APPLICATION USAGE AND THREAT REPORT

paloalto NETWORKS®

Research by Unit 42

Overview

The impact of data breaches is ever increasing, and more of our private data than ever is being stolen. As security professionals, defending our organizations can often times seem like a monumental, almost impossible task. Yet, there has never been as much focus, data, or development available to the security industry as there is today. It is only the small proportion of truly advanced adversaries that have proven to be resourceful, developing new tactics, techniques, and procedures as seen fit; whereas, the majority of adversaries reuse old tactics, techniques, and procedures, simply because they are effective and require little to no effort in execution. Even within the most sophisticated groups, commonalities exist within the attack lifecycle, which can be used to identify and stop them.

With this knowledge, we, as security professionals, must turn the tables on the adversaries and make it increasingly difficult and cost inefficient to launch an attack. The first step to this type of proactive defense is the sharing of tactics, techniques, and procedures, as well as threat intelligence in an open and free manner throughout the entire security community, including this report. The more we know about our adversaries, the harder it will be for them to successfully execute an attack, which allows us to proactively defend our organizations in a targeted manner, versus the traditional "find the needle in the haystack" model of reactive defense.

In this year's Application Usage and Threat Report, **Unit 42**, the Palo Alto Networks® threat intelligence team, examines key trends across the threat landscape and application usage, including topics on how organizations can educate users and utilize controls to effectively reduce the attack surface available to an adversary, the potential effects of non-standard network activity, the reuse of legacy attack tactics, and the benefits of open threat intelligence sharing.

Key Findings

Adversary dossiers for major threat actor groups
The tactics, techniques and procedures (TTPs) used by three major threat actor groups, including their targets, motivations and methods, which can be used to better protect your organization.
p4

Remote access application usage is rampant across all industries and regions
79 unique remote access applications were found to be in use across all regions and industries.
p6

SaaS-based application usage has continued to grow
SaaS-based application usage has grown 46% over the past 3 years, including more than 316 apps.
p8

Nearly half of all portable executables analyzed by WildFire were found to be malicious
p10

Over 40% of all email activity examined via WildFire containing a file attachment was found to be malicious in nature
p11

Macro-based malware has seen a resurgence and is among the most popular type of malware being distributed to users
The two most numerous examples are Dyre and Dridex: 10.2 percent of all sessions marked with malicious activity in WildFire was related to Dyre and Dridex.
p14

Current world events are being weaponized rapidly and used to piggyback attacks
The average time to weaponization was 6 hours from the initial reporting of a world event; some events taking as little as 3 hours to weaponization.
p16

Adversary Dossiers

A critical element to understand your organization's risk posture is gaining intelligence on the adversary groups that may attempt to breach your network.

The concept of attribution has been a hotly debated topic across the security industry, with some research organizations attempting to pinpoint the geographic location of the group, or reveal the names of the individuals launching the attacks. We believe in a different kind of attribution; one that focuses on the Tools, Tactics, and Procedures (TTPs) employed by the adversaries, which is a more actionable set of intelligence. Once you understand Indicators of Compromise (IOCs), such as command and control infrastructure, malware deployed, or methods of initial compromise, you can build preventative controls to stop them at every point in the attack lifecycle.

Gaining context around the adversary will also allow teams to prioritize their response efforts. For instance, organizations in government sectors will be more concerned by cyber espionage activity, versus a financial services organization, who would be more interested in cyber crime targeting financial gain. Below, we have gathered a set of profiles on three major threat actor groups, which security teams can use to understand if they could be targeted by the groups, and how to reduce their risk of being successfully breached.

CARBANAK

Known Aliases

Anunuk

Origin

Russia and Ukraine nexus

Motivation

Financial gain
Some evidence of cyber espionage

Summary

Responsible for the theft of hundreds of millions of dollars from various financial institutions beginning in late 2013

Used a number of techniques such as group transfers or withdrawls from compromised systems

Targeted Regions/Industries

Initial targeted region was Russia

In early 2014 attacks against United States and rest of Europe were observed

Attacks against China region have also been observed

Primarily targeted money processing services, ATMs, and financial accounts

Tactics and Tools Deployed

Utilizes the malware family known as Carbanak

Commonly delivered via spear-phishing email containing a malicious Office document or control panel (CPL) file

Malware provides backdoor remote access and data exfiltration features

Once a patient zero system has been compromised, additional reconnaissance is performed to identify ATMs, financial accounts, or other areas where money can be transferred

SANDWORM

Known Aliases

Quedagh

Origin

Russia nexus

Motivation

Cyber espionage

Summary

Cyber espionage group attributed to Russian nexus

First disclosed publically in October 2014

Known attacks began December 2013 and continued into 2014

Attributed to using the BlackEnergy Trojan to execute espionage activity against industrial control system (ICS) environments

Targeted Regions/Industries

Europe region
Telecommunications
Energy
Government
U.S.-based education institutions
ICS environments

Tactics and Tools Deployed

Utilizes two variants of the BlackEnergy Trojan

Has utilized a zero-day vulnerability (CVE-2014-4114) in the past for malware delivery

Also uses spear-phishing attacks

Developed custom plugin modules for BlackEnergy Trojan which allows for remote access, network traversal, keylogging, credential harvesting, network capturing, and screen capturing

SHELLCREW

Known Aliases

Shell Crew
Deep Panda
Axiom
Group 72

Origin

China nexus

Motivation

Espionage

Summary

A technically sophisticated and likely well-funded, state-sponsored APT group

Have used multiple zero days and can move very quickly once inside a network.

Known to layer different malware throughout a network to maintain persistence, as well as harvest and use legitimate network and remote access credentials.

Targeted Regions/Industries

Healthcare
Government
Manufacturing
Defense
Aerospace
Industrial
Pro-democracy NGO
Energy
Telecommunications
Academic institutions
Journalists
Think-tanks
Media
Specific companies affected
Premera Blue Cross
Anthem
- *OPM*
- *Bit9*
- *RSA*

Tactics and Tools Deployed

Utilizes doppelganger command and control domains to dupe users and obfuscate activity

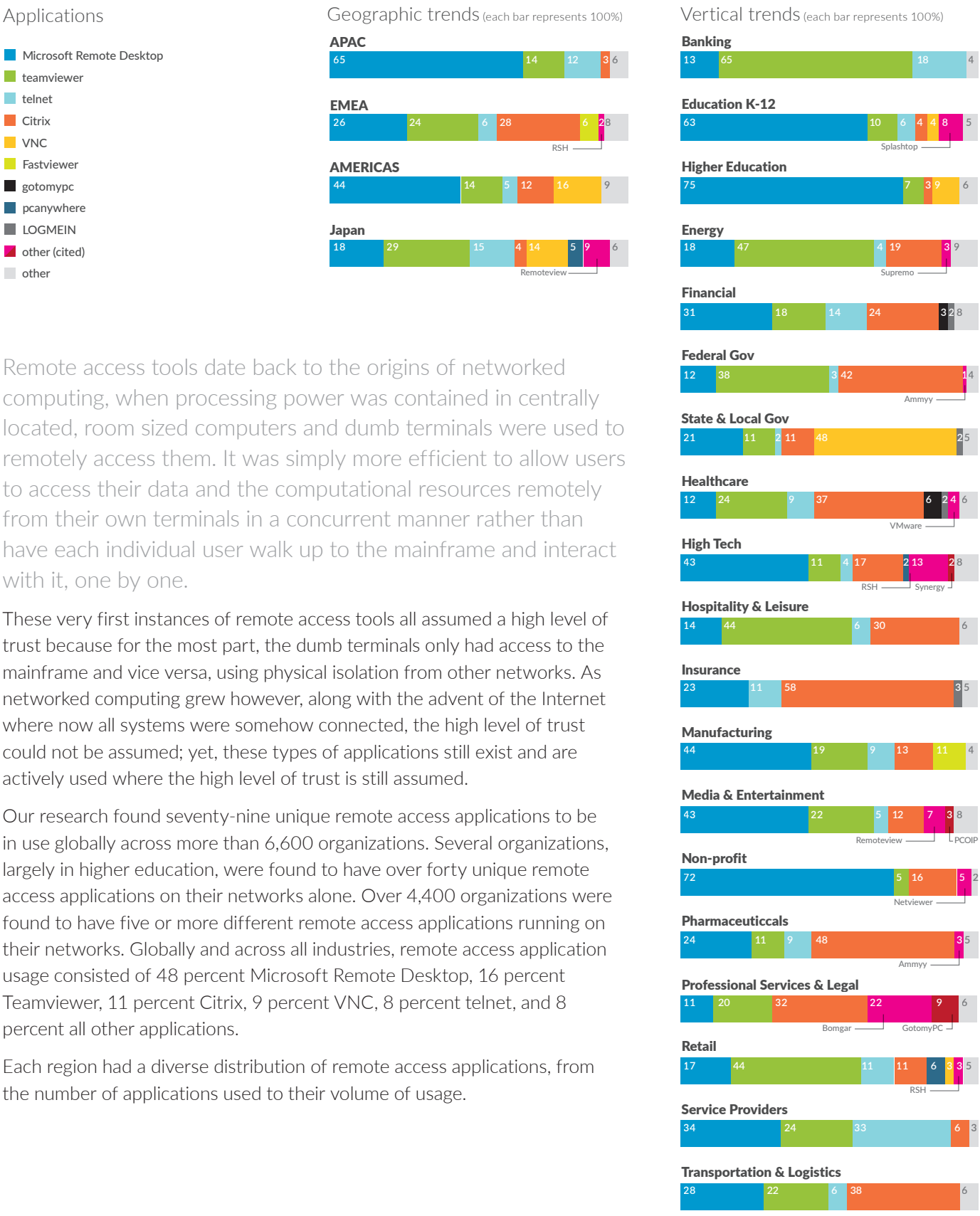
Heavy usage of spear-phishing and watering hole attacks to deliver malware or harvest credentials

Have been known to user zero day vulnerabilities

Has also been known to use legitimate network administration tools with legitimate compromised credentials

- *Malware families known to be used*
- *Poison Ivy*
- *GhOst*
- *Derusbi*
- *Scanbox*
- *Sakula*
- *Zxshell*
- *Zox family*
- *PlugX*

Remote Access Application Usage



Remote access tools date back to the origins of networked computing, when processing power was contained in centrally located, room sized computers and dumb terminals were used to remotely access them. It was simply more efficient to allow users to access their data and the computational resources remotely from their own terminals in a concurrent manner rather than have each individual user walk up to the mainframe and interact with it, one by one.

These very first instances of remote access tools all assumed a high level of trust because for the most part, the dumb terminals only had access to the mainframe and vice versa, using physical isolation from other networks. As networked computing grew however, along with the advent of the Internet where now all systems were somehow connected, the high level of trust could not be assumed; yet, these types of applications still exist and are actively used where the high level of trust is still assumed.

Our research found seventy-nine unique remote access applications to be in use globally across more than 6,600 organizations. Several organizations, largely in higher education, were found to have over forty unique remote access applications on their networks alone. Over 4,400 organizations were found to have five or more different remote access applications running on their networks. Globally and across all industries, remote access application usage consisted of 48 percent Microsoft Remote Desktop, 16 percent Teamviewer, 11 percent Citrix, 9 percent VNC, 8 percent telnet, and 8 percent all other applications.

Each region had a diverse distribution of remote access applications, from the number of applications used to their volume of usage.

Ammyy

In recent years, the legitimate remote access application known as Ammyy® has commonly been exploited by adversaries in 'vishing' or voice phishing attacks[1, 2, 3]. These attacks have been largely targeted at English-speaking countries and have been fairly successful in duping users into installing the remote access application and giving the adversary access to their systems.

The attack generally starts with a user receiving a phone call from a person purporting to be from Microsoft, Dell, or even their own organization's IT department. The adversary may then claim that the user's system has been discovered to be infected by some form of advanced malware and the user must now install a specific application (Ammyy) to remove it. The adversary then directs the user to either the official Ammyy website to download the server software or to another website that hosts the server software. The adversary then asks the user for the code that the Ammyy software generates, giving them complete access to the user's system. At this point, the adversary may claim the malware infection has been fixed or may begin to load actual malware onto the now remotely controlled system to hold the user at ransom or perform other nefarious activities. The industries with the most number of sessions captured for Ammyy usage were Federal Government, Manufacturing, and Energy.

What does this mean?

With such a variety of remote access application usage across enterprise networks, it is no wonder that these applications are oftentimes being leveraged for malicious activity by threat actors. Telnet and rsh, due to the era of their creation, were not established for password authentication or encryption and thus pass all of their activity in cleartext. This is a major vulnerability and could potentially be exploited with ease by an adversary. Microsoft Remote Desktop and Citrix have their own set of security vulnerabilities, and using client-less or cloud-based remote access applications also carry their own specific risks on how they are even secured in the first place. The biggest issue of using remote access applications, however, is that once an attacker has gained access, they now have effective control over the host with the remote access application server running on it, without having to compromise the affected host or attacking it using any other exploits.

Risks are additionally increased as more end users are given privileges to digital resources and begin installing unauthorized remote access applications. For users, this makes sense – remote access applications to their workstation, for example, allow them to continue to do work when they are remote or at home. With this type of usage, however, due to bypassing the organization's IT department and security teams, the application is often deployed in an insecure manner and not using best practices, which leads to using default passwords or at times bypassing any security controls that may have been put in place by the organization.

Remote access application usage is widespread, regardless of region or industry. With the ever-increasing usage of virtual systems, the cloud, and the Internet of Things, remote access application usage will, in turn, continue to increase. Restricting usage of remote access applications is unfeasible and inefficient, but implementing proper usage policies and controlling the deployment of these applications is feasible and must be practiced by all organizations.

[1] http://resources.infosecinstitute.com/phishing-techniques-similarities-differences-and-trends-part-iii-vishing/
[2] http://www.networkworld.com/article/2605887/microsoft-subnet/zero-day-opens-the-way-to-hack-back-against-fake-microsoft-tech-support-scammers.html
[3] http://www.ammyy.com/en/admin_mu.html

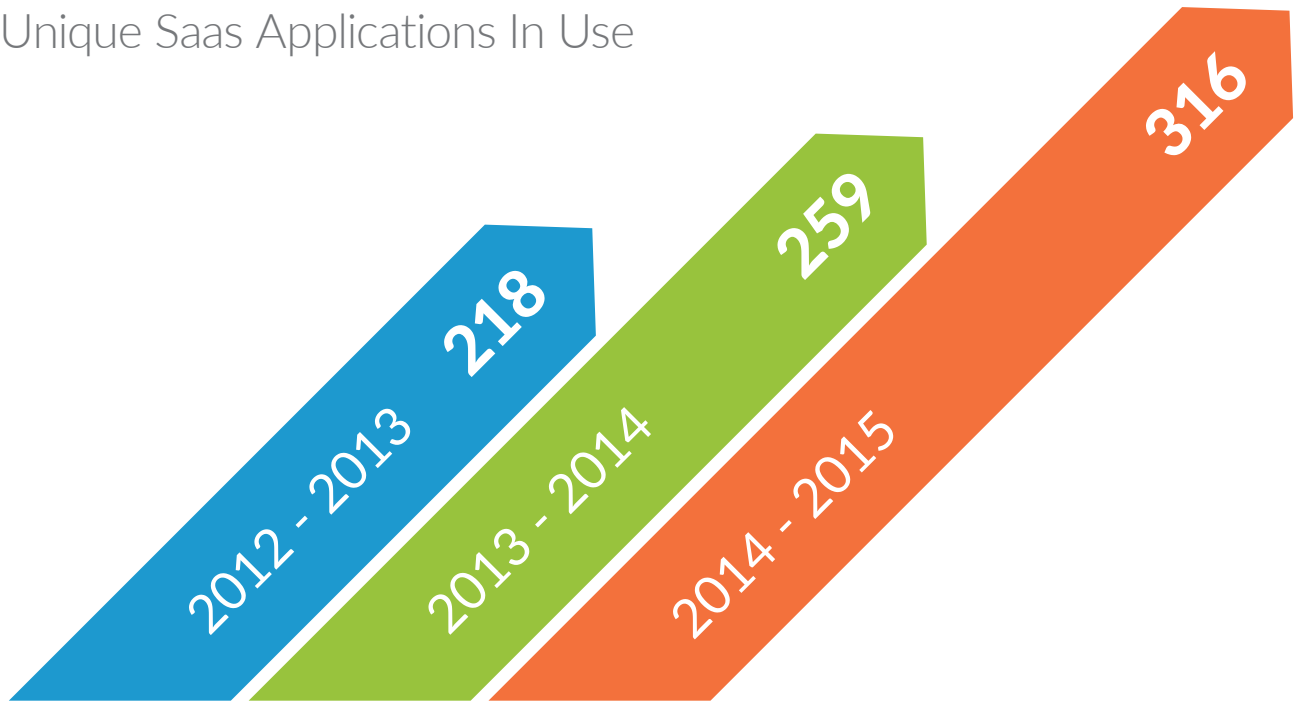
SaaS-based Application Trends

Organizations are adopting SaaS-based application services at a breakneck pace. These applications continue to redefine the network perimeter, providing critical functionality and efficiency, but at the same time introduce potential new security and data risks if not properly controlled. Often, individuals or departments will begin using un-sanctioned SaaS services, creating a "shadow IT" environment, further complicating the visibility into day-to-day user activity and the security of sensitive data.

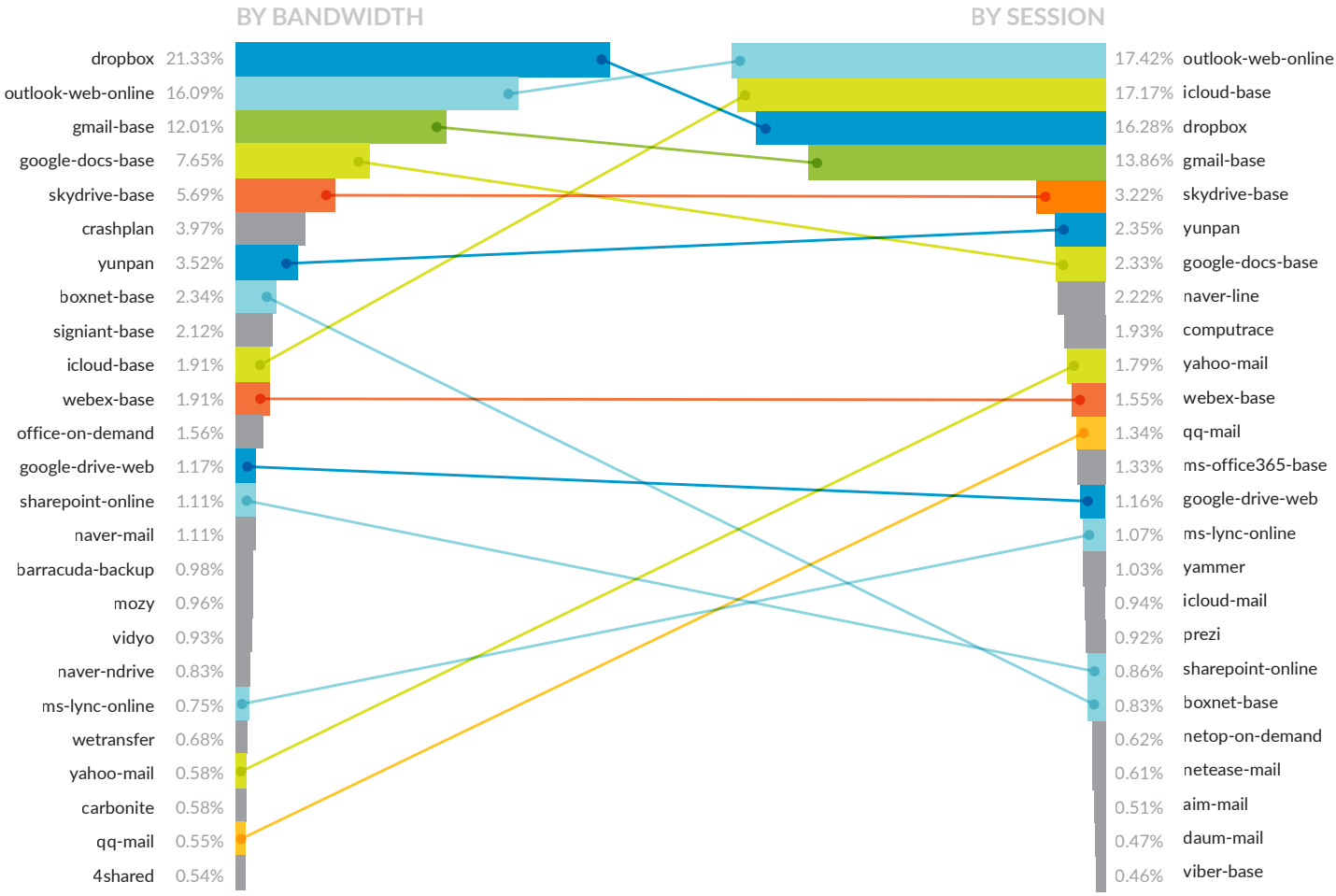
Between 2012 and 2015, we found a 46 percent increase in usage of SaaS applications on customer networks, highlighting the continued importance of assessing the security and data risks these services introduce.

Looking deeper into the category of applications that comprise the 316 dataset, we found that overwhelming these applications fell into two categories: email (38 percent) and file storage (40.7 percent). These figures are concerning, due to the fact that a large portion of this activity is likely non-sanctioned usage of unknown or uncontrolled applications. In most organizations that do SaaS applications, users are provided access to a specific list of services the organization has deemed acceptable or suitable for business purposes. Given the large percentage of usage and the high number of unique SaaS applications observed, it can be concluded that users are likely not following these types of usage policies, and are instead engaging in rampant usage of non-sanctioned SaaS applications. This further increases the risk of data leakage to organizations, due to the lack of visibility from regular logs or notifications from the unauthorized SaaS storage providers, as well as additional risk of the intermeshing of users' personal email and work emails, which may cause situations where a user may be attacked on their personal emails and the adversary then pivots to the work email account.

Unique Saas Applications In Use



Usage of Top 25 SaaS-based applications



What does this mean?

The constant battle between security professionals and end users has been the level of usability that a user needs, and to what extent we are willing to sacrifice security for it. SaaS services shine the light on this issue further, in large part because at this point in most users' Internet career, the use of SaaS is a normal, everyday occurrence. The use of Gmail to check their email, Dropbox to upload some files, or iCloud to synchronize their pictures is a part of their everyday workflow. Deploying policies to completely prevent this type of behavior can be impractical, given the widespread and often business-relevant usage of these applications. Ideally, organizations have a multi-pronged approach that does not blindly restrict usage, but ensures that only authorized SaaS applications are in use, layered with the visibility and security controls required to ensure the sanctity of the organizations' security posture and data. Lastly, regular user education about SaaS services in general, and why it may be a risk to the organization, should be regularly performed. Asking security professionals to secure SaaS applications is oftentimes a challenging task for both the requester and the implementer, but it is something that will be required even more so as industries move more and more toward these applications and services.

Unknown Threat Data and Analysis

New for this year, Palo Alto Networks Unit 42 team used the AutoFocus™ threat intelligence service to data-mine and analyze malware-specific activity from WildFire™.

Top 10 applications delivering unknown threats by session (WildFire)

Percent of Malicious Sessions

Applications delivering unknown malware:

Understanding the application attack surface facing your organization is a critical tool security teams can use to understand the risk posture of their organization. From a volume-based perspective it is clear that web browsing and SMTP still reign supreme as a delivery vector, being responsible for 96 percent of all malicious sessions. Adversaries are well aware of the pervasive nature of these applications throughout most organizations, meaning they offer the quickest and easiest route to infection. With this knowledge in mind, most security organizations have implemented the majority of their defenses on these two applications, and for good reason.

Taken another way, our data shows that about 4 percent of malicious sessions is delivered via applications other than web browsing and SMTP. The essential question becomes: are you prepared for the 4 percent? Just this small percentage represents hundreds of thousands of malicious sessions, and we believe also trends toward use by more sophisticated adversaries.

Ensuring that unknown threats cannot get into your organizations through SMTP and web-browsing is a good way to create a strong "front door," but you have to consider all the alternate routes adversaries will take, including using applications such as FTP, Webdav, or Yunpan, as we see above. Security teams must consider every possible application attack vector that exists across their network as the "widows, cracks, and holes in the roof," because attackers will certainty not stick to just walking in through the front door.

Top 10 application subcategories by percentage of malicious sessions (WildFire)

Percent of Malicious

Applications delivering unknown malware by application subcategory:

The observations on the left provide information on the number of malware samples delivered via each application category, compared to the total samples seen within that category. For instance, the chart shows that out of all the content observed over remote access applications, 16.5 percent of it was malware. Taken together with the volume-based information in the previous section, this data allows you to prioritize your security efforts on the applications and categories used most by attackers.

Time for PE!

Portable executables (PE), commonly known as program files or files ending with the extension '.exe', were found to be prevalent throughout the WildFire data and highly malicious in nature, with about 82.4 percent of observed executables categorized as malware, including a whopping 49 percent of unique samples. This type of activity is not surprising; using a PE to launch an attack on a potential victim is the most direct method, as it generally does not require additional exploit code or packaging to be successful. Instead, using PEs relies on the unaware user to trust the executable file to be launched. To further increase the chance of successful exploitation of the user, a common tactic used by adversaries is the use of double extensions, where a file may actually be a PE with the .exe extension, but the adversary will append a familiar document extension such as .doc, .pdf, or .jpg before the .exe extension, and even go so far as to change the icon of the file so that it is inline with the file it purports to be.

Gone Phishin'

Examination of the session data in how potential malware is delivered also served an interesting, yet again, not surprising finding in that phishing attacks are rampant and widespread. Phishing in various forms has been in use by adversaries from the very beginning, and continues to be used due to its efficacy. Much like PEs, phishing generally requires no additional exploitation by the adversary, other than attaching a malicious file to the phishing email or simply pasting a link to a website hosting the malicious file. It is no wonder adversaries continue to use phishing as a main tactic and vector for attack.

For the timeframe of this report, about 41.4 percent of all emails with a file attachment observed via WildFire were found to contain malicious code or behavior. Of note as well is that advanced or nation-state-sponsored adversaries are just as likely to use phishing attacks as a profit-driven cybercriminal. Much like the examination of portable executables, this is a significant percentage of malicious activity occurring over email and, in general, should be a cause for great concern.

What does this mean?

90 percent of all laptops and desktop computers still consist of various flavors of Microsoft Windows, and due to the lack of vulnerabilities to exploit when using portable executables to launch an attack, all of these systems are, in essence, vulnerable. Automated preventative measures must be deployed as a first line of defense before a user is given the potential opportunity to launch an unknown and possibly malicious executable file. Preventatives measures could include technology such as URL filters, file type filters (such as warning users before downloading an executable, or outright blocking them), malware sandboxes, or other endpoint technologies.

These technologies are also essential when it comes to phishing attacks, as, historically, users have been found to be unable to fend for themselves when it comes to social engineering-type attacks. Due to the prevalence of email as a communication method between users, unlike PEs, email cannot simply be blocked. Whitelisting is not a valid tactic either as there are absolutely legitimate reasons why a user may need to contact another user, who is not in a whitelist, via email or receive email from a user who is not whitelisted. This leads us to two potential solutions to reduce the attack surface: automated preventative measures using technology, and user education.

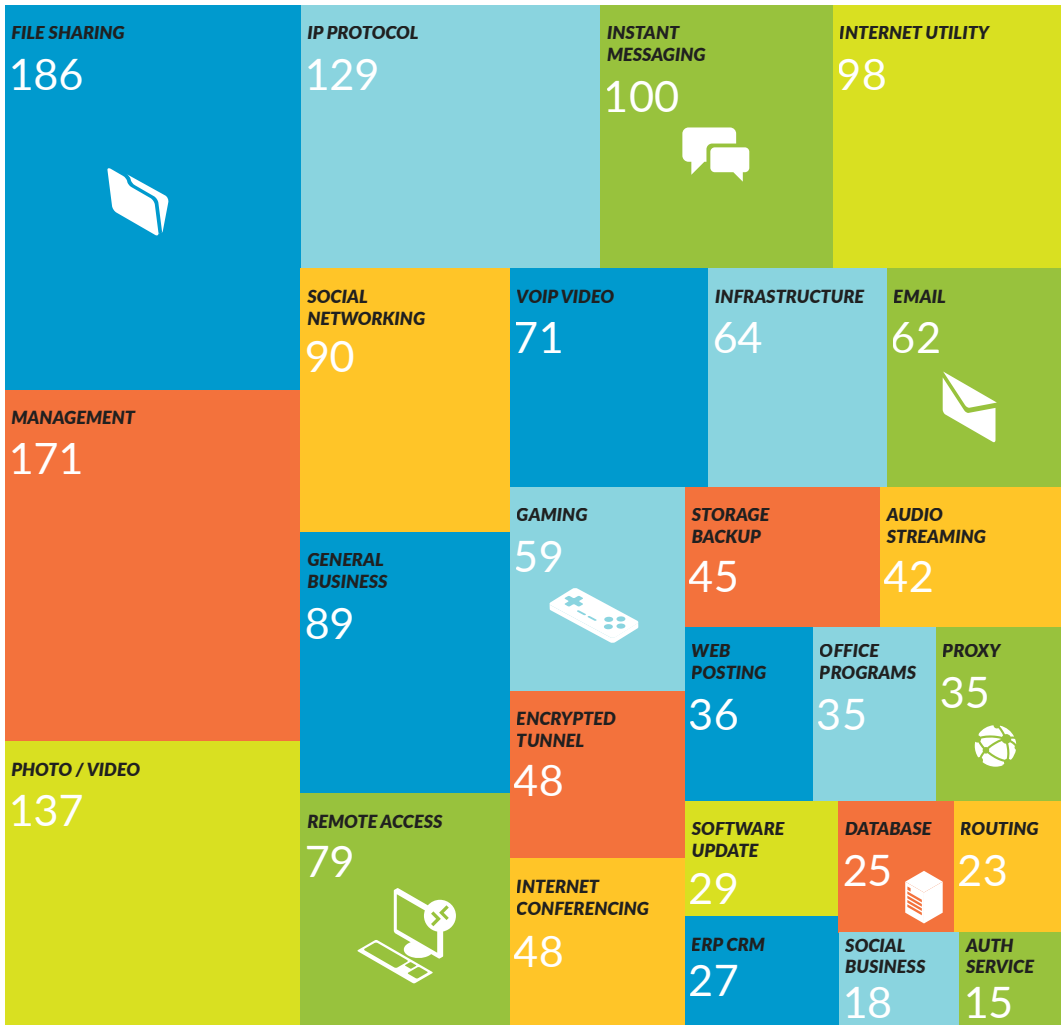
Global Application Usage Snapshot

The rise of applications in the business environment is nothing new. We continue to see more applications being used by more people on a continual basis. When looking through our data, a few key facts stood out: the categories of applications that were being used most often and the sheer number of applications within those categories. Below, you can find the number of application variants in use on a global level, with individual regional breakdowns by application subcategory and the top 25 applications found in the Appendix at the end of the report.

Highlights:

- 10% of all applications in use are file sharing, which could represent potential data security risk for organizations, for a total of 186 applications.
- 137 photo video applications, meaning users are accessing a myriad of often non-work related applications from corporate devices, which could impact productivity or deliver malware, or nearly 8% of all applications.
- 4.5% of all applications are remote access, and as we saw earlier in this report, can present a major security risk, for a total of 79.

Total number of applications per subcategory



The (re)Rise of Macro Malware

In 1995, the first macro-based malware, WM/Concept, was unleashed upon the public and began the initial wave of macro-based malware targeting the Microsoft Word® and Excel® applications. Twenty years later, adversaries appear to have rediscovered macro-based malware and are using it as an effective and efficient attack vector against users.

What is a macro?

Macros were originally developed for the Microsoft Office® suite as a way to automate repetitive tasks or share tasks between different users. The system was designed so that a user could use a simple feature to record a repetitive task, which would then automatically be transcribed into a language known as Visual Basic for Applications (VBA). The macro automated the task and the VBA code could then be shared with other users.

While the intentions of macros in Microsoft Office documents were altruistic, the unfortunate side effect was the creation of an easy-to-use and effective vehicle for malicious code.

Unfortunately, macros were not designed with security in mind; functionality was the main goal and macros allowed users to be more productive by speeding up repetitive tasks. While the intentions of macros in Microsoft Office documents were altruistic, the unfortunate side effect was the creation of an easy-to-use and effective vehicle for malicious code.

The most famous and well-known macro-based malware was the Melissa virus in 1999. It was distributed within a Word document that would gather the first 50 entries from a user's address book and then mail a copy of the macro-infected Word document to each entry via Microsoft Outlook®. Once the recipients opened the document, the cycle would continue ad nauseam. Due to the sheer, overwhelming number of infected systems attempting to send out emails in a much smaller Internet, the Melissa virus placed many major email servers into a denial-of-service state, causing significant impact due to loss of productivity and remediation actions needed.

Where are we now?

In response to the Melissa virus event and other macro malware, Microsoft put multiple mitigations in place to prevent the spread of macro-based malware. In Office 2003, only digitally signed macros could be run by default. In Office 2007, the letter "m" was appended to the usual Office file extensions (.docxm, .xlsxm, .pptxm) to signify that the file contained a macro. Finally, in Office 2013, macros were simply turned off by default, showing users a notification if a macro was embedded in the document they had opened. The actions taken by Microsoft significantly reduced macro-based malware infections and, in turn, reduced the popularity of macro-based malware usage by adversaries.

No good deed goes unpunished, however. In the last decade, as the Internet surged in popularity and necessity, a generation of users now exist who have never used macros or are even aware of what they are due to the dormancy of macros, in general. Users have a tendency to have a singular goal in mind, which is to accomplish the given task at hand. This causes users to ignore warnings or pop-up messages indicating potential danger ahead because, to them, these buttons and dialogues are simple barriers to their productivity. The lack of awareness and a focus on getting to the user's desired content or task has led to a sudden resurgence in the usage of macro-based malware as users unwittingly are enabling macros in Office documents more and more often.

The two most observed malware families delivered via macro abuse are the Dridex and Dyre malware families. In the timeframe of this report, 10.2 percent of all activity flagged as malicious involved these malware.

Dridex[4]

Dridex is a banking Trojan descended from the GameOver Zeus family of malware. Its functions are extremely similar to the well-known GameOver Zeus variants such as Cridex[5], targeting online banking credentials and containing configurations to mimic logins for financial institutions. Dridex differs from its malware relatives, however, in the fact that it utilizes macro-embedded Office documents to load itself onto potential victim hosts, where it then begins harvesting banking credentials. Well over 99 percent of Dridex sessions were delivered over various email protocols or web browsing.

Dyre/Upatre

Upatre is the name of the malware downloader, generally delivered via a macro-based malware Office document, which then retrieves Dyre (Dyreza), a banking Trojan similar in function to GameOver Zeus and its variants. In addition, Upatre utilizes the Microsoft Outlook email client to send itself out to additional victims, effectively worming its way across the Internet. As with Dridex, over 99 percent of these sessions were over various email protocols of web browsing.

99 percent of these sessions were over various email protocols of web browsing

What does this mean?

Although extremely numerous and popular at this time, both Dridex and Dyre/Upatre are fairly easy to prevent from entering an organizational environment, due to the usage of simple delivery mechanisms, such as a file attachment to an email or an email containing a link to a suspicious file. Still, examining the sheer volume of macro-based malware demonstrates that macro-based malware is a real threat to enterprises. Organizations may need to begin including specific user education on macros, explaining what they are, what they do and, lastly, what users need to be aware of to prevent malicious activity from occurring.

[4] http://researchcenter.paloaltonetworks.com/2014/10/dridex-banking-trojan-distributed-word-documents/
[5] https://blogs.mcafee.com/mcafee-labs/banking-malware-dridex-arrives-via-phishing-email

Weaponization of World Events

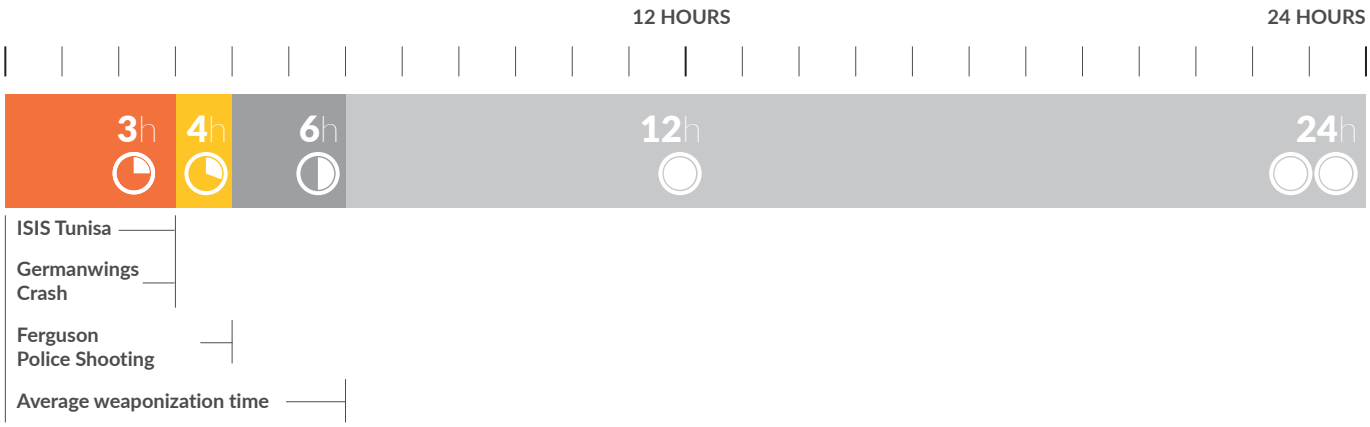
Abuse of current events in cyberattacks is not a new discovery; weaponization of regularly scheduled world events such as the Olympics or the FIFA World Cup is extremely common and something to be expected when defending our organizations. As the world gets more and more connected, however, and with the continued surge of social media as a valid news outlet, world news is traveling faster than ever; thus, an ever-increasing variety of lures to weaponize are available at the adversary's fingertips.

Why do these work?

Humans are by nature curious creatures. In the mythology of Pandora's box, the first woman, Pandora, is given a sealed box by the Greek gods, with strict instructions never to open it. Curiosity comes over Pandora, however, and she eventually does open the box. Unfortunately, the box contained death and all the other evils that would eventually befall mankind. Much like Pandora, users, even if given strict instructions never to open unknown files or email messages, will, at some point, be overcome by curiosity and do exactly that. The main issue lies in the fact that users are not faced with a single Pandora's box, however; they are constantly faced with a barrage of Pandora's boxes and other threats, any of which may be the single point of entry an attacker needs to compromise an organization's infrastructure.

Examining the time delta of weaponization

Several world events were examined for evidence of weaponization, and generally, any given world event widely reported in news outlets was found to be weaponized within six hours on average, several even within three hours.



Ferguson Police Shooting

On August 9th, 2014, the fatal shooting of Michael Brown by a police officer sparked significant unrest and demonstrations in the town of Ferguson, Missouri. The unrest continued for months, culminating with continued protests after the announcement of the chief of police's resignation on March 11th, 2015. In the early hours of March 12th, 2015, two police officers were shot outside a Ferguson police station.

As news outlets began to report on this story, in roughly ***four hours*** time Palo Alto Networks observed an email pass through the WildFire cloud using the headline of an article in the Washington Times as the subject line using a spoofed Washington Times email address. The email contained a file attachment which was properly identified as malicious.

ISIS Tunisia Attack

On March 19th, 2015, the Wall Street Journal posted an article on their website regarding the terrorist group Islamic State taking responsibility for a deadly attack on a museum in Tunisia's capital.

Within ***three hours*** of the initial reporting, Palo Alto Networks observed an email pass through the WildFire cloud using the exact same subject as the title of the news article, utilizing a spoofed Wall Street Journal email address. The email contained a malicious attachment identified as part of the Dyre/Upatre email worm family.

Germanwings Crash

On March 24th, 2015, Germanwings Flight 9525 crashed in the French Alps, killing all 144 passengers and six crew members. On March 27th, 2015, multiple news outlets began to report that the co-pilot may have had hidden mental illness and crashed the plan deliberately.

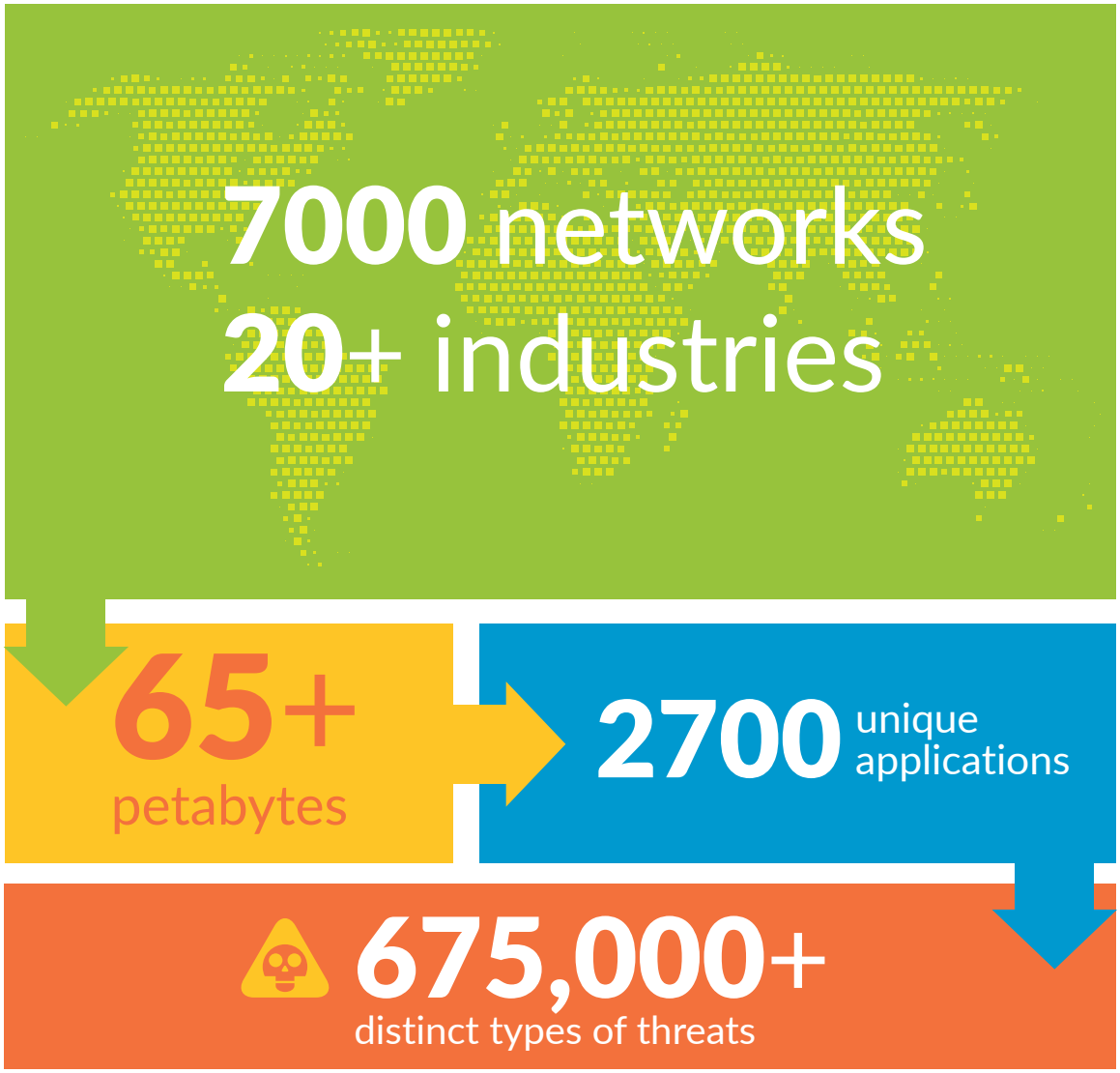
In less than ***three hours*** of media outlets reporting this story, Palo Alto Networks again observed the weaponization of the event, observing an email with the title of an NBC News article as the subject line being sent to multiple users using a spoofed NBC News email address. The email contained a malicious executable payload which was found to be a part of the Dyre/Upatre email worm family by Wildfire.

What does this all mean?

Threat actors can and will utilize any potential attack vector they can, with no regard for morality. They will prey on our natural curiosity and emotions to easily gain access to a system or to lure us into opening a potentially malicious file. In the sample of world events analyzed, the average time of weaponization from the initial reporting of a world event was thirteen hours with the time to weaponization as short as three hours. These attacks generally used file attachments purporting to be media files or other documents associated with the world event. Users, as well as security organizations, must maintain situational awareness of current events worldwide to understand when and why attacks may occur more often.

Demographics and Methodology

The Application Usage and Threat Report (September 2015) from Palo Alto Networks examined nearly 7,000 networks worldwide over 20 industries during a 12 month time period, consisting of over 65 petabytes of data. Nearly 2,700 unique applications were found on these enterprise networks and over 675,000 distinct types of threats were logged. In addition, we examined data from WildFire via the AutoFocus threat intelligence service, combing through millions of unique malware samples and sessions collected during the same time period.



Summary

From the Palo Alto Networks datasets, including information from over 7,000 networks and the AutoFocus service, it is apparent that the biggest risk to enterprises is the users themselves. Users are constantly faced with a barrage of attacks, both old and new, as well as self-installed, potential points of entry. User education must be an emphasis throughout all organizations, with a trend toward automated prevention systems at every stage of the attack lifecycle and every layer of an organization's infrastructure. This, in combination with the continued emphasis on open and free threat intelligence sharing will allow organizations to take on a proactive, targeted defensive posture. Data breaches are a significant cost to organizations; why not make it costly for adversaries to execute their attacks as well?

Recommendations

1. **Deploy automated prevention systems at all layers of infrastructure that are also able to execute preventative actions at every stage of the attack lifecycle**. The sheer volume of attacks faced by an enterprise network is too significant not to have automated preventative measures in place and rely instead on manual mechanisms. Many of the highly publicized breaches in the last few years have had successful detections of the initial breach, yet due to a lack of automated prevention, adversaries were not able to be stopped before exfiltration and additional damages were incurred.

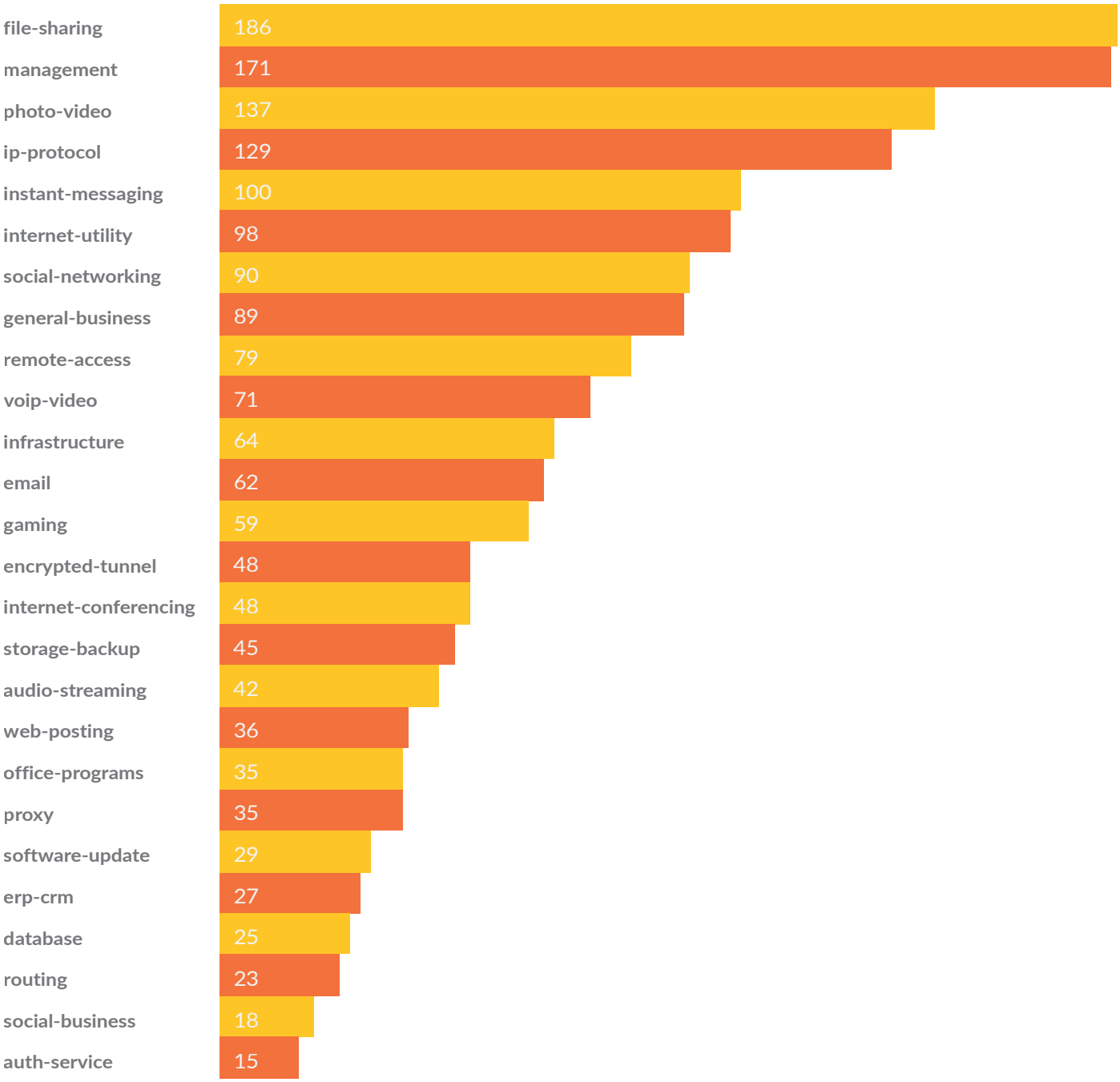
2. **Find the usage policy balance in the organization**. A too-strict usage policy will cause users to become frustrated and find workarounds to their problems. A too-lenient usage policy will increase the attack surface for an adversary and potentially leave too many vulnerabilities in the organization's infrastructure. Organizations must be able to quickly and automatically identify authorized applications and non-authorized applications, and then apply control measures on both.

3. **Maintain situational awareness for not just the cyberthreat landscape, but also world events**. Constantly reacting to security incidents is a zero-sum game; organizations must be able to proactively put preventative measures in place, as much as possible, to be able to concentrate on the truly unknown attacks. Organizations should be constantly gathering and collating data based on intelligence sharing, open source intelligence, or derivations from closed source intelligence.

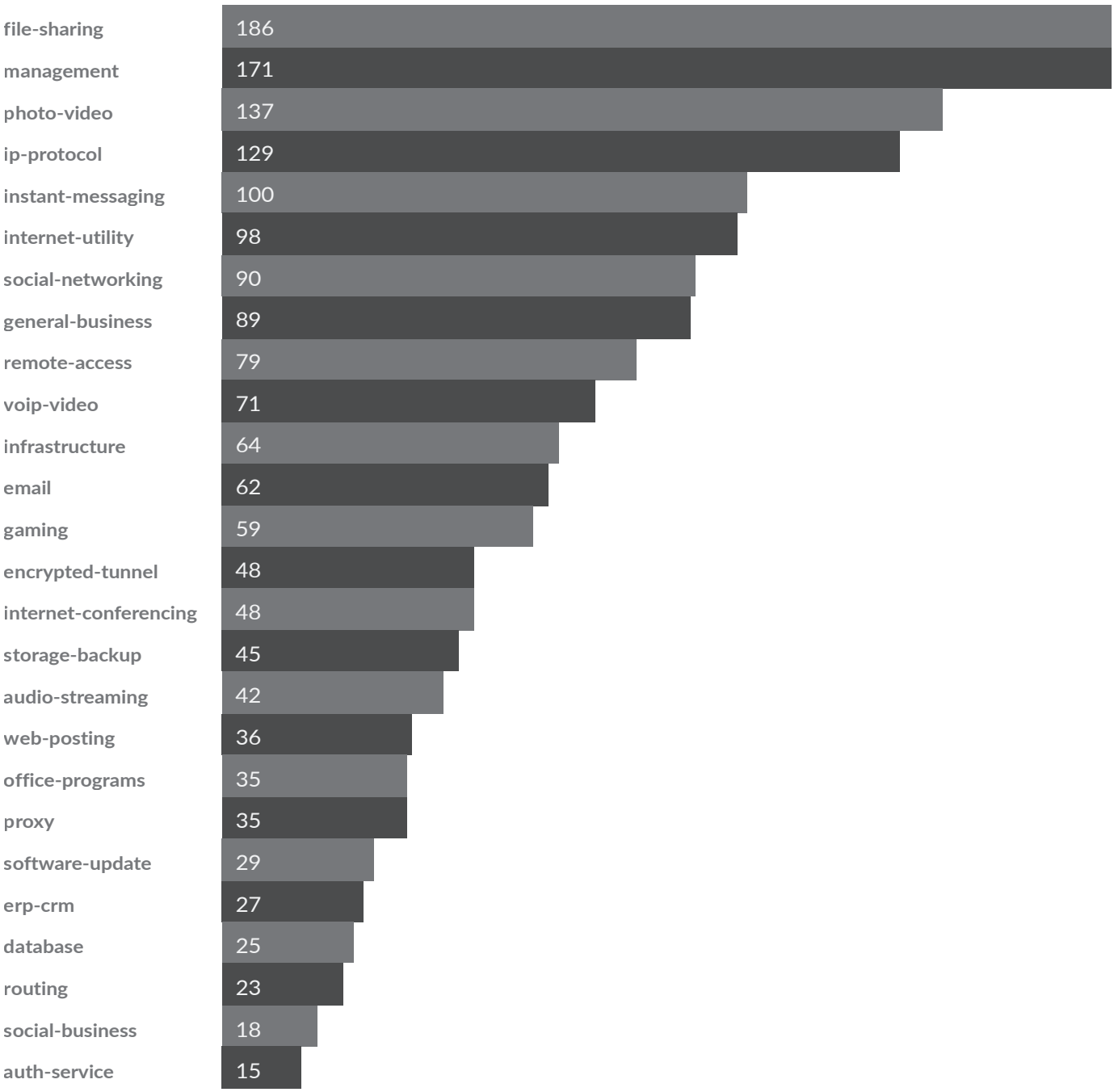
Appendix

The following section contains an overview of application usage. Content is broken down into global and regional categories — and further subcategorized by application session and bandwidth percentage.

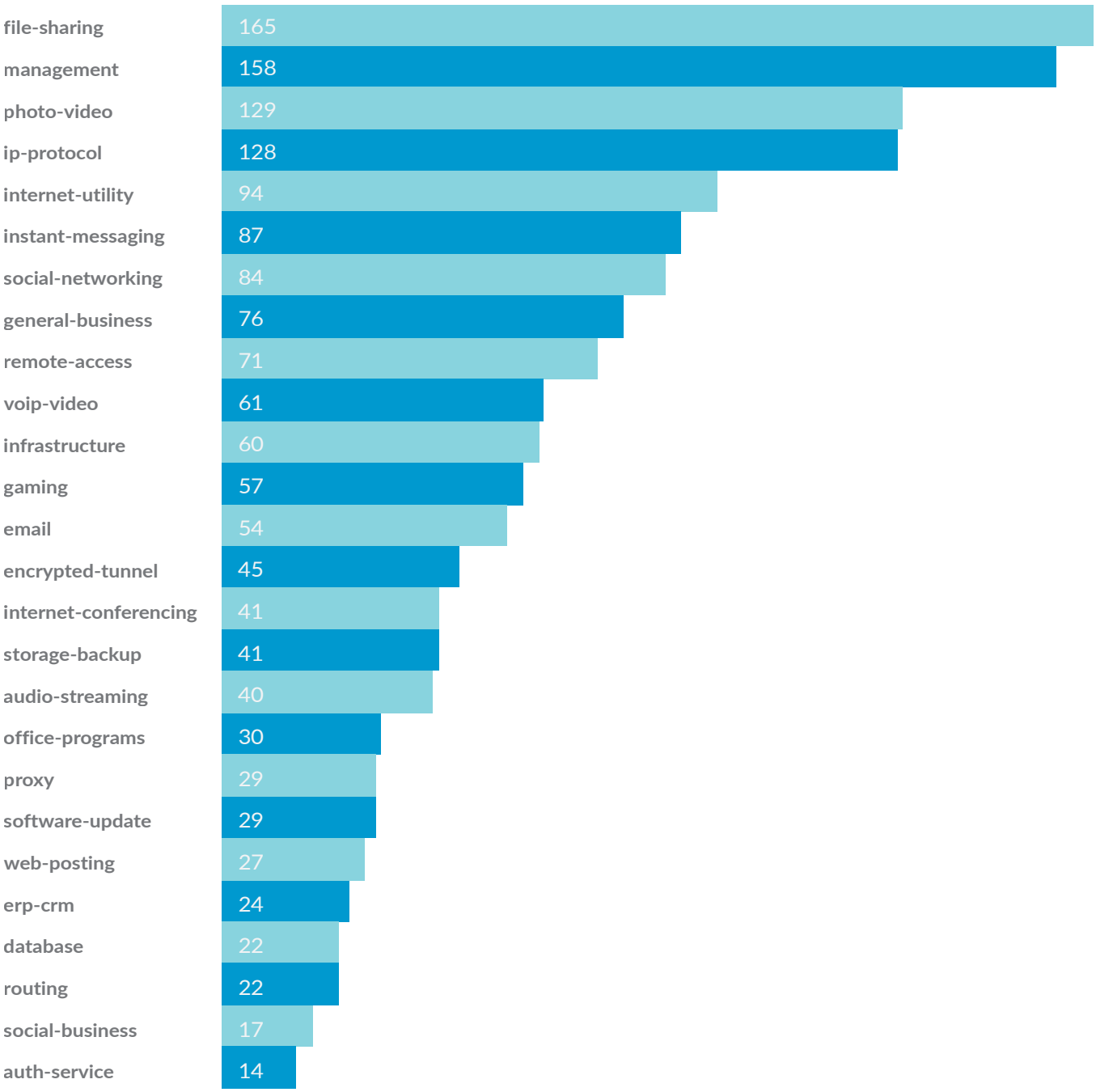
Global Application usage by Subcategory



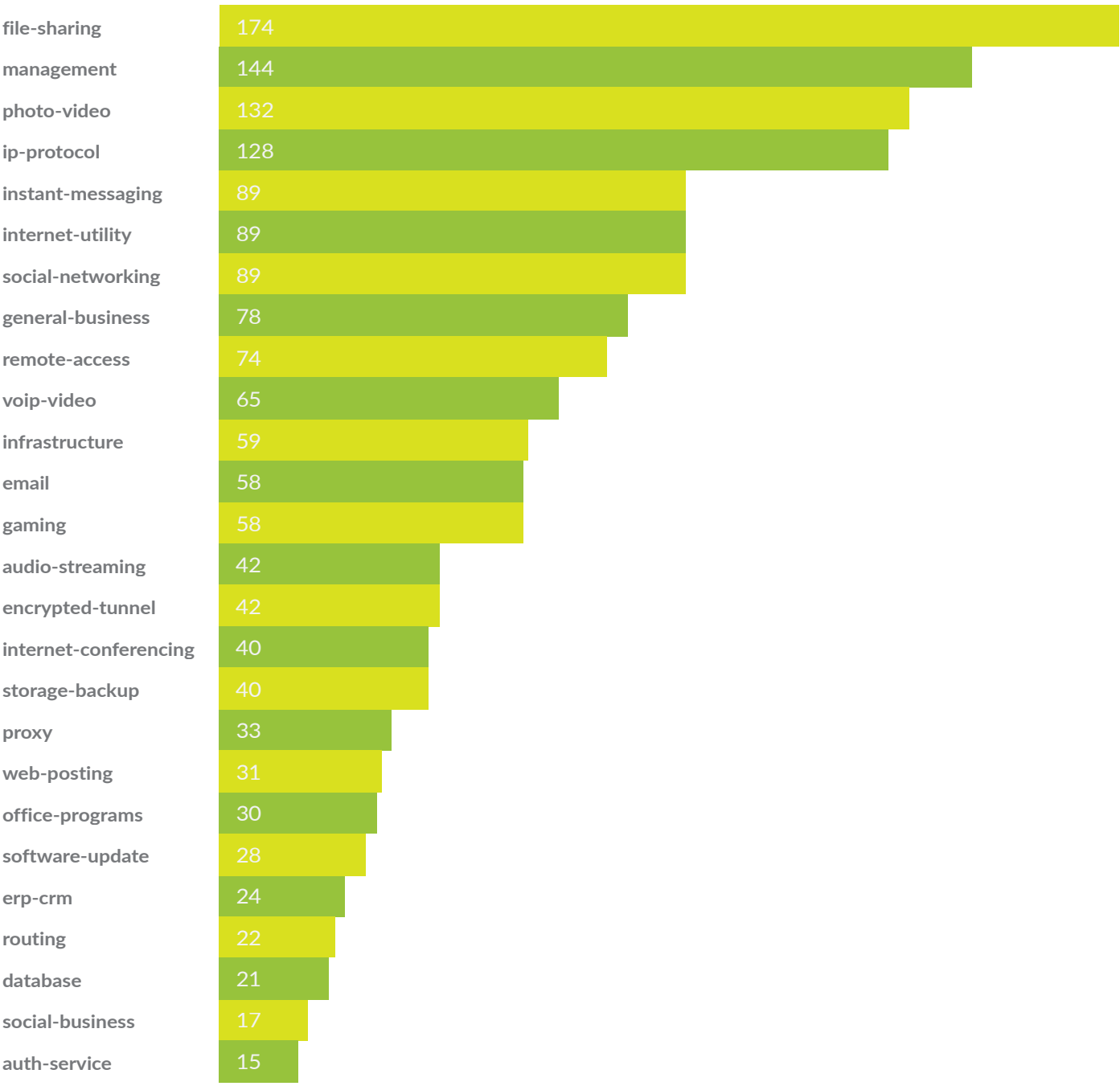
Americas Application usage by Subcategory



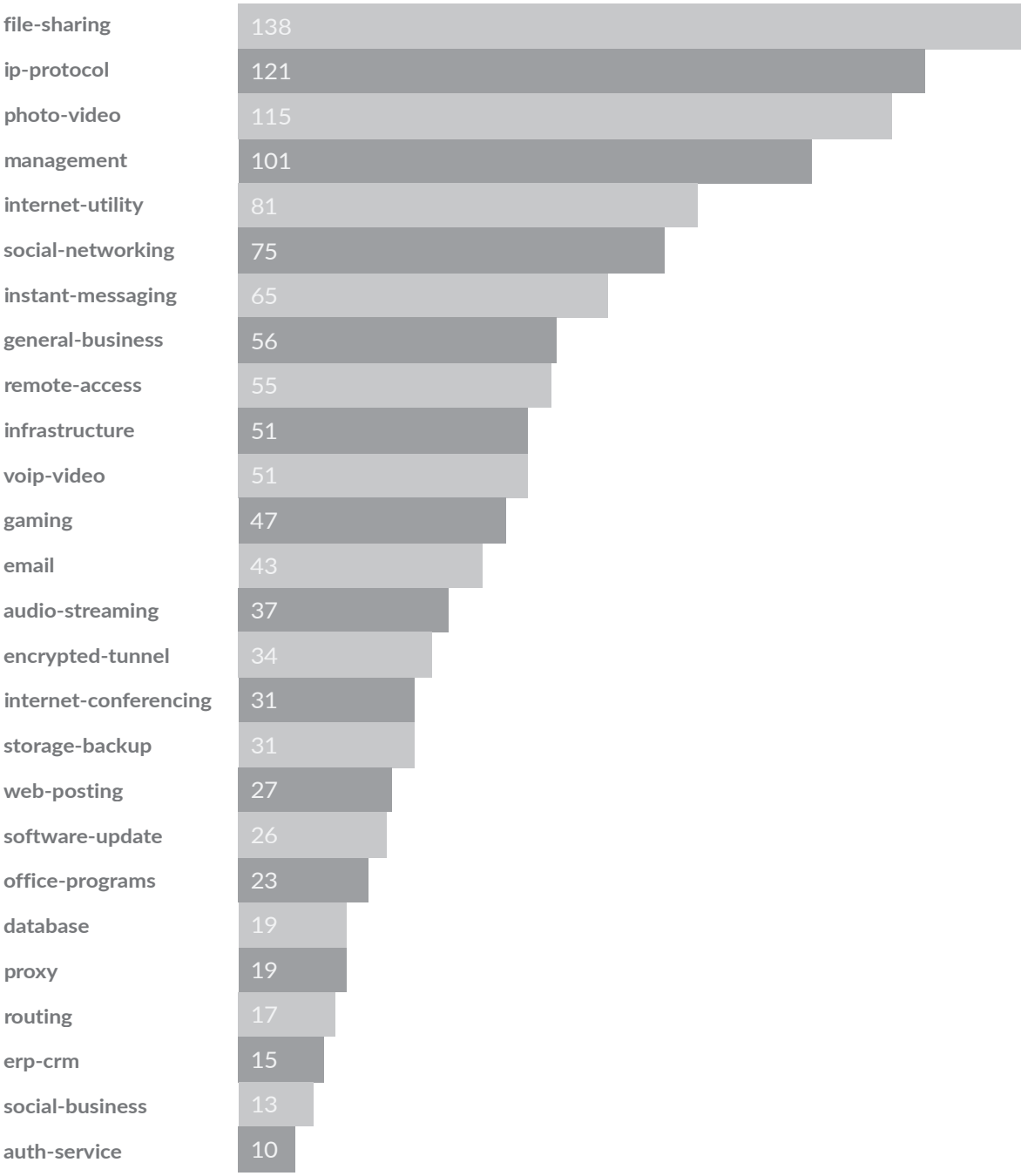
Europe, the Middle East and Africa Application usage by Subcategory



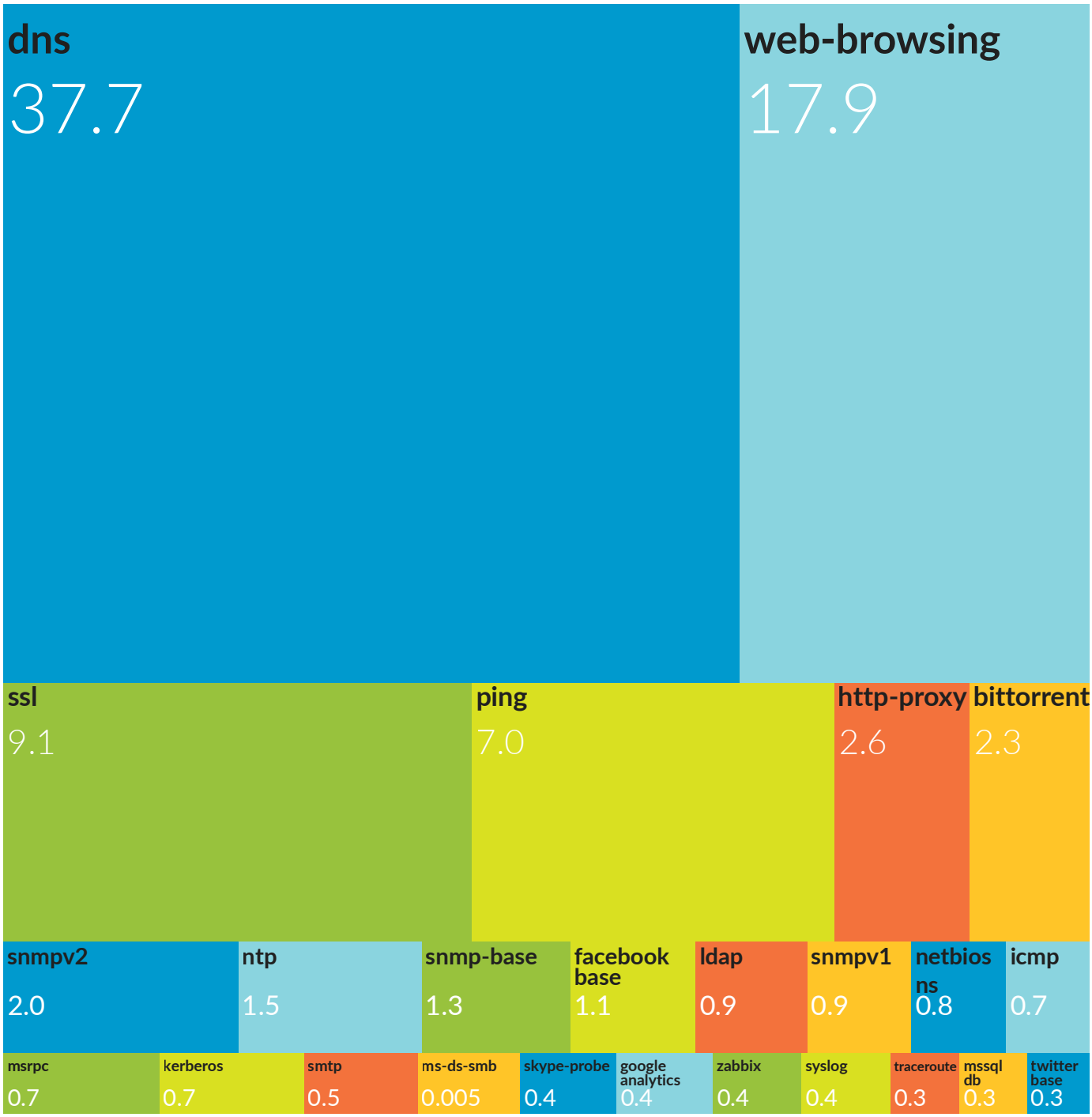
Asia Pacific Application usage by Subcategory



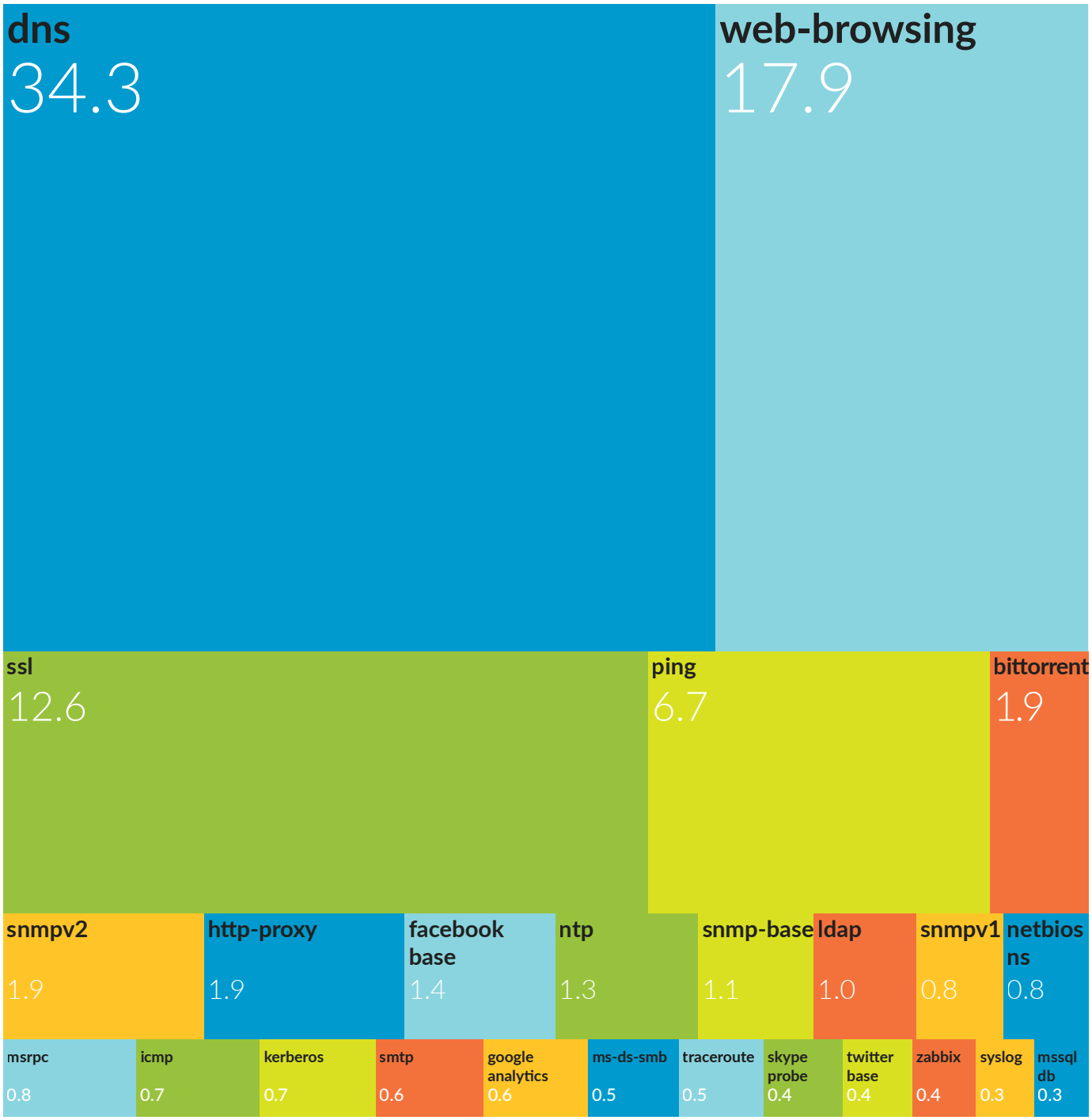
Japan Application usage by Subcategory



Global Top 25 Applications by Session (percent of total sessions)

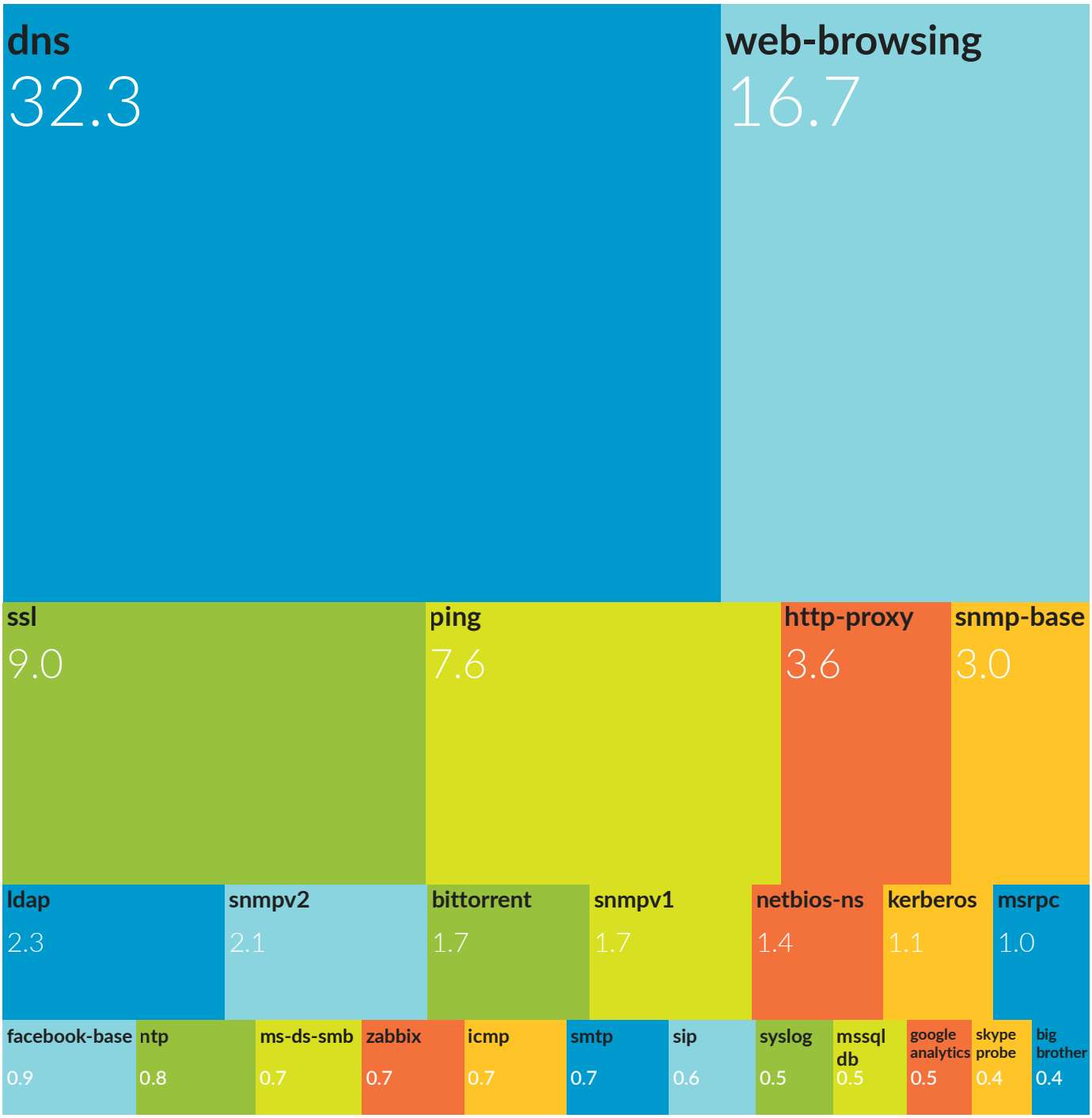


Americas Top 25 Applications by Session (percent of total sessions)

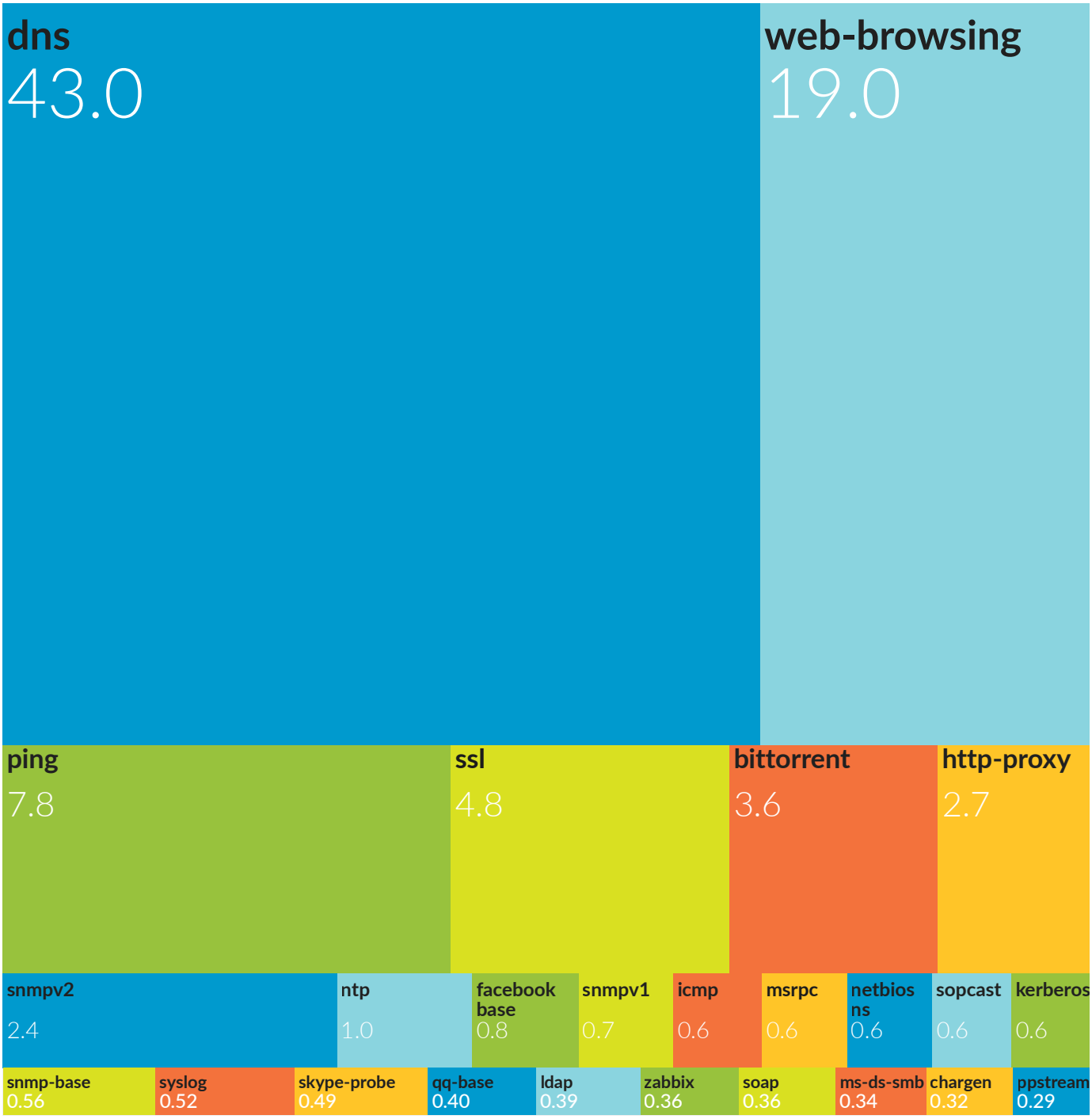


Europe, the Middle East and Africa Top 25 Applications by Session

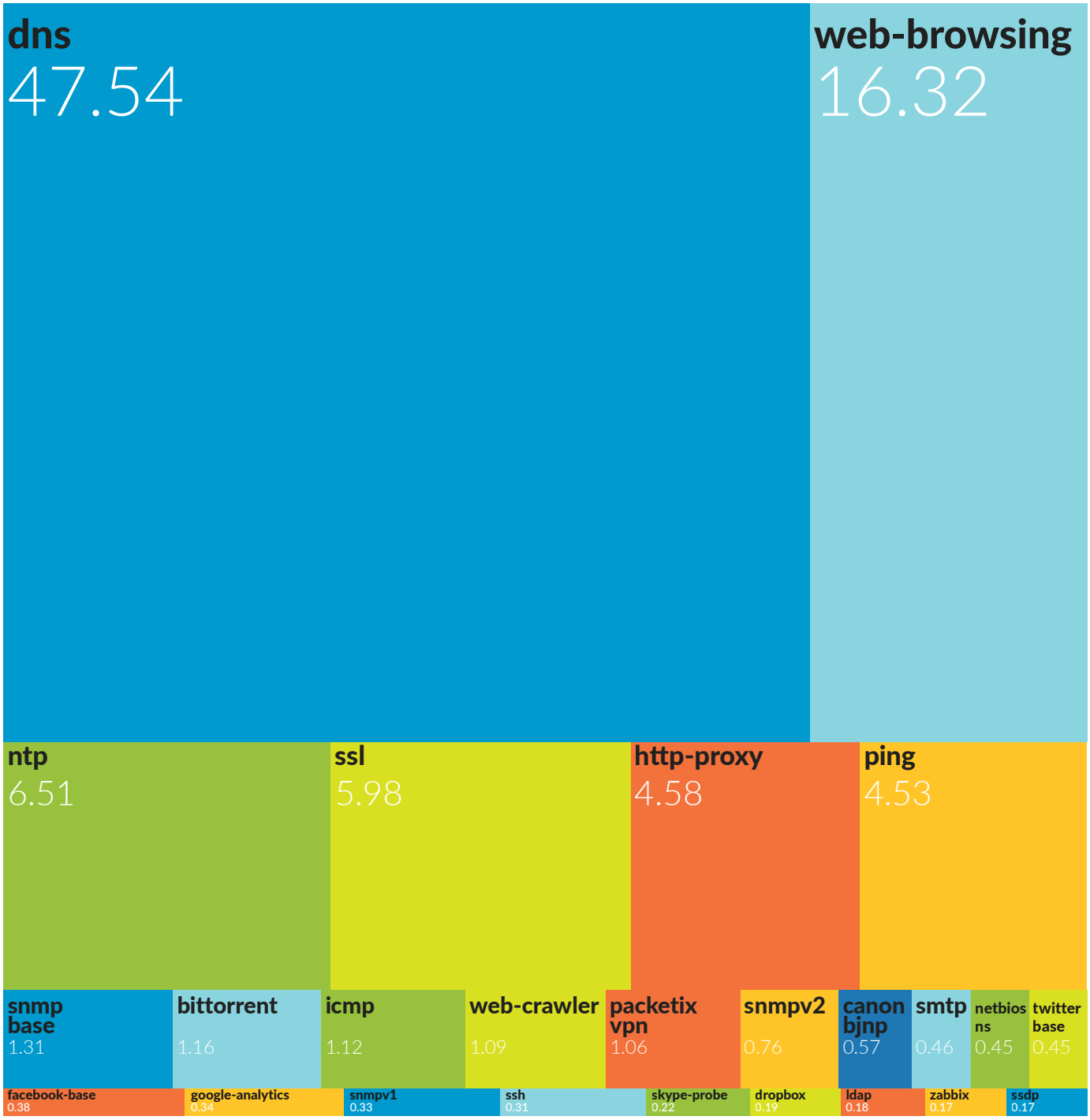
(percent of total sessions)



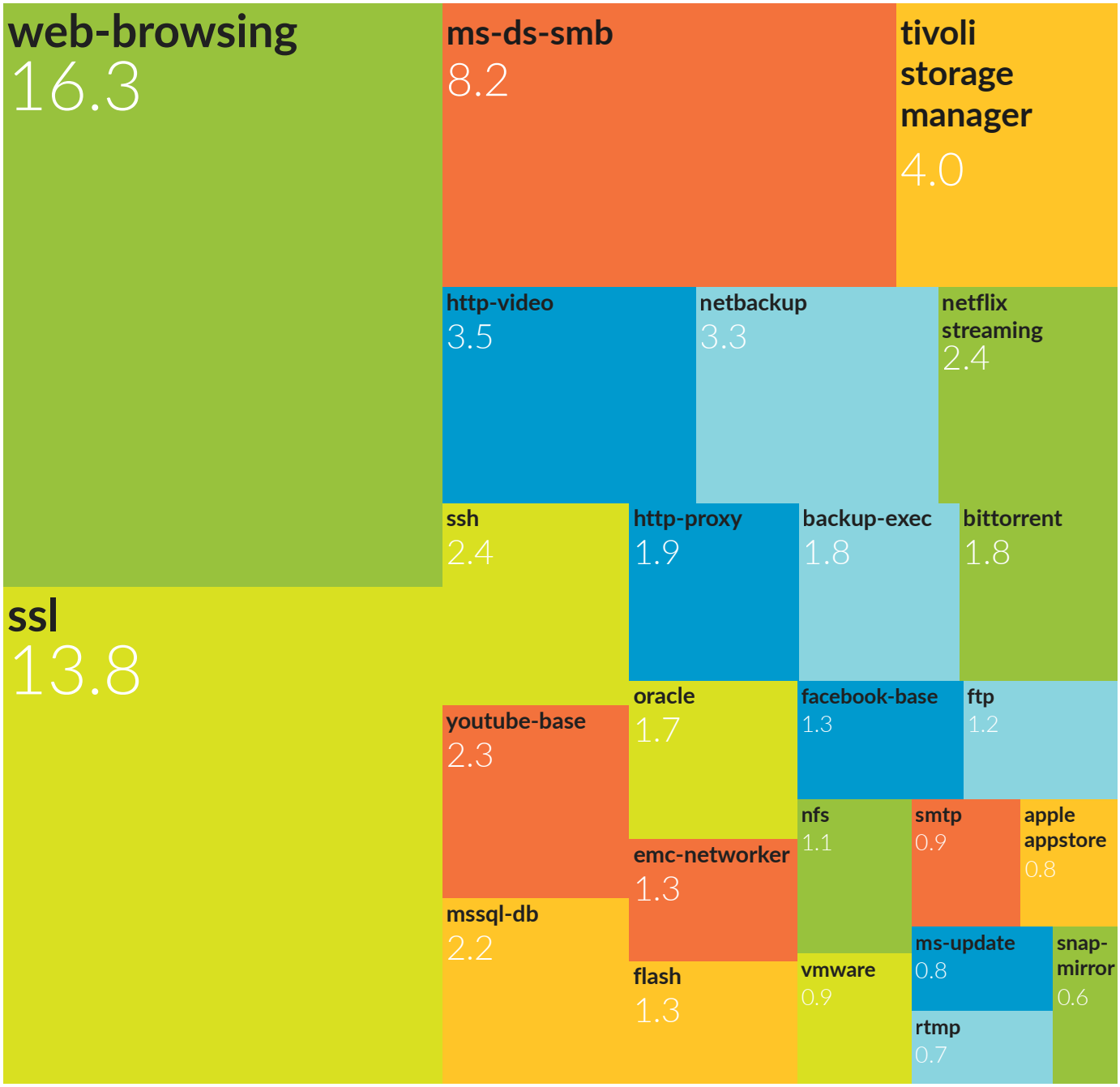
Asia Pacific Top 25 Applications by Session (percent of total sessions)



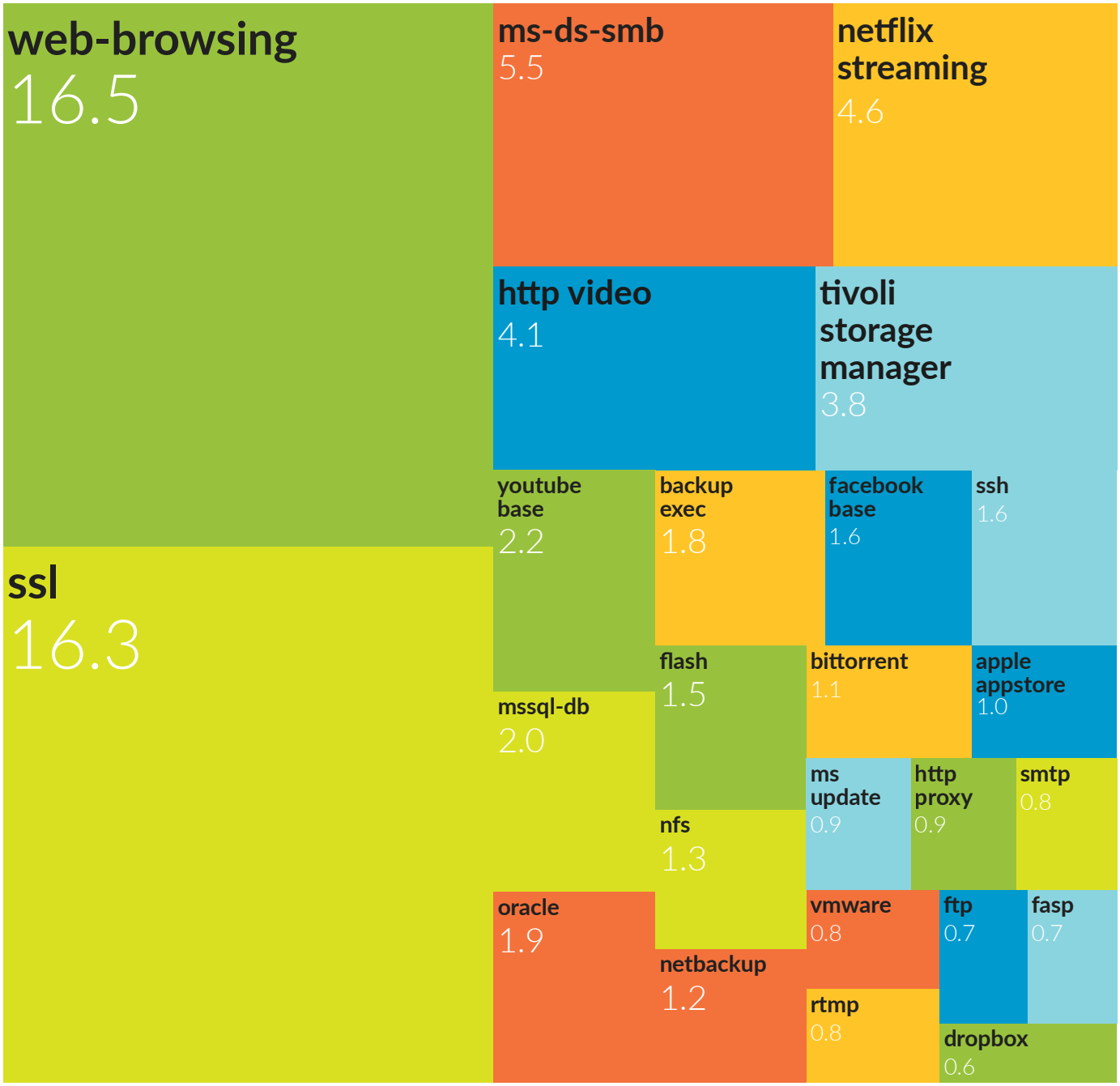
Japan Top 25 Applications by Session (percent of total sessions)



Global Top 25 Applications by Bandwidth (percent of Global bandwidth)

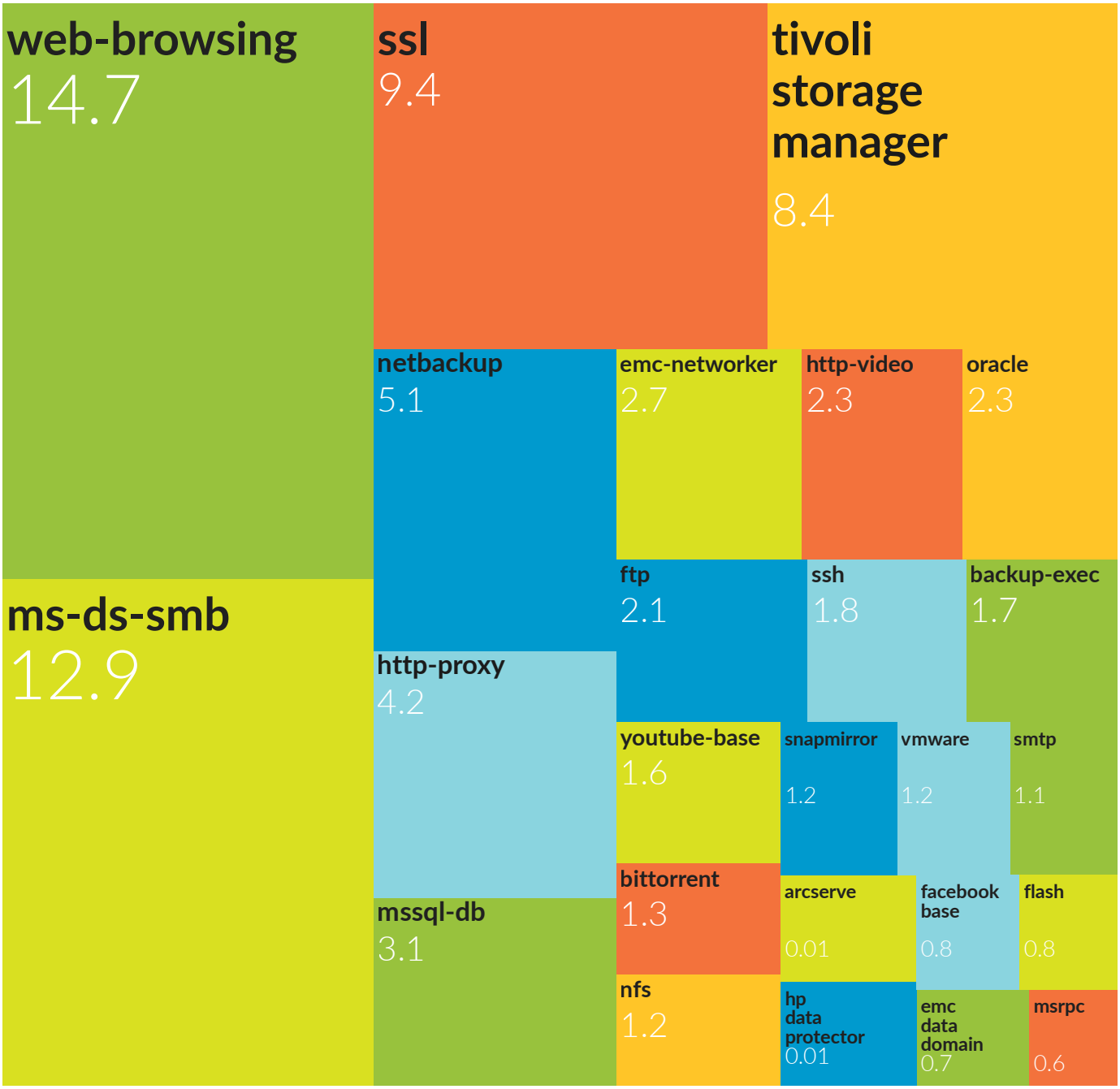


Americas Top 25 Applications by Bandwidth (percent of Global bandwidth)

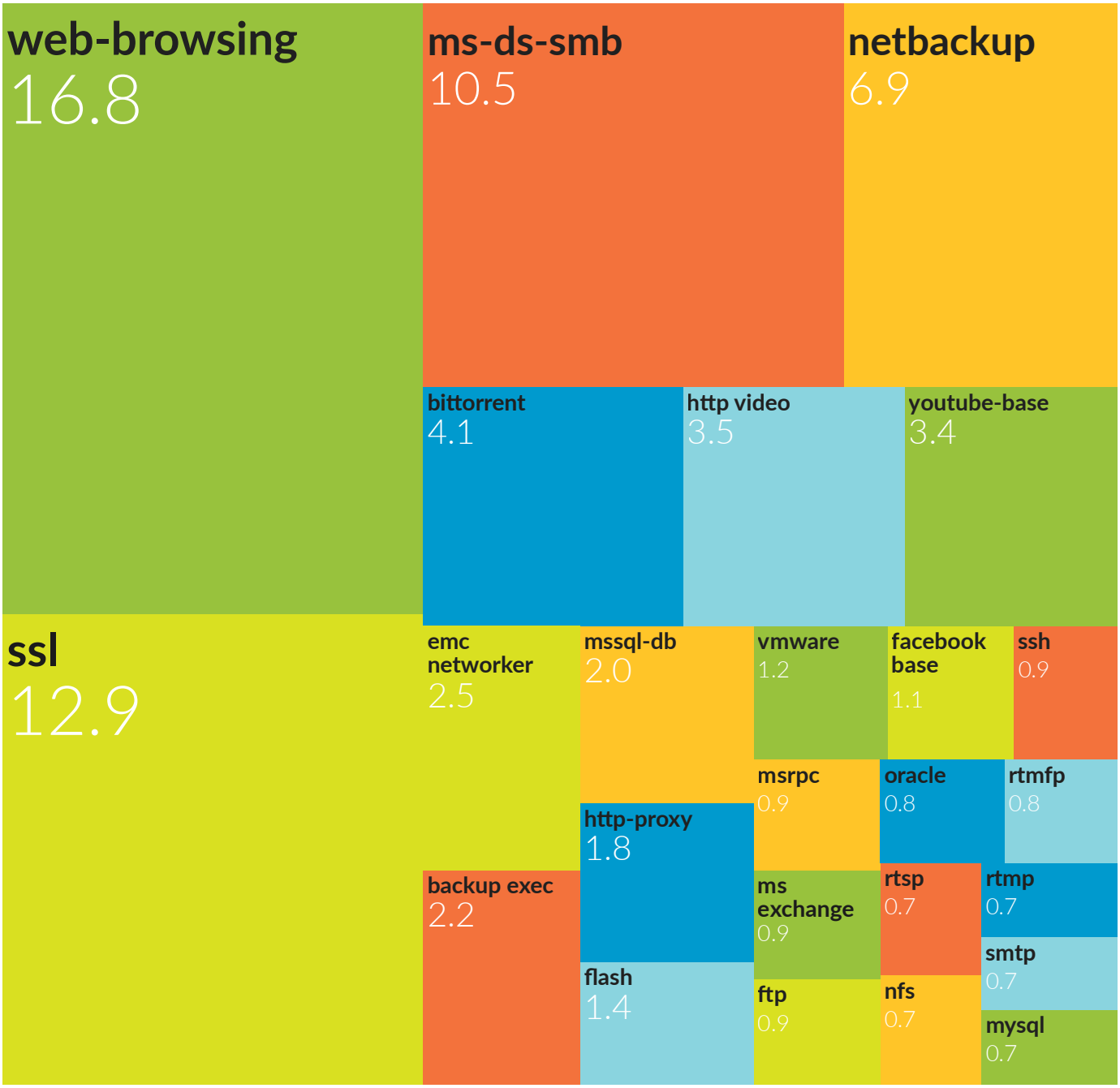


Europe, the Middle East and Africa Top 25 Applications by Bandwidth

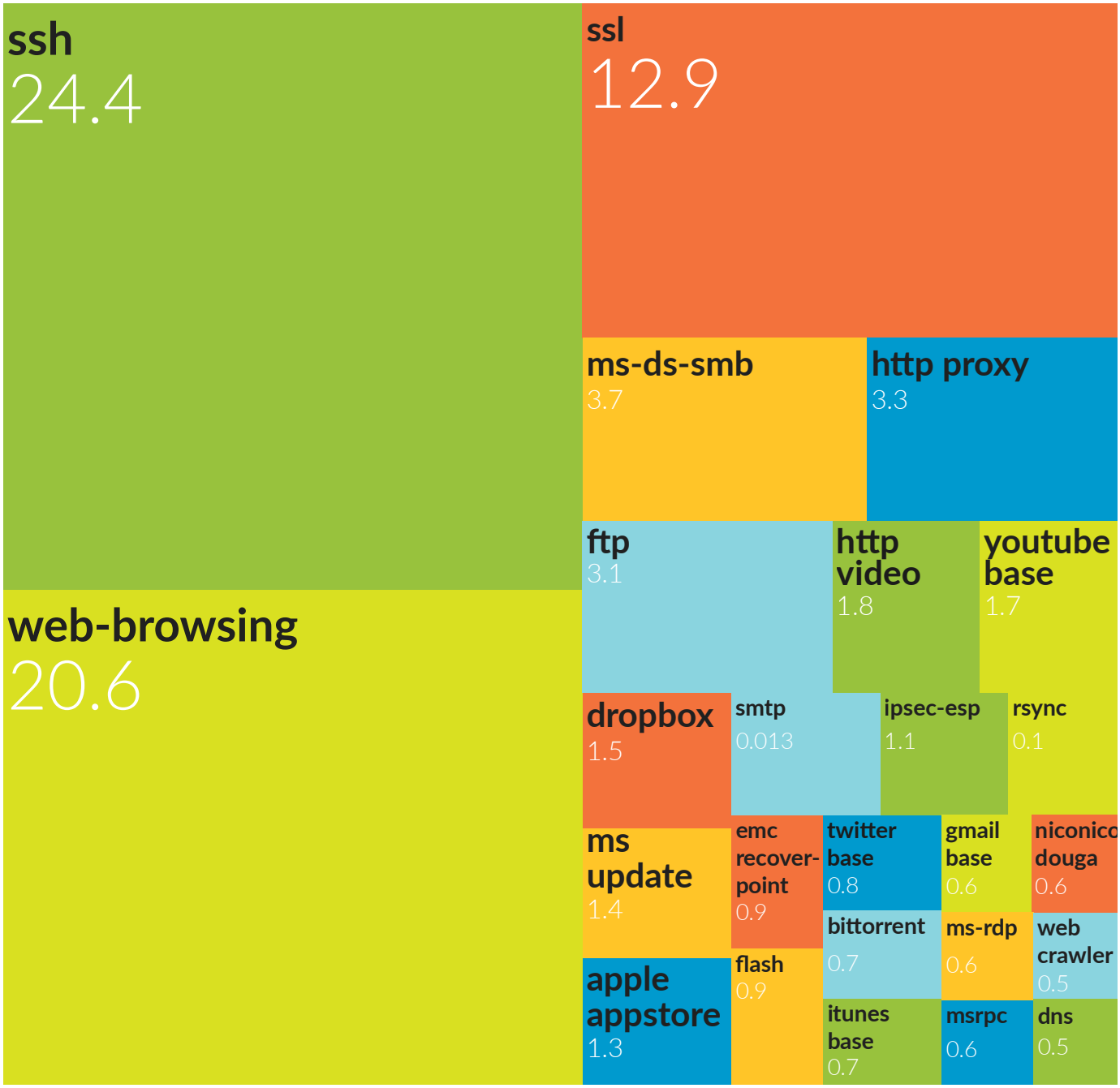
(percent of Global bandwidth)



Asia Pacific Top 25 Applications by Bandwidth (percent of Global bandwidth)



Japan Top 25 Applications by Bandwidth (percent of Global bandwidth)



Palo Alto Networks
4401 Great America Parkway
Santa Clara, California, 95054

+1-408-753-4000 main
+1-866-320-4788 sales
+1-866-898-9087 support
www.paloaltonetworks.com