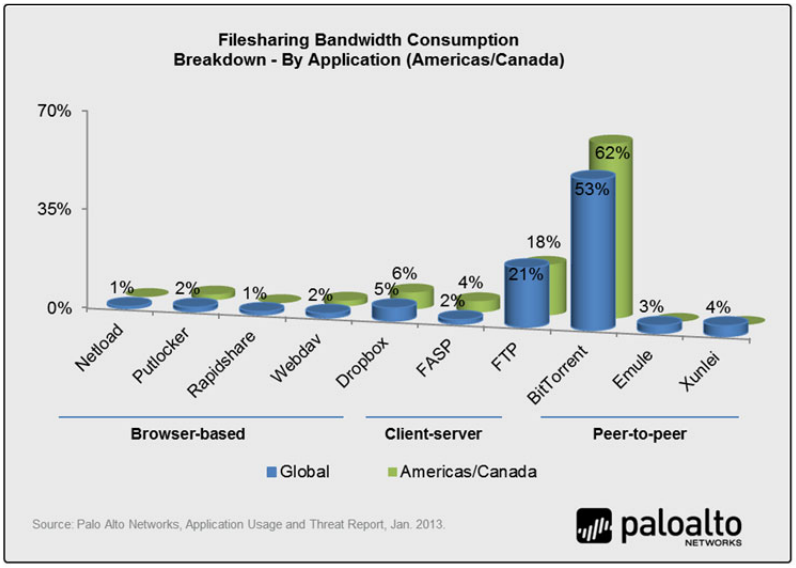


Figure 2: Top 10 filesharing applications based on total filesharing category bandwidth consumption.

What is the business value of 21 photo-video applications per network? The use of video for business purposes is known and proven; it's used for marketing promotions, lead generation, product announcements, training, and education to name just a few examples. For business purposes, the most common applications are YouTube and HTTP video, and perhaps Vimeo. On average, in the Americas/Canada, there were 21 photo-video applications found and they were consuming 16% of total bandwidth, which raises the question – what is the business use case variants such as Netflix streaming and Hulu Networks on a corporate network? The volume of threat logs observed within photo-video is relatively low.

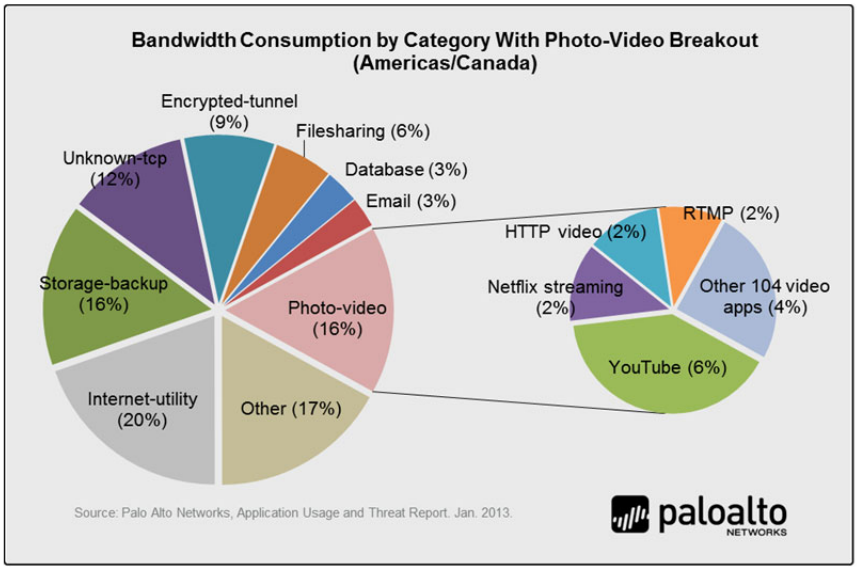
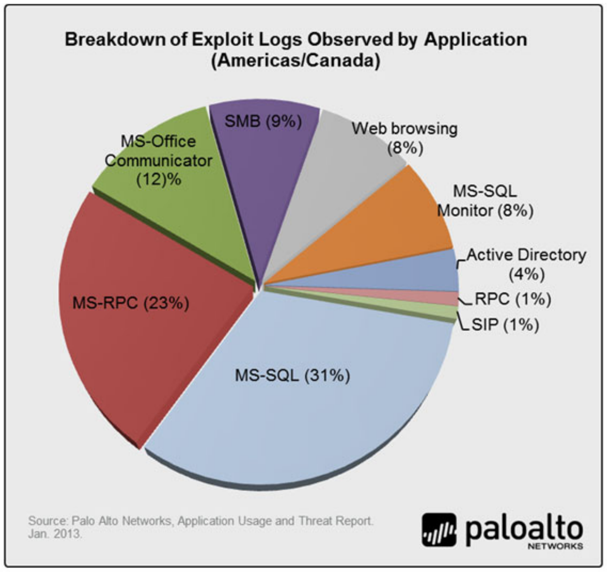


Figure 3: Top photo-video applications, based on bandwidth consumption.

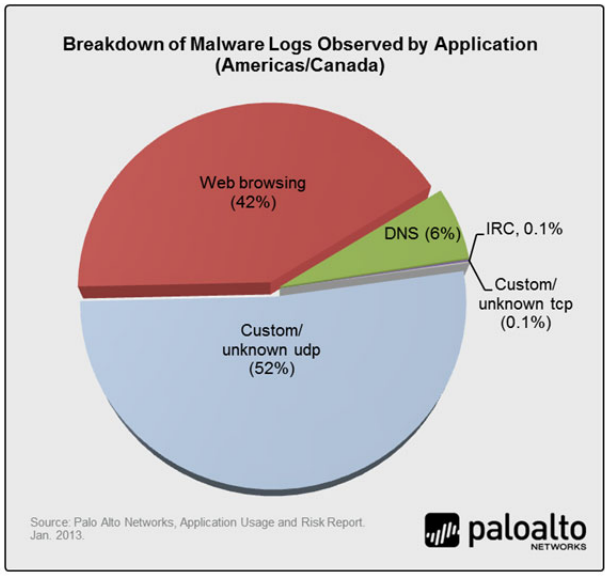
Application vulnerability exploits target high-value business applications. The data shows that exploits such as those that are identified and blocked by an IPS are targeting internal, high-value business applications. Of the 1,317 applications, 9 of them represent 97% of the exploit logs observed – the volume of malware (botnets, spyware, keyloggers) within this set of applications was negligible.



Source: Palo Alto Networks, Application Usage and Threat Report. Jan. 2013.

Figure 4: Applications with the highest concentration of exploit logs.

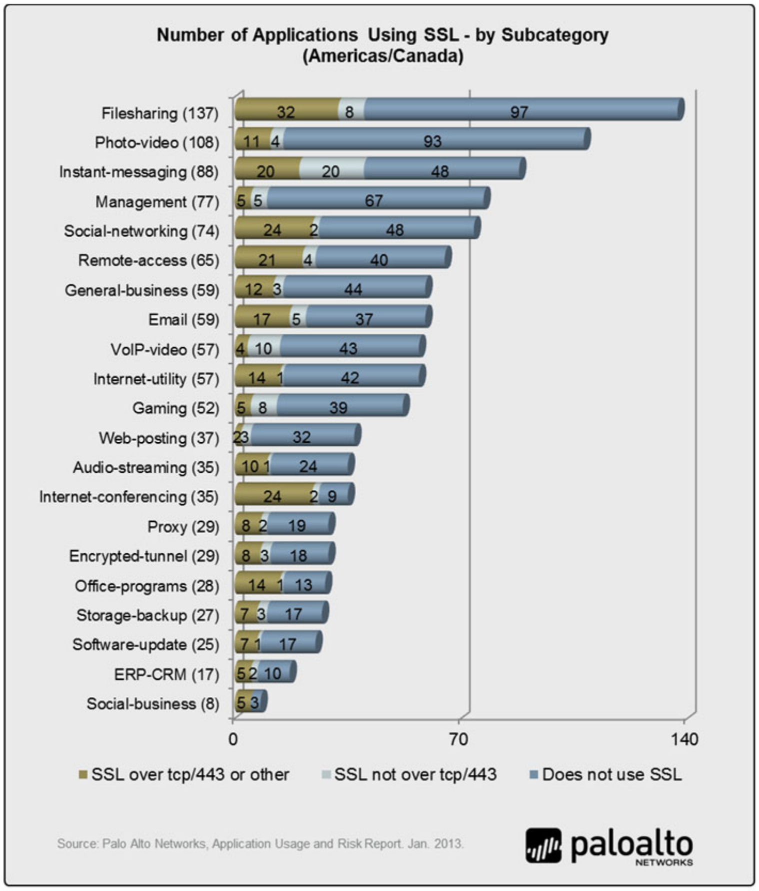
Malware is adept at hiding in unknown and custom application traffic. Nearly 100% of the malware logs (botnets, spyware, keyloggers, etc.) were found in only 5 applications – with the bulk of the logs masking themselves as custom or unknown UDP. UDP traffic, like DNS, is stateless in nature and exhibits a high session count with a small number of bytes per session. Unknown traffic exists on every network in a small amount – yet it will represent a significant volume of risk – making it a perfect example of the 80%-20% rule – a high volume of risk comes from a small volume of traffic.



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 5: Applications with the highest concentration of malware logs.

343 applications can use SSL – is a security feature also masking malicious activity? 26% of the 1,317 applications found (343) use SSL in some way shape or form; 88of the 340 applications that use SSL, never use port 443, nor do they use SSL defined ports (39 hop ports, 35 use port 80, 9 use a range of non-standard ports). A more interesting view is the fact that of the 343 apps that do in fact use tcp/443 (HTTPs), 109of them (47%) are client server. The question that the use of SSL in such a wide range of applications is this – how many of them might be masking criminal activity and what is the best way to balance security and network protection via decryption?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 6: Category breakdown of applications that are capable of using SSL.

Data Sources and Additional Facts: The Americas and Canada

A summary of the data sources, statistics and key facts observed in the Americas and Canada are listed below.

- A total of 1,317 applications consumed more than 5.2 petabytes (5,284,807,275,813,190 bytes) of bandwidth across 1,124 participating organizations.

- Bandwidth consumption is roughly equivalent to 1.7 million 2 hour HD movie downloads (average download size of 3GB).

- Roughly 1,700 unique critical, high and medium severity threats representing more than 164 million logs were observed.

	Threat Logs Viewed – by Severity			
Threat Type	**Critical**	**High**	**Medium**	**Total**
Malware: spyware	987,382	7,078	49,009,937	50,004,397
Malware: net-worm	68,273			68,273
Malware: keylogger		13		13
Malware: botnet	60,261,070	13,826,568	1,879	74,089,517
Malware: backdoor	25,188	2,637,301	177,254	2,839,743
Malware: adware	4,026,111	10,162	14,613	4,050,886
Malware: total logs	65,368,024	16,481,122	49,203,683	131,052,829
Exploit: sql-injection		1,160	245,686	246,846
Exploit: overflow	954,018	4,840,881	10,061,625	15,856,524
Exploit: code-execution	4,118,788	9,433,228	3,776,463	17,328,479
Exploit: total logs	5,072,806	14,275,269	14,083,774	33,431,849
Grand Total	**70,440,830**	**30,756,391**	**63,287,457**	**164,484,678**

- Collectively, social networking, filesharing and photo-video applications represented 24% of the applications (319) and 23% of total bandwidth (~408,000 2hr high-definition movie downloads), but only 0.2% of all threat logs observed.

- The number of application variants found in each category: social networking (74), filesharing (137) and photo-video (108).

- Each network analyzed had an average of 15 social networking, 20 filesharing, and 21 photo-video application variants.

- Of the 74 social networking applications found, the four Facebook functions (-base, -apps, -social-plugins, -posting) represent 71% of all social networking bandwidth; Tumblr usage in the Americas and Canada was higher than all the other regions at 14% of social networking bandwidth.

- Google + used most heavily in the Americas/Canada; 91% of the 1,124 organizations – Google + posting found in only 1 organization.

- Myspace continues to survive - found in 74% of the organizations; Myspace posting was highest byte/session at 2.6MB (Facebook positing only 111KB).

- The 137 filesharing applications found consume a 6% of the bandwidth observed with BitTorrent and FTP representing 3% and 1% respectively.

- The top 10 filesharing applications represent 92% of the respective bandwidth; 81% of the respective threat logs observed, and they are distributed across the all three technologies (3 P2P, 3 client/server, 4 browser-based); FTP displayed the highest number of filesharing threat logs (primarily exploits).

- 97% of all exploit logs were found in ten applications; nine of the applications are internal/infrastructure applications (databases, Active Directory, RPC, etc.).

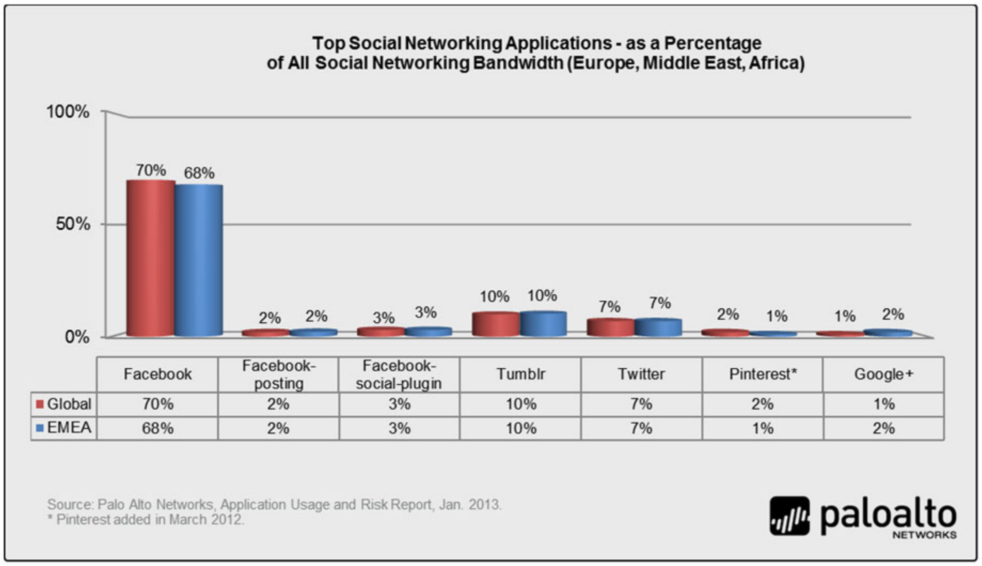
- 99.99% of all malware logs were found in only five (out of 1,317) applications with custom/unknown-UDP representing the highest volume at 52%.

- 26% of the 1,317 applications found (334) use SSL in some way shape or form; 83 of them never use port 443, nor do they use SSL defined ports (39 hop ports, 35 use port 80, 9 use a range of non-standard ports).

Key Findings: Europe, Middle East and Africa

The European, Middle east and Africa dataset represents more 859 organizations distributed across 39 countries with 78% of the participating organizations coming (in order) UK, Germany, France, Spain, Netherlands, Italy, Norway, Russia, Denmark and Belgium.. A total of 1,304 applications were detected along with 1,300 unique threats that had generated 54 million threat logs.

Common sharing applications are pervasive, but they display a lower than expected percentage of overall threats when compared to the other categories. Social networking, filesharing and photo-video applications collectively represent 25% of the applications (320), 16% of the bandwidth yet only 0.2% of the threat logs. The low threat log count should not be misinterpreted as a low risk statement. The volume observed is relative to the other applications found during the analysis. Facebook continues to dominate the social networking landscape – four Facebook functions (Facebook-base, -apps, -posting, and social-plugins) consumes 73% of all social networking bandwidth - leaving only 27% of the bandwidth for the other 70 variants found.



Top Social Networking Applications - as a Percentage of All Social Networking Bandwidth (Europe, Middle East, Africa)

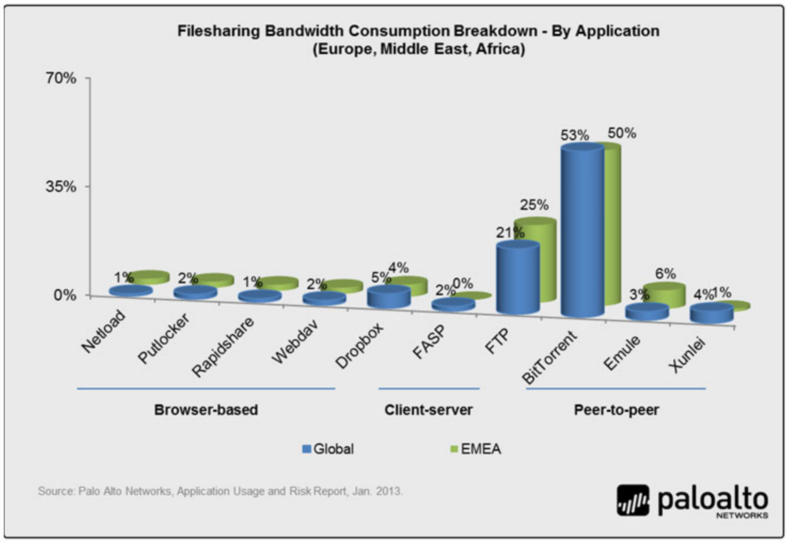
	Facebook	Facebook-posting	Facebook-social-plugin	Tumblr	Twitter	Pinterest*	Google+
🟥 Global	70%	2%	3%	10%	7%	2%	1%
🟦 EMEA	68%	2%	3%	10%	7%	1%	2%

Source: Palo Alto Networks, Application Usage and Risk Report, Jan. 2013.
* Pinterest added in March 2012.

Figure 7: Top social networking application bandwidth consumption, as a percentage of social networking bandwidth observed.

Usage of Tumblr and Pinterest mimics the global use while Google + was found in 89% of the organizations but very few users are posting; Google + posting found in only 3 organizations (out of 859). Myspace continues to be found in 65% of the organizations; Myspace posting had the highest bytes/session within social networking.

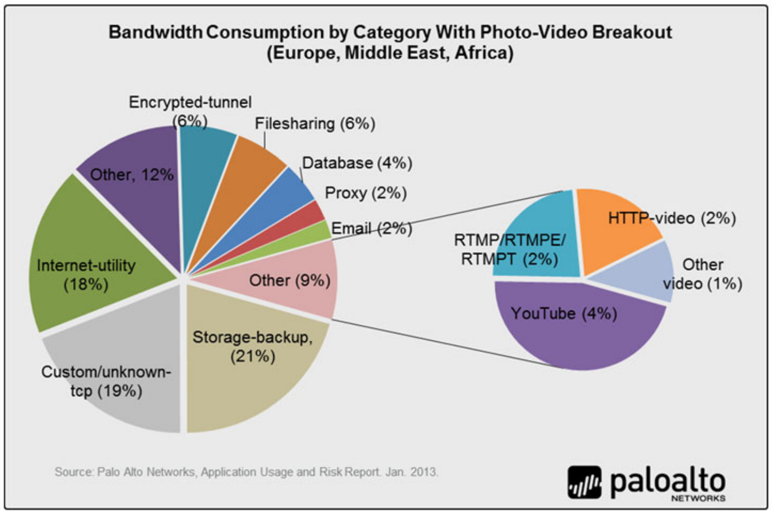
Filesharing usage diversifies somewhat but BitTorrent and FTP still consume the most bandwidth. Not surprisingly, filesharing use in Europe, Middle East and Africa mimic the patterns seen globally. There were 142 different filesharing applications found with an average of 21 found on 97% of the 859 networks analyzed (5 client/server, 11 browser-based, 5 P2P). Within the 142 filesharing applications, the bulk of the threats and related logs were targeted at FTP and WebDAV. Despite control efforts, BitTorrent continues to be used heavily, both in terms of frequency of use (63%) and volume of use (3% of TOTAL bandwidth). It is much like a weed that continues to return, despite repeated control efforts. It raises the question of whether or not it can ever be controlled.



Source: Palo Alto Networks, Application Usage and Risk Report, Jan. 2013.

Figure 8: Top 10 filesharing applications based on total filesharing category bandwidth consumption.

What is the business value of 22 photo-video applications per network? The use of video for business purposes is known and proven; it's used for marketing promotions, lead generation, product announcements, training, and education to name just a few examples. For business purposes, the most common applications are YouTube and HTTP video, and perhaps Vimeo. On average, there were 22 photo-video applications found and they were consuming 16% of total bandwidth, which raises the question – what is the business use case of so many variants?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 9: Top photo-video applications, based on bandwidth consumption.

Application vulnerability exploits target high-value business applications. The data shows that exploits such as those that are identified and blocked by an IPS are targeting internal, high-value business applications. Of the 1,304 applications, 10 of them represent 97% of the exploit logs observed and of those, 9 are considered business critical.

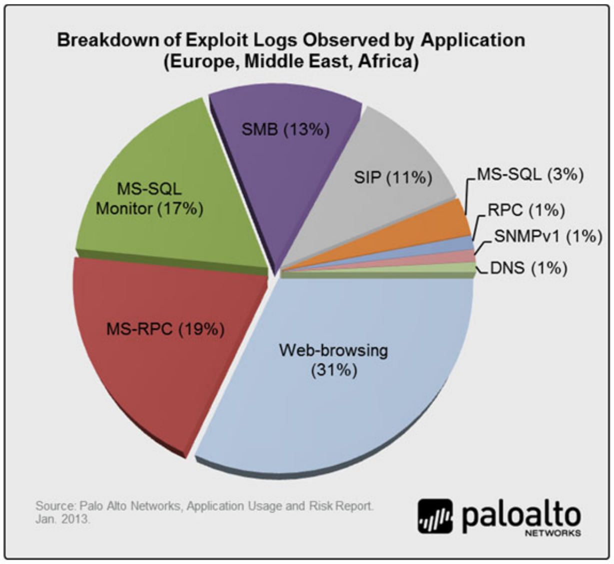


Figure 10: Applications with the highest concentration of exploit logs.

Malware is adept at hiding in unknown and custom application traffic. Nearly 100% of the malware logs (botnets, spyware, keyloggers, etc.) were found in only 5 applications – with the bulk of the logs (74%) masking themselves as custom or unknown UDP. UDP traffic, like DNS, is stateless in nature and exhibits a high session count with a small number of bytes per session. Unknown traffic exists on every network in a small amount – yet it will represent a significant volume of risk – making it a perfect example of the 80%-20% rule – a high volume of risk comes from a small volume of traffic.

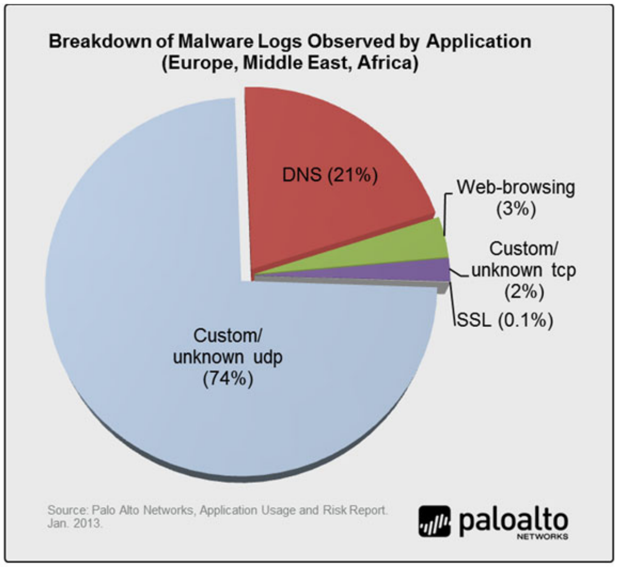
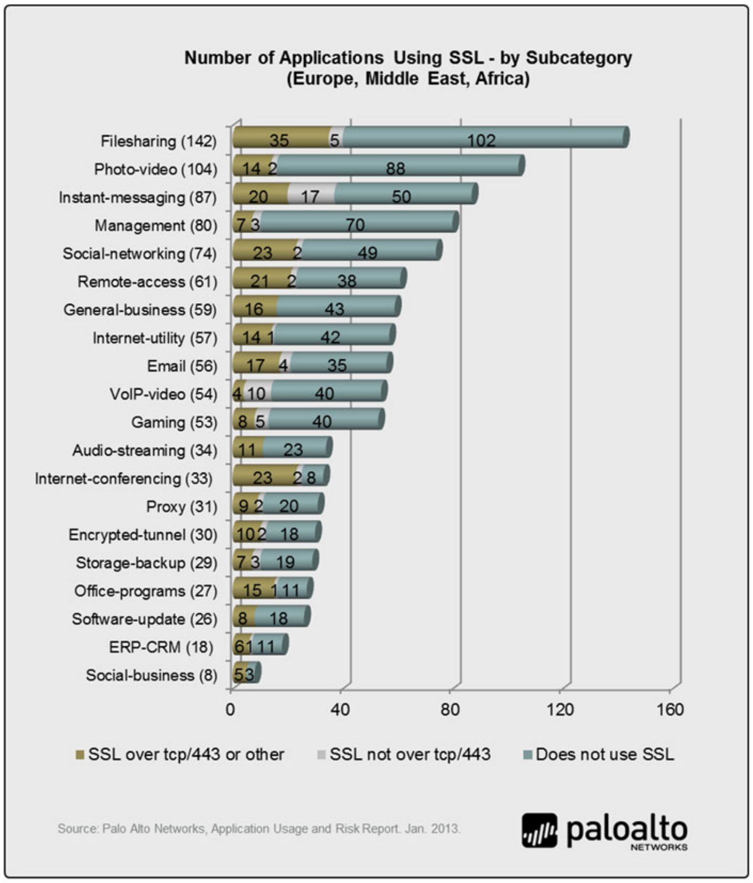


Figure 11: Applications with the highest concentration of malware logs.

340 applications can use SSL – – is it a security feature also masking malicious activity? 25% of the 1,304 applications found (340) use SSL in some way shape or form; 65 of the 340 applications that use SSL, never use port 443, nor do they use SSL defined ports (25 hop ports, 27 use port 80, 13 use a range of non-standard ports). A more interesting view is the fact that of the 340 apps that do in fact use tcp/443 (HTTPs), 124 of them (36%) are client server. The question that the use of SSL in such a wide range of applications is this – how many of them might be masking criminal activity and what is the best way to balance security and network protection via decryption?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 12: Category breakdown of applications that are capable of using SSL.

Data Sources and Additional Facts: Europe, Middle East and Africa

A summary of the data sources, statistics and key facts observed in Europe, Middle East and Africa are listed below.

- A total of 1,304 applications consumed more than 4.39 petabytes (4,394,816,598,983,220 bytes) of bandwidth across 859 participating organizations.
- Bandwidth consumption is roughly equivalent to 1.4 million 2 hour high-definition movie downloads (average download size of 3GB).
- Roughly 1,300 unique critical, high and medium severity threats representing more than 54 million logs were observed.

	Threat Logs Viewed – by Severity			
Threat Type	**Critical**	**High**	**Medium**	**Total**
Malware: spyware	736,368	144,080	953,167	1,833,615
Malware: net-worm	69,525			69,525
Malware: keylogger		1		1
Malware: botnet	22,353,364	7,498,156	30	29,851,550
Malware: backdoor	111	229,707	17,589	247,407
Malware: adware	4,942,006	616,414	5,691	5,564,111
Malware: total logs	28,101,374	8,488,358	976,477	37,566,209
Exploit: sql-injection		3,815	733,820	737,635
Exploit: overflow	198,591	2,667,292	562,677	3,428,560
Exploit: code-execution	4,233,166	5,338,581	3,451,159	13,022,906
	4431757	8009688	4747656	17,189,101
Grand Total	32,533,131	16,498,046	5,724,133	54,755,310

- Collectively, social networking, filesharing and photo-video applications represented 25% of the applications (320) and 16% of total bandwidth (~236,000 2hr high-definition movie downloads), but only 0.2% of all threat logs observed.
- The number of application variants found in each category: social networking (74), filesharing (142) and photo-video (104).
- Each network analyzed had an average of 14 social networking, 21 filesharing, and 22 photo-video application variants.
- Of the 74 social networking applications found, the four Facebook functions (-base, -apps, -social-plugins, -posting) represent 73% of all social networking bandwidth.
- Myspace was found in 66% of the organizations, while Myspace-posting was found in only 4% of the 859 organizations yet it has the highest byte-per-session consumption within social networking (slightly less than 1MB per session).
- Google-plus-posting is nearly non-existent in EMEA-based enterprise environments – found in only 3 of the 859 participating European organizations. Comparatively, posting activity for Linked-In and Facebook were found in 735 and 457 organizations respectively.
- The 142 filesharing applications found consume a 6% of the bandwidth observed with BitTorrent and FTP representing 3% and 2% respectively.

- The top 10 filesharing applications represent 99% of the respective bandwidth; 99% of the respective threat logs observed, and they are distributed across the all three technologies (3 P2P, 3 client/server, 4 browser-based).

- FTP and Webdav displayed the highest number of filesharing threat logs (primarily exploits) and were the second and sixth most heavily used filesharing applications.

- 99% of all exploit logs were found in ten applications; nine of them applications are internal/infrastructure applications (databases, SMB, Active Directory, RPC, etc.).

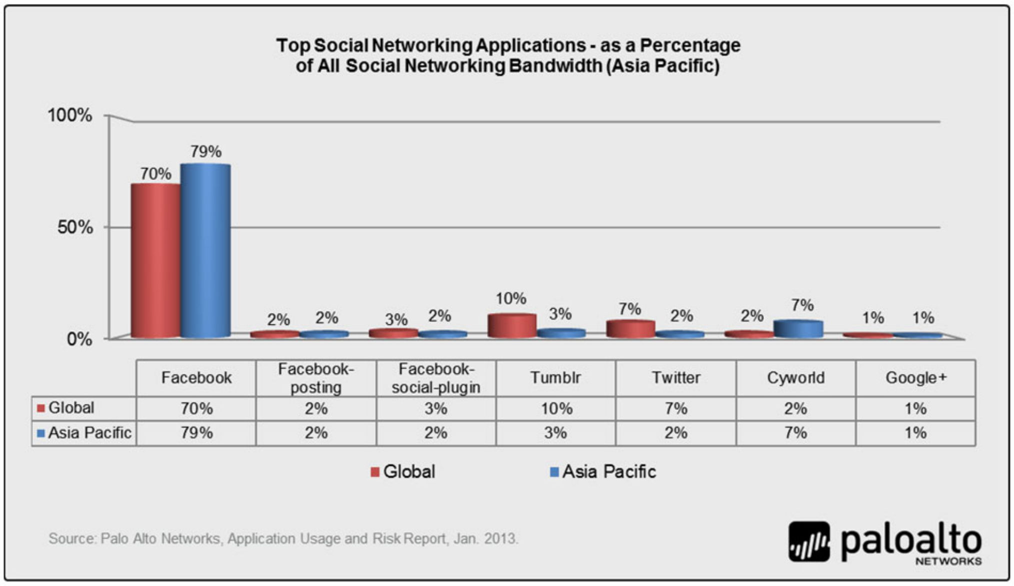
- 99.99% of all malware logs were found in only five (out of 1,304) applications with custom/unknown-UDP representing the highest volume at 74%.

- 25% of the 1,304 applications found (340) use SSL in some way shape or form; 65 of the 340 applications that use SSL, never use port 443, nor do they use SSL defined ports (25 hop ports, 27 use port 80, 13 use a range of non-standard ports).

Key Findings: Asia Pacific

The Asia Pacific dataset represents 774 organizations distributed across 16 countries with 82% of them coming from 8 countries (in order) Taiwan, Australia, Singapore, Korea, China, Thailand, Philippines and Vietnam. A total of 1,244 applications were detected along with 1,700 unique threats that had generated 44 million threat logs.

Common sharing applications are pervasive, but they display a lower than expected percentage of overall threats when compared to the other categories. Social networking, filesharing and photo-video applications collectively represent 24% of the applications (320), 27% of the bandwidth yet only 1% of the threat logs. The bulk of the threats viewed was a *cross-site scripting exploit* found in Facebook-apps. Note that Facebook continues to dominate the social networking landscape – four Facebook functions (Facebook-base, -apps, -posting, and social-plugins) consume 83% of all social networking bandwidth - leaving only 17% of the bandwidth for the other 70 variants found.



	Facebook	Facebook-posting	Facebook-social-plugin	Tumblr	Twitter	Cyworld	Google+
🟥 Global	70%	2%	3%	10%	7%	2%	1%
🟦 Asia Pacific	79%	2%	2%	3%	2%	7%	1%

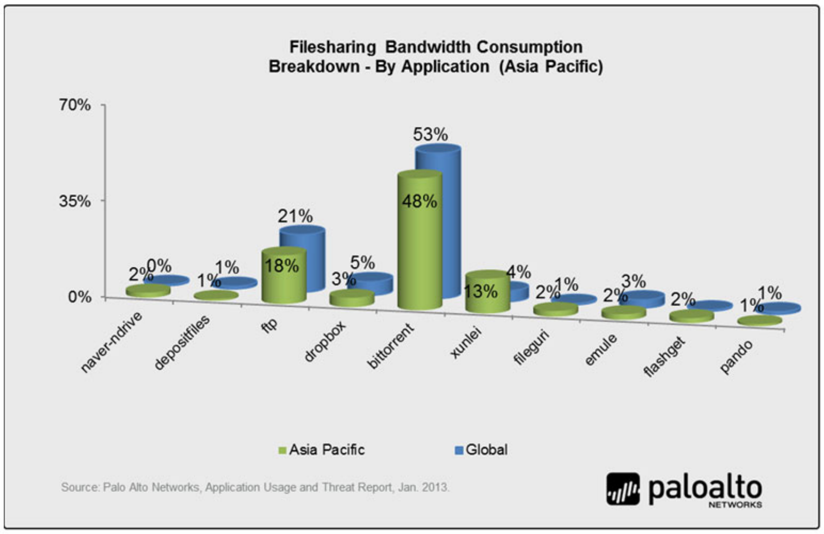
Source: Palo Alto Networks, Application Usage and Risk Report, Jan. 2013.

Figure 13: Top social networking application bandwidth consumption, as a percentage of social networking bandwidth observed.

Usage of Tumblr was nearly non-existent while Cyworld, a local social media application, was found to be used more heavily than in any other region. Google + used in 87% of the 774 organizations but Google + posting found in only 1 organization. Webshots, found in only 22% of the participating Asia Pacific organizations had the highest byte/session social networking usage (500KB/session), for reference purposes, Facebook posting is only 100KB.

Filesharing usage in APAC is dominated by P2P applications. In other regions filesharing was a bit more balanced across different technologies – in APAC it is dominated by 6 different P2P applications in the top 10. There were 132 different filesharing applications found with an average of 24 found on 99% of the 774 networks analyzed (5 client/server, 11 browser-based, 5 P2P). Within the 132 filesharing applications, the bulk of the threats and related logs were targeted at FTP.

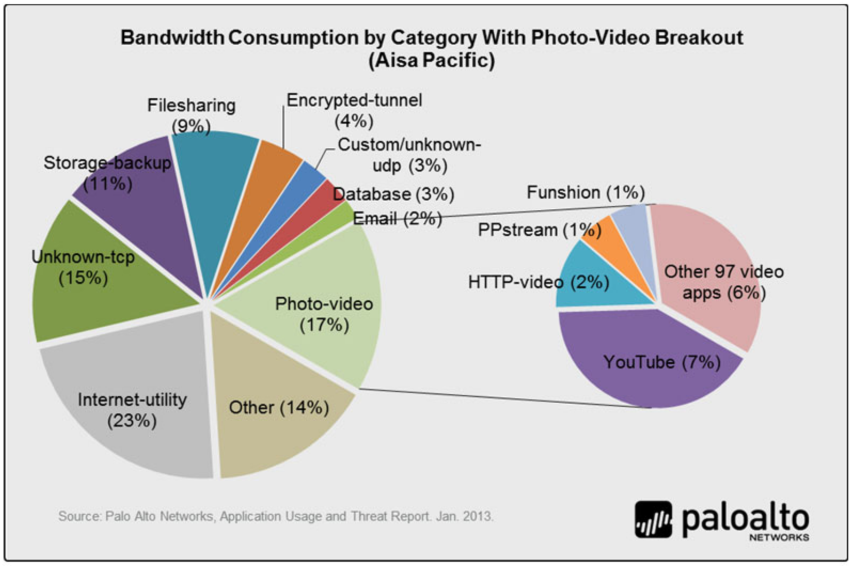
Despite control efforts, P2P in general, and BitTorrent specifically continue to be used heavily, both in terms of frequency of use (63%) and volume of use (6% of TOTAL bandwidth). It is much like a weed that continues to return, despite repeated control efforts. It raises the question of whether or not it can ever be controlled.



Source: Palo Alto Networks, Application Usage and Threat Report, Jan. 2013.

Figure 14: Top 10 filesharing applications based on total filesharing category bandwidth consumption.

What is the business value of 21 photo-video applications per network? The use of video for business purposes is known and proven; it's used for marketing promotions, lead generation, product announcements, training, and education to name just a few examples. For business purposes, the most common applications are YouTube and HTTP video, and perhaps Vimeo. On average, in the APAC, there were 21 photo-video applications found and they were consuming 17% of total bandwidth, which raises the question – what is the business use case of so many variants?



Source: Palo Alto Networks, Application Usage and Threat Report. Jan. 2013.

Figure 15: Top photo-video applications, based on bandwidth consumption.

Application vulnerability exploits target high-value business applications. The data shows that exploits such as those that are identified and blocked by an IPS are targeting internal, high-value business applications. Of the 1,244 applications, 9 of them represent 98% of the exploit logs observed and of those, 7 are considered business critical.

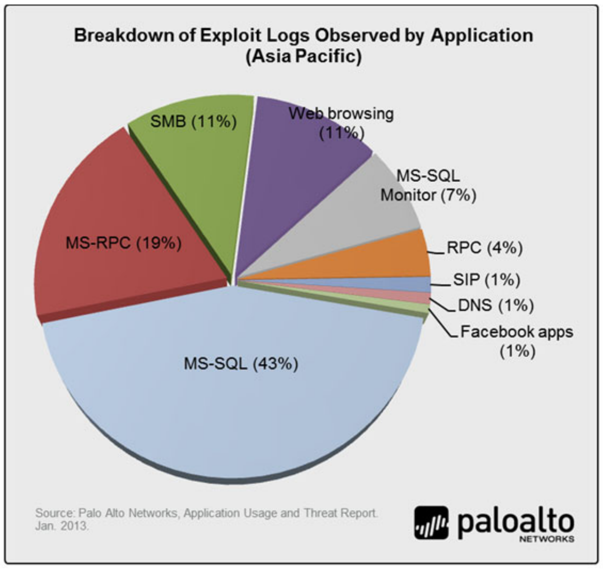


Figure 16: Applications with the highest concentration of exploit logs.

Malware is adept at hiding in unknown and custom application traffic. Nearly 100% of the malware logs (botnets, spyware, keyloggers, etc.) were found in only 4 applications – with the bulk of the logs (45%) masking themselves as custom or unknown UDP. UDP traffic, like DNS, is stateless in nature and exhibits a high session count with a small number of bytes per session. Unknown traffic exists on every network in a small amount – yet it will represent a significant volume of risk – making it a perfect example of the 80%-20% rule – a high volume of risk comes from a small volume of traffic.

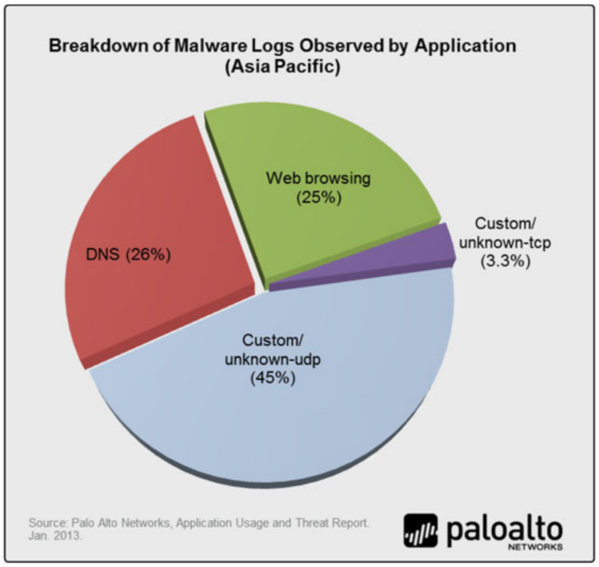
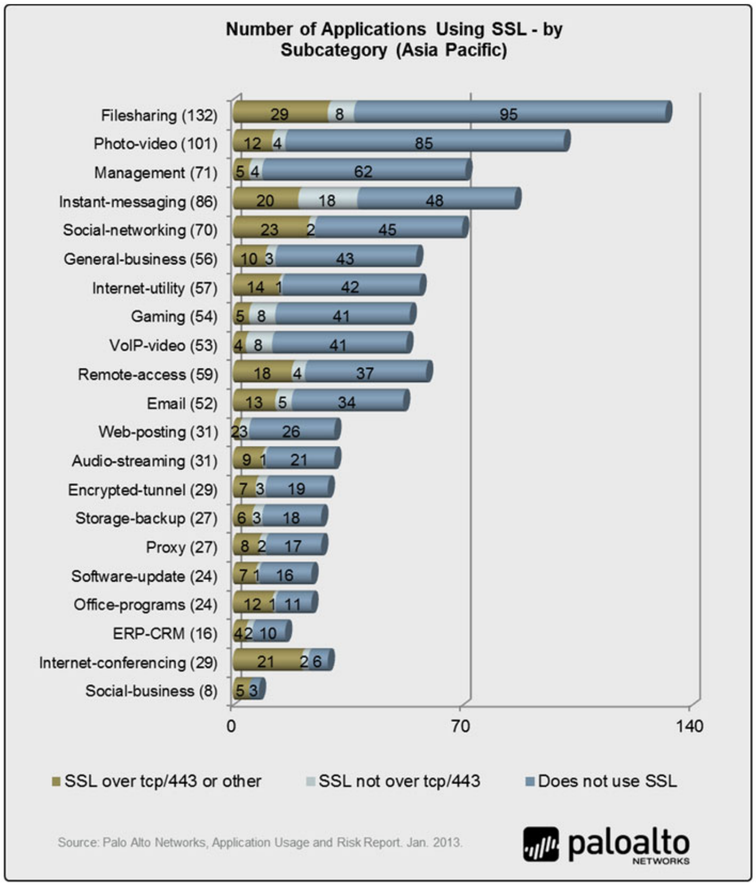


Figure 17: Applications with the highest concentration of malware logs.

317 applications can use SSL – is it a security feature also masking malicious activity? 25% of the 1,244 applications found (317) use SSL in some way shape or form; 83of the 317 applications that use SSL, never use port 443, nor do they use SSL defined ports (37 hop ports, 30 use port 80, 13 use a range of non-standard ports). A more interesting view is the fact that of the 340 apps that do in fact use tcp/443 (HTTPs), 104 of them (45%) are client server. The question that the use of SSL in such a wide range of applications is this – how many of them might be masking criminal activity and what is the best way to balance security and network protection via decryption?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 18: Category breakdown of applications that are capable of using SSL.

Data Sources and Additional Facts: Asia Pacific

A summary of the data sources, statistics observed and the key facts are listed below. Additional commentary and analysis is included throughout the report.

- A total of 1,244 applications consumed more than 2.3 petabytes (2,331,251,386,112,620 bytes) of bandwidth across 774 participating organizations.
- Bandwidth consumption is roughly equivalent to 774,000 2 hour HD movie downloads (average download size of 3GB).
- Roughly 1,700 unique critical, high and medium severity threats representing more than 44 million logs were observed.

	Threat Logs Viewed – by Severity			
Threat Type	**Critical**	**High**	**Medium**	**Total**
Malware: spyware	1,291,062	43,811	1,546,640	2,881,513
Malware: net-worm	1,629,139			1,629,139
Malware: keylogger		1,922		1,922
Malware: botnet	15,067,644	6,575,535	1,425	21,644,604
Malware: backdoor	1,066	1,906,904	5,851	1,913,821
Malware: adware	4,076,647	1,784	20,237	4,098,668
Malware: total logs	**22,065,558**	**8,529,956**	**1,574,153**	**32,169,667**
Exploit: sql-injection		311	386,357	386,668
Exploit: overflow	311,716	359,137	5,249,612	5,920,465
Exploit: code-execution	1,038,793	3,350,084	1,371,006	5,759,883
Exploit: total logs	**1,350,509**	**3,709,532**	**7,006,975**	**12,067,016**
Grand Total	**23,416,067**	**12,239,488**	**8,581,128**	**44,236,683**

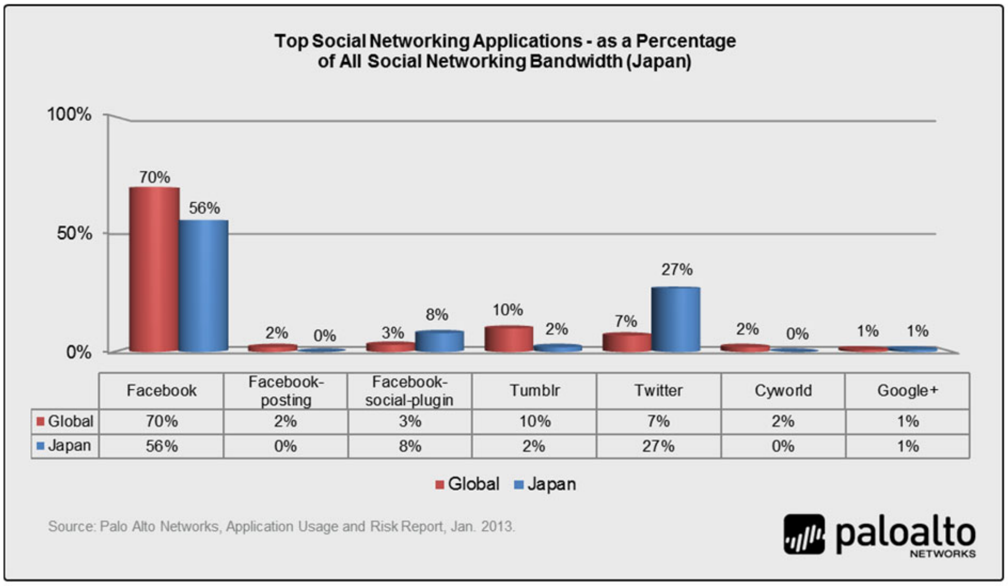
- Collectively, social networking, filesharing and photo-video applications represented 24% of the applications (303) and 27% of total bandwidth (~213,000 2hr high-definition movie downloads), but only 1% of all threat logs observed – primarily Facebook Apps.
- The number of application variants found in each category: social networking (70), filesharing (132) and photo-video (101).
- Each network analyzed had an average of 12 social networking, 24 filesharing, and 21 photo-video application variants.
- Of the 70 social networking applications found, the four Facebook functions (-base, -apps, -social-plugins, -posting) represent 83% of all social networking bandwidth.
- Google + used in 87% of the 774 organizations – Google + posting found in only 1 organization; Myspace continues to survive - found in 52% of the organizations.
- Webshots, found in 22% was highest byte/session social networking usage (500KB/session) – Facebook posting is only 100KB.
- The 142 filesharing applications found consume a 6% of the bandwidth observed with BitTorrent and FTP representing 3% and 2% respectively.
- The top 10 filesharing applications represent 92% of the respective bandwidth; 96% of the respective threat logs observed, and they are dominated by P2P (6 P2P, 2 client/server, 2 browser-based); FTP displayed the highest number of filesharing threat logs (primarily exploits).

- 98% of all exploit logs were found in nine applications; 7 of them applications are internal/infrastructure applications (databases, Active Directory, RPC, etc.).
- 99.99% of all malware logs were found in only 4 (out of 1,244) applications with custom/unknown-UDP representing the highest volume at 45%.
- 25% of the 1,244 applications found (317) use SSL in some way shape or form; 83 of the 317 applications that use SSL, never use port 443, nor do they use SSL defined ports (37 hop ports, 30 use port 80, 13 use a range of non-standard ports).

Key Findings: Japan

The Japanese dataset represents 299 networks analyzed with 960 applications and nearly 500 unique threats that generated 4.68 million threat logs.

Common sharing applications are pervasive, but they display a lower than expected percentage of overall threats when compared to the other categories. Social networking, filesharing and photo-video applications collectively represent 29% of the applications (274), 15% of the bandwidth yet only 0.4% of the threat logs. . This is not to say these applications are low risk – the data shows that a greater percentage of the threats (exploits and malware) were found in other applications. Facebook (browsing and social plugins) and Twitter dominate the social networking usage – consuming a collective 91% of the bandwidth, leaving a mere 9% of the social networking bandwidth for the other 63 variants found.



	Facebook	Facebook-posting	Facebook-social-plugin	Tumblr	Twitter	Cyworld	Google+
🟥 Global	70%	2%	3%	10%	7%	2%	1%
🟦 Japan	56%	0%	8%	2%	27%	0%	1%

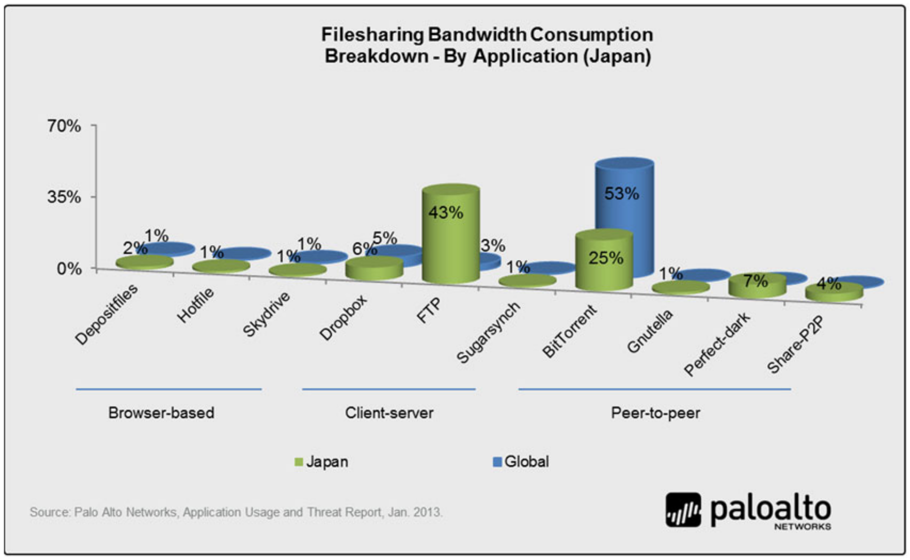
Source: Palo Alto Networks, Application Usage and Risk Report, Jan. 2013.

Figure 19: Top social networking application bandwidth consumption, as a percentage of social networking bandwidth observed.

Japan is the only region where Twitter is more than a quarter of the social networking bandwidth – all other regions, use is less than 10%. Google + was found in 77% of the 299 organizations, but Google + posting was not found in any Japanese organizations. Netlog, found in 16% of the 299 organizations was highest byte/session social networking usage.

Filesharing usage in Japan is dominated by FTP and BitTorrent. Japan is the only region where an application other than BitTorrent was the largest consumer of bandwidth. FTP consumed 43% of the filesharing bandwidth while BitTorrent consumed 25%. Two other P2P applications, Perfect Dark and Share-p2p were used more heavily in Japan than in other regions. Despite control efforts, P2P in general continues to be used heavily. It is much like a weed that continues to return, despite repeated control efforts, raising the question of whether or not it can ever be controlled.

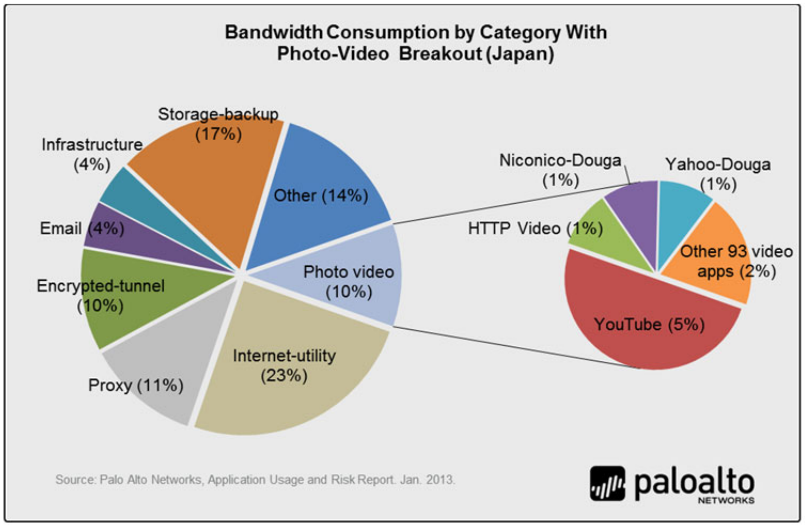
Collectively, 112 filesharing applications were found to be consuming 4% of all bandwidth observed. The bulk of the threat logs, primarily exploits were targeted at FTP.



Source: Palo Alto Networks, Application Usage and Threat Report, Jan. 2013.

Figure 20: Top 10 filesharing applications based on total filesharing bandwidth consumption.

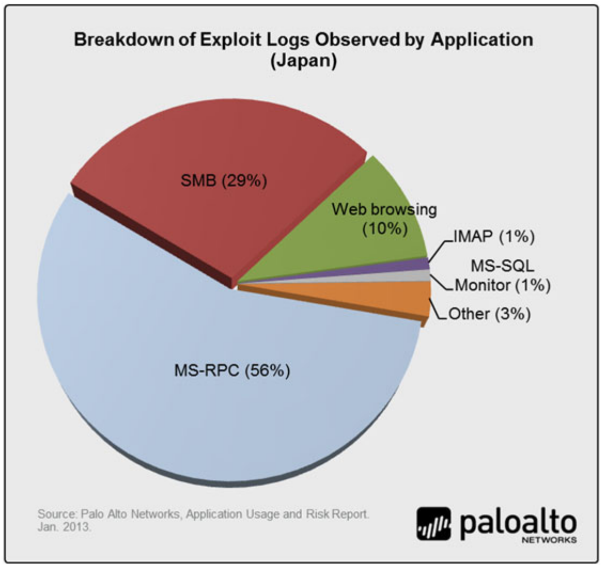
What is the business value of 19 photo-video applications per network? The use of video for business purposes is known and proven; it's used for marketing promotions, lead generation, product announcements, training, and education to name just a few examples. For business purposes, the most common applications are YouTube and HTTP video. A total of 96 photo-video applications were found within the 299 participating networks with an average of 19 on every network. Collectively they consumed 10% of total bandwidth, which raises the question – what is the business use case of so many variants?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 21: Top photo-video applications, based on bandwidth consumption.

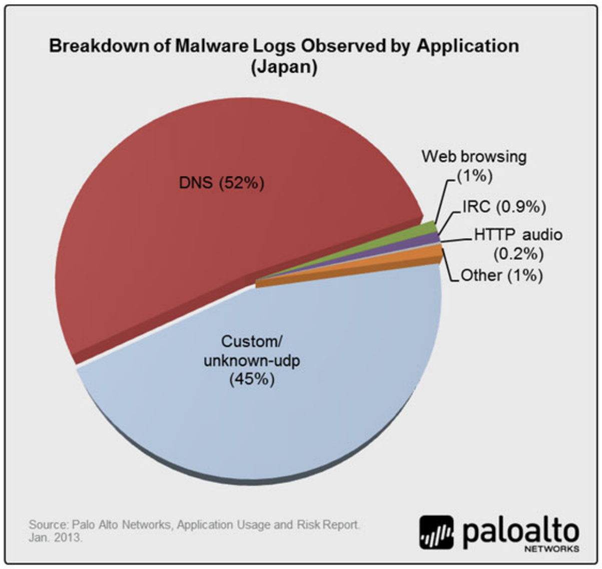
Application vulnerability exploits target high-value business applications. The data shows that exploits such as those that are identified and blocked by an IPS are targeting internal, high-value business applications. Of the 960 applications, 6 of them represent 97% of the exploit logs observed and of those, 5 are considered business critical.



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 22: Applications with the highest concentration of exploit logs.

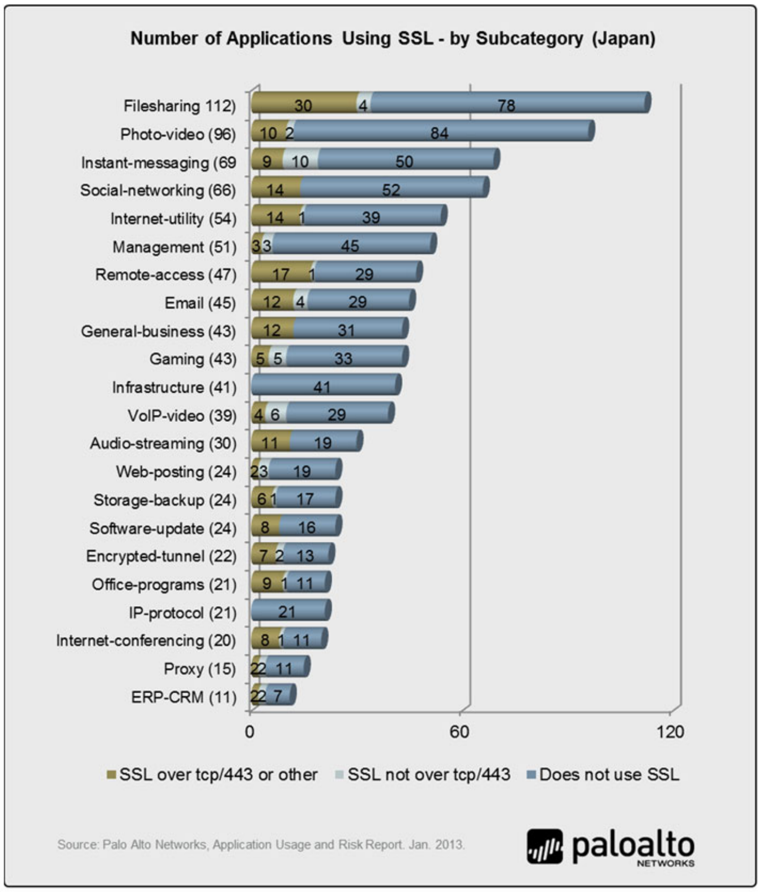
Malware is adept at hiding in unknown and custom application traffic. Nearly 100% of the malware logs (botnets, spyware, keyloggers, etc.) were found in only 4 applications – with the bulk of the logs (45%) masking themselves as custom or unknown UDP. UDP traffic, like DNS, is stateless in nature and exhibits a high session count with a small number of bytes per session. Unknown traffic exists on every network in a small amount – yet it will represent a significant volume of risk – making it a perfect example of the 80%-20% rule – a high volume of risk comes from a small volume of traffic.



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 23: Applications with the highest concentration of malware logs.

156 applications can use SSL — is it a security feature also masking malicious activity? 16% of the 960 applications found (156) can use SSL in some way shape or form; 48of them never use port 443, nor do they use SSL defined ports (17 hop ports, 21 use port 80, 103 use a range of non-standard ports). A more interesting view is the fact that of the 340 apps that do in fact use tcp/443 (HTTPs), 109 of them (56%) are client server. The question that the use of SSL in such a wide range of applications is this – how many of them might be masking criminal activity and what is the best way to balance security and network protection via decryption?



Source: Palo Alto Networks, Application Usage and Risk Report. Jan. 2013.

Figure 24: Category breakdown of applications that are capable of using SSL.

Data Sources and Additional Facts: Japan

A summary of the data sources, statistics observed and the key facts are listed below. Additional commentary and analysis is included throughout the report.

- A total of 960 applications consumed more than 589 terabytes (589,106,890,881,747 bytes) of bandwidth across 299 participating organizations.
- Bandwidth consumption is roughly equivalent to 196,000 2 hour high definition movie downloads (average download size of 3GB).
- Roughly 500 unique critical, high and medium severity threats representing more than 4.68 million logs were observed.

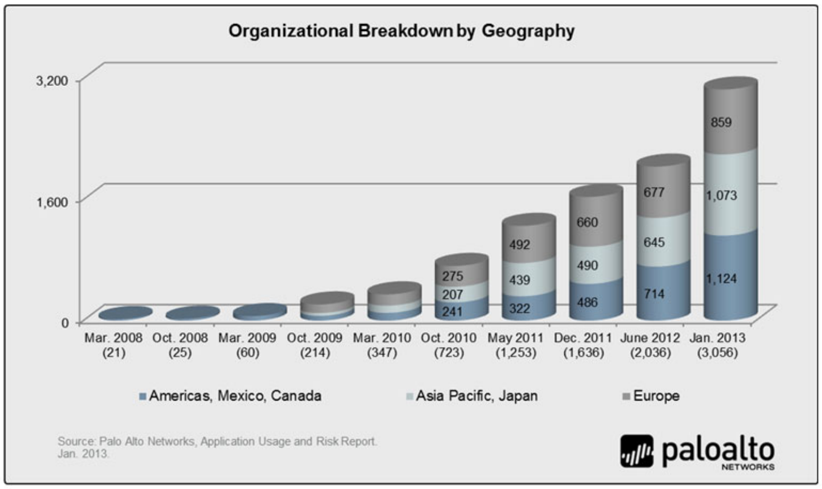
	Threat Logs Viewed – by Severity			
Threat Type	**Critical**	**High**	**Medium**	**Total**
Malware: spyware	38,711	14	36,080	74,805
Malware: net-worm	3			3
Malware: keylogger				
Malware: botnet	864,843	2,306,585		3,171,428
Malware: backdoor	379	6,852	17,909	25,140
Malware: adware	430,956	7	35	430,998
Malware: total logs	**1,334,892**	**2,313,458**	**54,024**	**3,702,374**
Exploit: sql-injection		303	42,736	43,039
Exploit: overflow	95,979	13,426	331	109,736
Exploit: code-execution	12,607	729,907	83,202	825,716
Exploit: total logs	**108,586**	**743,636**	**126,269**	**978,491**
Grand Total	**1,443,478**	**3,057,094**	**180,293**	**4,680,865**

- Collectively, social networking, filesharing and photo-video applications represented 25% of the applications (274) and 15% of total bandwidth (~31,000 2hr high-definition movie downloads), but only 0.4% of all threat logs observed.
- The number of application variants found in each category: social networking (68), filesharing (112) and photo-video (96).
- Each network analyzed had an average of 11 social networking, 19 filesharing, and 13 photo-video application variants.
- Of the 74 social networking applications found, the four Facebook functions (-base, -apps, -social-plugins, -posting) represent 64% of all social networking bandwidth.
- Twitter consumes 27% of social networking bandwidth more than 3 times the next closest competitor.
- Google + used in 77% of the 299 organizations – Google + posting not found in any Japanese organizations
- Myspace continues to be found in 52% of the organizations; myspace posting was the 2nd highest bytes/session within social networking; Netlog, found in 16% of the 299 organizations was highest byte/session social networking usage
- The 112 filesharing applications found consume a 4% of the bandwidth observed with FTP and BitTorrent representing 3% collectively.

- The top 10 filesharing applications represent 92% of the respective bandwidth; 89% of the respective threat logs observed, and they are distributed across the all three technologies (4 P2P, 3 client/server, 3 browser-based).
- FTP displayed the highest number of filesharing threat logs (primarily exploits).
- 97% of all exploit logs were found in 6 applications; 5 of them are internal/infrastructure applications (databases, Active Directory, RPC, etc.).
- 99.99% of all malware logs were found in only five (out of 960) applications with custom/unknown-UDP representing the highest volume at 45%.
- 16% of the 960 applications found (156) use SSL in some way shape or form; 48 of the applications that use SSL, never use port 443, nor do they use SSL defined ports (17 hop ports, 19 use port 80, 12 use a range of non-standard ports).

Demographics and Methodology

The latest edition of the Application Usage and Risk Report summarizes 3,056 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. Jan. 2013.

Figure XX: Geographic distribution of participating organizations.

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, where it monitors traffic traversing the network. 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.

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its innovative platform enables enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks platform is its next-generation firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks products are used by more than 10,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.