

ELEVENTH EDITION • JUNE 2014



APPLICATION USAGE AND THREAT REPORT



AN ANALYSIS OF APPLICATIONS AND THEIR LINK TO CYBER THREATS WITHIN THE ENTERPRISE

TABLE OF CONTENTS



Executive Summary	3
Does High Volume Usage = High Volume Threat Activity?	4
Justifying the Business Use Case	5
Code Execution Exploits Dominate Threats in Common Sharing Applications	5
<i>Smoke.Loader Botnet Controller</i>	6
Recommendations for Protection	7
UDP: The Malware Hiding Place of Choice	8
Potential for Proactive Controls	9
Brute Force Attacks Target Business Applications and Services	10
<i>Security Recommendations</i>	11
How Many Applications on Your Network Use SSL?	12
Threats Using Encryption: Hiding in Plain Sight?	13
Has the Heartbleed Risk Come and Gone?	13
<i>Addressing the Heartbleed Risk</i>	14
Summary	15
Recommendations	15
Appendix A: Regional Observations	16
Regional Data Summaries	16
Common Sharing Applications – Regional Observations	17
Business Application Threat Activity – Regional Observations	19
SSL Usage – Regional Observations	19
Demographics and Methodology	20
About Palo Alto Networks®	20

EXECUTIVE SUMMARY

When asked to describe the current cyber threat landscape, one of the more balanced and objective answers might be that threats are “hiding in plain sight.” Today’s advanced cyber threats use applications as their infiltration vector, exhibit application-like evasion tactics, and act as, or use common network applications for communications and exfiltration. One needs to look no further than the recent high profile attacks to support this description. Today’s attacks are hiding in plain sight and use applications such as FTP, RDP, SSL, and netbios to achieve their objectives. These applications were found on nearly every network we analyzed and it’s evident they have now become a favorite vehicle through which attackers can mask their activities.

With this premise as the backdrop, the *Application Usage and Threat Report (June 2014)* from Palo Alto Networks provides a global view into enterprise application usage and the associated cyber threat landscape. We accomplish this by summarizing network traffic assessments conducted across more than 5,500 organizations worldwide between March 2013 and March 2014. This version of the report will analyze the relationship between threats and their application vectors. The most surprising data points being both the diversity of applications displaying threat activity and the high concentration of activity surrounding only a few key techniques.

Key findings include:

Common sharing applications remain a favorite when it comes to the delivery of an attack, but remain low in terms of overall threat activity.

- 19% of all threats we observed were code execution exploits that were delivered across common sharing applications
- Only 5% of all threat activity was seen within these applications

A small number of applications exhibited nearly all of the observed threat activity.

- 94% of all vulnerability exploit logs we observed were found in only 10 applications
- 99% of all malware logs were found in UDP; the majority of which were generated by a single threat

Data reveals that an increasing number of applications can transmit over encrypted channels.

- 34% of all applications (539) we observed can use SSL in some manner. Given the propensity to use applications to mask malicious activity, we have to ask ourselves the following questions:
 - Is SSL in use as a privacy function or evasion tactic?
 - How many applications on our network can use SSL and do you know which ones they are?
 - Finally, what is your confidence level that they are free of malicious activity?

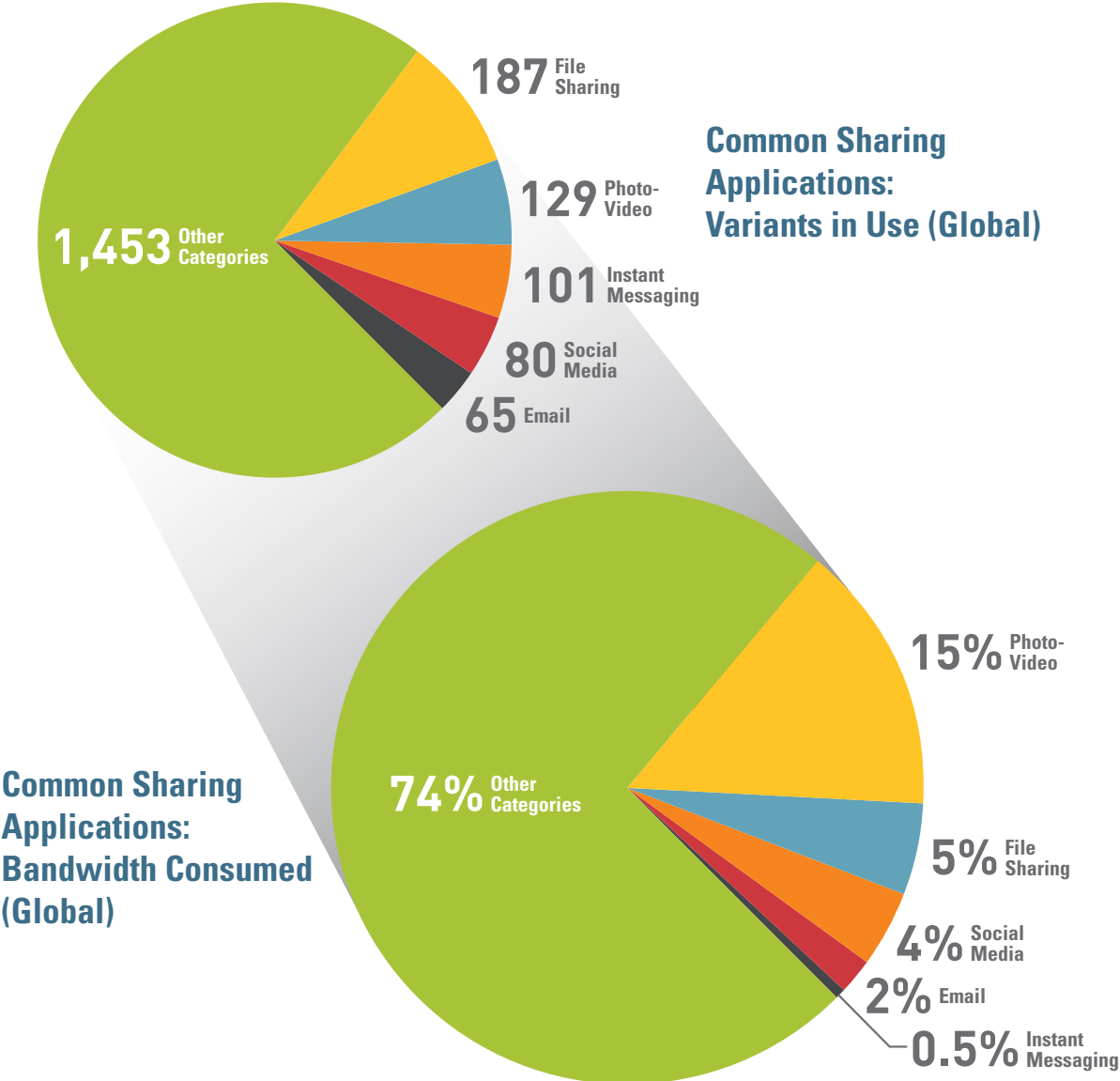
The application and threat patterns discussed within this report place an appropriate emphasis on the need to continually detect and assess the applications traversing your network. Too often, the focus is directed towards noisy, higher profile applications while in reality our findings demonstrate that it’s actually the quiet “workhorse” applications that are in the greatest need of protection.

DOES HIGH VOLUME USAGE = HIGH VOLUME THREAT ACTIVITY?

There is an ongoing assumption that common sharing applications are the source of all security challenges that organizations face today. As with most assumptions, the data shows that this is only partially true. Common sharing applications, defined as email, instant messaging, social media, file sharing, and video, were heavily used

across all global regions. This class of applications represented 27% of all applications found, consumed 26% of all bandwidth, and was directly linked to the delivery of 32% of all attacks. The threat activity however was disproportionately low, at roughly 5%.

FIGURE 1: Common sharing applications in use and bandwidth consumed.



JUSTIFYING THE BUSINESS USE CASE

Before discussing the threat activity within common sharing applications it's important to have a brief conversation regarding the business case justifying the high number of variants within each group found in use. For example, within the group of file sharing applications, an *average* of 25 variants (12 browser-based, 5 peer-to-peer and 8 client-server) were found on 93% of the 5,500+ networks analyzed.

COMMON SHARING APPLICATION FREQUENCY OF USE

What is your exposure relative to the business and security risks?



FILESHARING

187 variants found across
93% of all networks
Average of 25 per organization



VIDEO

129 variants found across
91% of all networks
Average of 30 per organization



SOCIAL MEDIA

80 variants found across
91% of all networks
Average of 29 per organization



EMAIL

65 variants found across
97% of all networks
Average of 15 per organization



INSTANT MESSAGING

101 variants found across
89% of all networks
Average of 18 per organization

At most, any one organization may “officially approve” the use of a handful of each application type, but it is unlikely that there is justification for 25 different file sharing or 30 video applications on *each* network. In many cases, users are oblivious to the business or security risks associated with the use of common sharing applications. As a result, they've created a new standard that assumes they can use any application at any time. To the security professional, the security and business risks are real and include:

- Loss of corporate data and copyright violations – inadvertent or purposeful.
- Cyber threat introduction as a target, propagation channel, or exfiltration vector.
- Regulatory compliance violations – is the use of the application allowed?
- Bandwidth impact – how does personal use of video or file sharing applications impact the VoIP applications?

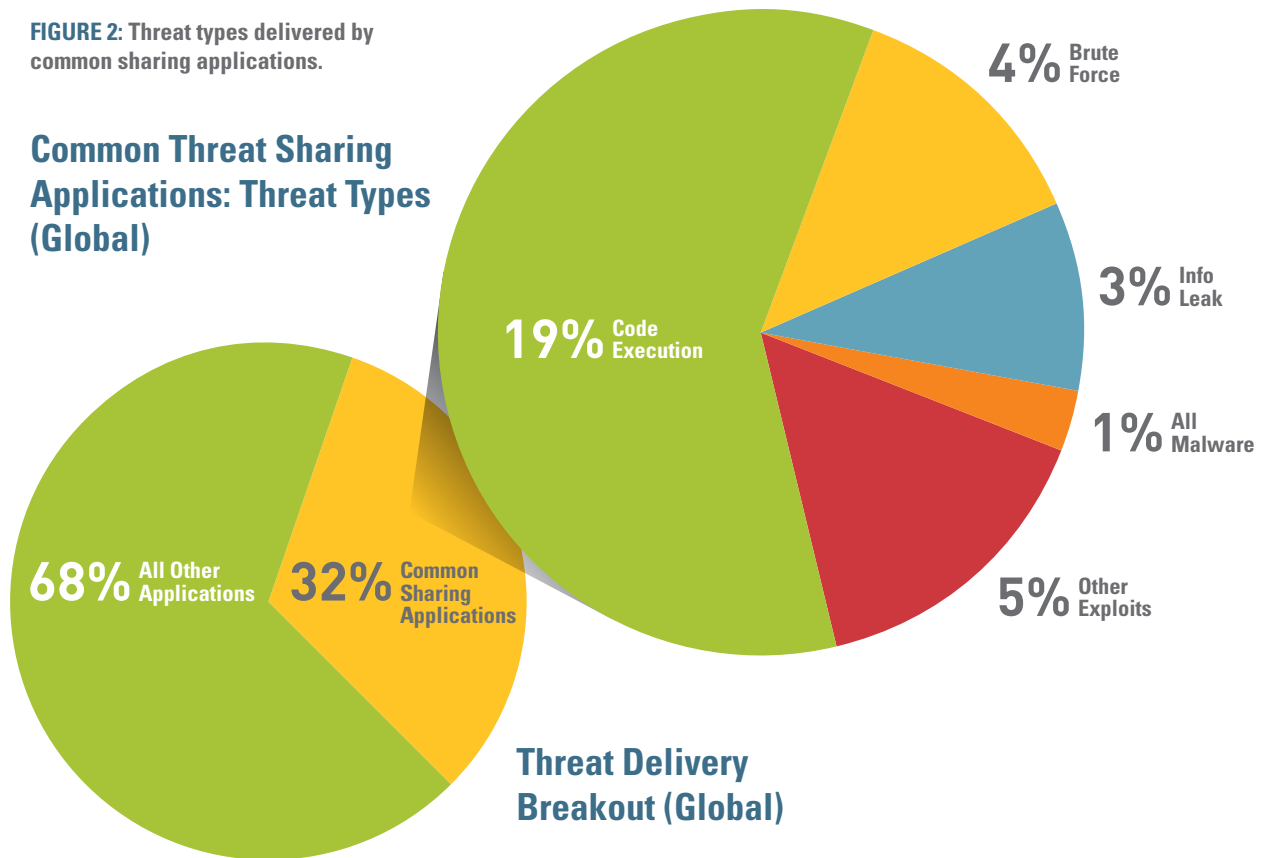
CODE EXECUTION EXPLOITS DOMINATE THREATS IN COMMON SHARING APPLICATIONS

Common sharing applications delivered 32% of *all* threats found (exploits and malware), and surprisingly, 19% of *all* code execution exploits found. Email, file sharing, and social media were the top threat delivery mechanisms, yet the threat activity (communications and malicious activity) observed within these application categories was disproportionately low, at roughly 5% of all activity.





As shown in figure 2, within threats delivered across all applications, 19% were code execution exploits found within common sharing applications. Code execution exploits are vulnerabilities within an application that allow attackers to execute their payload. Perhaps via a drive-by download, or by enticing the user to open a malicious PDF, or a Microsoft Word file.

FIGURE 2: Threat types delivered by common sharing applications.

Common Threat Sharing Applications: Threat Types (Global)



TOP COMMON SHARING APPLICATION EXPLOIT DELIVERY VECTORS

 <p>EMAIL SMTP, POP3, IMAP, Microsoft Exchange</p>		<p>FILESHARING FTP, WebDav</p>
 <p>SOCIAL MEDIA Facebook, Twitter, LinkedIn</p>		<p>INSTANT MESSAGING Microsoft Lync</p>

The initial payload may be the first phase of the attack, and one that allows the attacker to establish control over the endpoint. That initial endpoint infection is typically not the target, but the network resources are – and once on the network, attackers can begin their next phase. Once the endpoint is under control, a second payload is installed that enables attackers to utilize the endpoint for whatever criminal purposes they desire.

Knowing that code execution exploits were the most common type of threat, and that email, file

sharing, and social media were the most widely used delivery mechanisms helps bring clarity to the low activity puzzle. Once attackers have delivered their initial payload, they no longer have need for the application itself. Further clarity can be found by examining how a code execution exploit may be used as part of a multi-phased attack.

SMOKE.LOADER BOTNET CONTROLLER

The threat traffic analysis showed Smoke.Loader botnet controller activity within several applications including Facebook and Twitter. Smoke.Loader can be installed several ways – one of which is via the Blackhole exploit kit which often utilizes several known code execution vulnerability exploits (CVE-2010-0188, CVE-2007-5659, CVE-2008-0655, CVE-2007-5659, and CVE-2009-0927), all of which were observed in SMTP, POP3, IMAP, and web-browsing traffic. Once the Blackhole exploit kit is delivered to the victim’s browser, the attacker gains control of the system and installs the Smoke.Loader malware.

Smoke.Loader enables remote management of the endpoint to perform a range of malicious activities including:

- Download and install (i.e. load) other malware
- Install different files based on the geographic location of the infected system
- Steal passwords for filesharing, instant messaging, and other applications
- Disable antivirus programs
- Proxy the attacker’s traffic through the compromised system, bypassing IP-based authentication systems

In this example, the threat activity is indeed observed within common sharing applications (Facebook and Twitter), but the volume was not significant. This is an excellent example of a multi-phased approach that’s routinely used in today’s cyber attack. In this example, the attack entry-vector was different than the application used as the exit-vector (social media, web-browsing). And in both directions the attacker used applications that are commonly found on most networks.

RECOMMENDATIONS FOR PROTECTION

The fact that known exploits are delivered by common sharing applications such as email, file sharing, and social media makes proactive controls relatively easy – in theory anyways.

1. Ensure all desktop applications are current with security updates from the manufacturers – educate users to say “Yes” to automatic updates. The code execution exploits that allowed the Blackhole exploit kit to be installed are several years old and have actively been patched.
2. If updating the applications is not viable, you should employ an up-to-date IPS and next-generation endpoint protection software to help mitigate the associated risks.
3. Many of these applications transmit over encrypted SSL channels. Consider selectively decrypting and inspecting common sharing application traffic.

FIGURE 3: Smoke.Loader installation and exfiltration process.



UDP: THE MALWARE HIDING PLACE OF CHOICE

It is no secret that modern attackers have become highly adaptable in order to avoid traditional security and that they constantly modify their malware executables in order to bypass existing threat prevention techniques. What is much less understood is that attackers will also heavily modify and customize their communications – not only to confuse traditional security, but also for more functional purposes. One example is the heavy use of UDP by malware creators.

The data shows that many of the 66 botnets we detected in this research used UDP for their command and control channel. The heaviest malware activity was generated by the ZeroAccess botnet, which can be installed in the same manner as Smoke.Loader – via the Blackhole exploit kit.

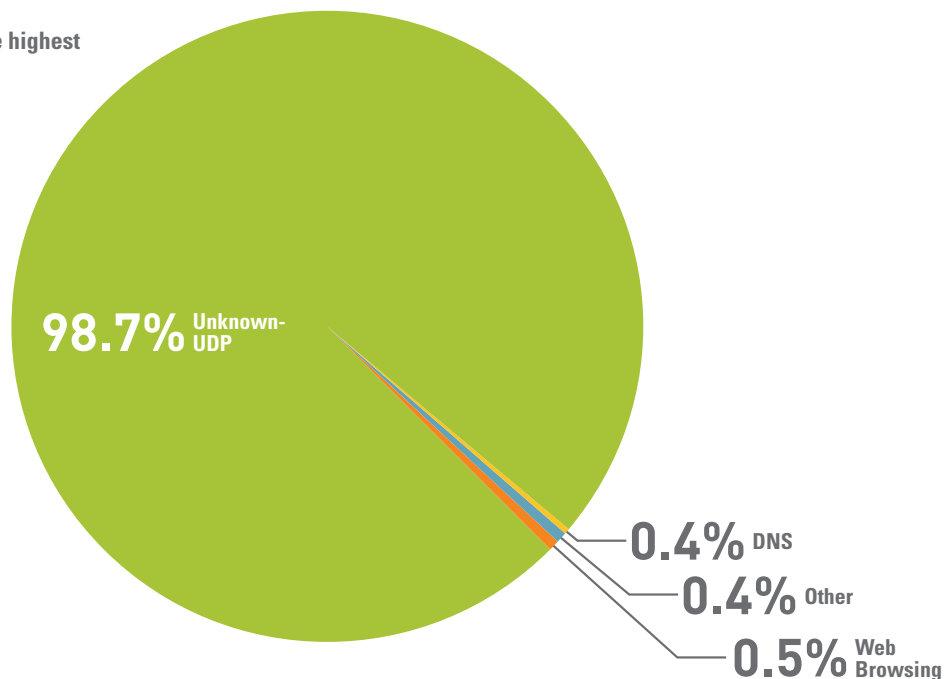
The ZeroAccess botnet is used by cyber criminals for three purposes:

1. Use computer resources to solve cryptographic hash challenges for generating Bitcoins (“mining”)
2. Perpetuating click-fraud against online advertisers
3. Generating spam e-mails

Once installed on the network, ZeroAccess will initiate connections with its peers using a customized peer-to-peer protocol as well as other customized UDP to communicate with its command and control infrastructure. Whereas a traditional Trojan might generate a single alert every five minutes when it reaches out to a single command-and-control server, ZeroAccess constantly reaches out to hundreds of other systems to build up its network, thereby generating a massive number of alerts. This wide-reaching peer-to-peer design during the data collection period is the driving force behind the high level of activity and it is critically important in maintaining the reliability and survivability of the botnet.

FIGURE 4: Applications with the highest volume of malware activity.

Applications with Most Malware Activity (Global)



1. Resilience: the widespread network of peer-to-peer nodes is one reason the attempted takedown by Microsoft and other organizations has largely failed. No one node represents the “kill point,” making it nearly impossible to take ZeroAccess down.

2. Distributed processing: continually solving cryptographic hash challenges requires significant computing resources and the use of many computers is a known and successful mechanism to address this resource challenge. One significant risk that organizations may face is that of a self-imposed denial-of-service attack. If ZeroAccess were able to navigate its way into a virtual server farm or datacenter, the massive drain on business servers may pose the risk of failure.

The use of custom peer-to-peer across UDP works well from the attacker’s point of view, but typically does not match any known UDP applications, resulting in the botnet traffic being identified as unknown-UDP. This technique of hiding in plain sight is common in malware traffic and is

one of the key reasons why Unknown-UDP was where the highest volume of malware activity was found.

POTENTIAL FOR PROACTIVE CONTROLS

Our analysis shows that customized or modified traffic is highly correlated with threats. This indicates that proactively controlling or blocking “unknown” traffic could easily provide a powerful and untapped strategy for controlling modern threats. This however does not imply a replacement of threat signatures, but an augmentation of them. Attackers are in a constant struggle to find new ways of breaking into networks, and security companies are likewise in a constant exercise of delivering new protections for new threats. However, the same creativity that attackers use to find new attack vectors can also be used against them. By blocking or tightly controlling unknown traffic, security teams can greatly reduce their attack surface and proactively manage new, evolving threats in real time.

BRUTE FORCE ATTACKS TARGET BUSINESS APPLICATIONS AND SERVICES

While common sharing applications showed a high number of code execution exploits being delivered, and network services such as UDP that are typically ignored displayed high malware traffic, the internal business applications and network services displayed a significant volume of brute force attack activity. Brute force attacks can be used to either disable a service or to compromise it, “taking it over” to use it for a range of malicious purposes.

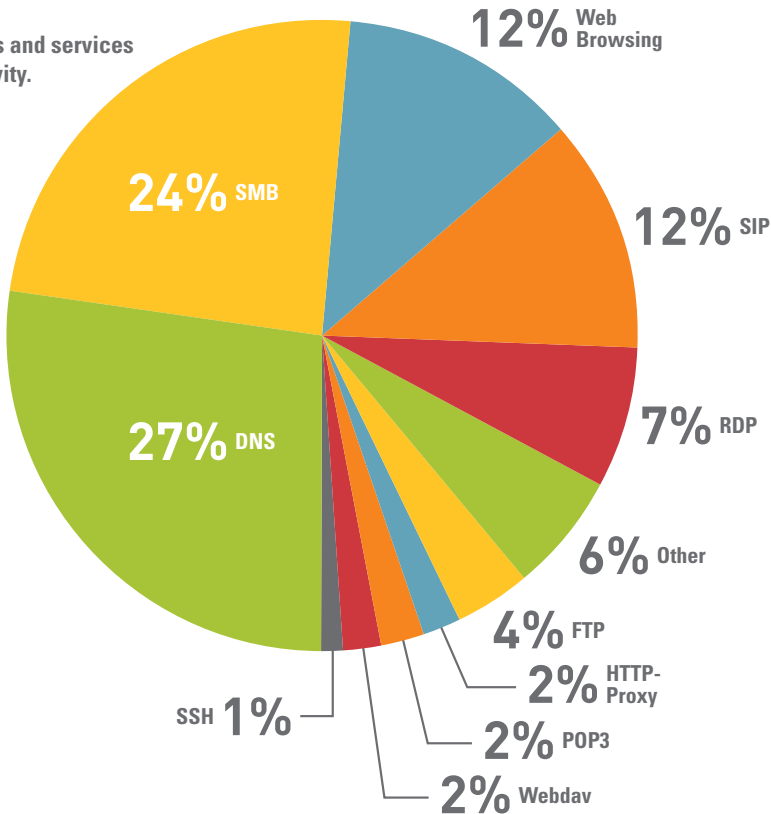
Two of the most commonly targeted applications, DNS and SMB, represent significant risks to the organization if cyber criminals are able to successfully control them. Both applications hold significant information about other business applications and services on the network. Specifically, the DNS server holds the names of other servers on the network. And SMB, acting as the

file transfer protocol for all Microsoft (and many other) server-based applications, can provide cyber criminals with direct access to all of the data held within those business applications. If the SMB server is compromised, then so too can other applications attached to that server. Two examples of the brute force attacks within these applications are described below.

- DNS ANY queries brute force attack:** an attacker finds one or more open DNS resolvers – DNS servers on the Internet open to anyone to query against – and uses that to direct an “any” query to a target (victim) DNS service. While most DNS queries specify a single type of record, such as MX for e-mail or NS for Name Server, the ANY query requests a list of all records that match a given name. This information is valuable to attackers who conduct

FIGURE 5: Business applications and services delivering the most exploit activity.

Top Applications Exhibiting Exploit Activity (Global)



reconnaissance against a target, as they can learn about many services with a single request. However, the ANY request is even more damaging when used in a DNS amplification attack. If attackers forge the source IP of their ANY request packet, the DNS server will send the response to their victim instead of back to the attacker. As the response packets are much larger than the request, this gives attackers the ability to amplify their effective bandwidth and flood their victim with traffic, overwhelming their service and rendering it unusable.

- **Microsoft Windows SMB NTLM authentication lack of entropy attack:** entropy, in the computer world, equates to randomness – so in this case, lack of entropy means a lack of randomness within the SMB authentication mechanism, specifically cryptography. The vulnerability is based on flaws found in the pseudo-random number generator (PRNG) used in the SMB challenge-response protocol where attackers repeatedly perform authentication attempts until the server generates the duplicate challenge. In short, the authentication

challenges are too predictable and not unique enough. This vulnerability allows attackers to access the SMB service as an authorized user giving them read/write access to files, as well as other SMB shared resources and remote code execution (via DCE/RPC).

SECURITY RECOMMENDATIONS

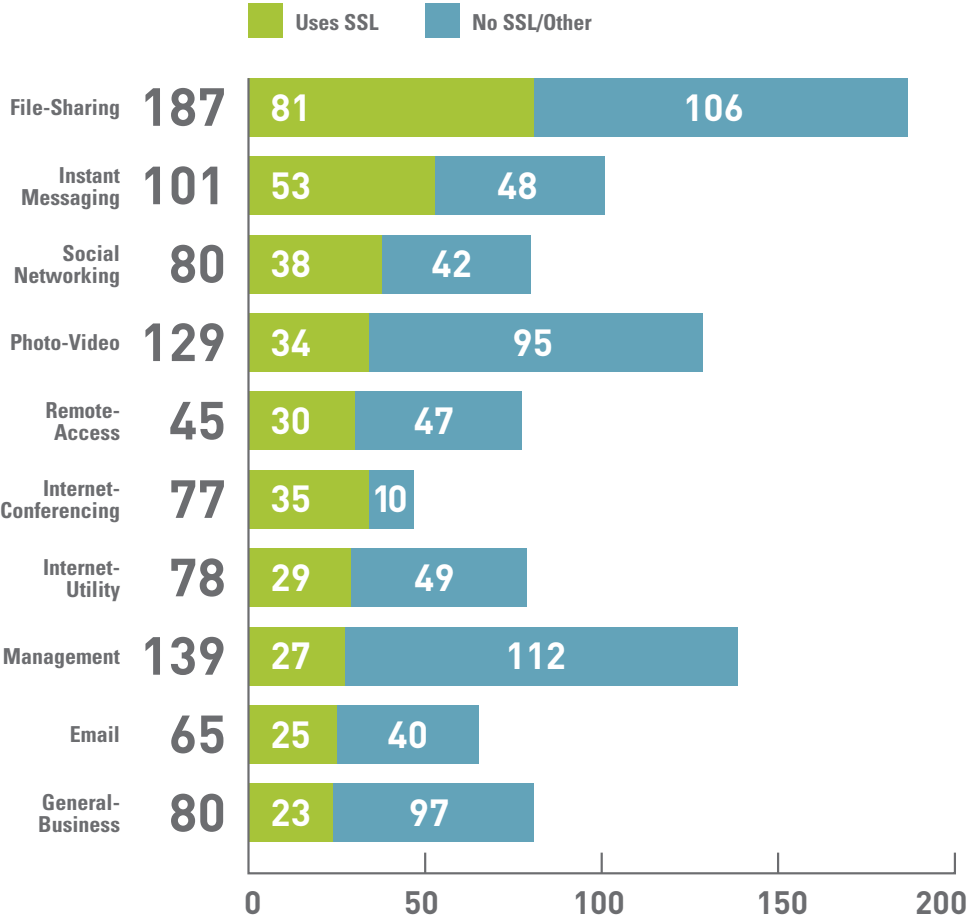
Both of these attacks provide good reason to consider isolation of the application or service and validation of the users through network segmentation. In many organizations, the speed of growth and the volume of network changes have led to an open and very flat network which becomes very difficult and costly to secure. Recommended mitigation steps would be to make sure that the SMB server is patched and up-to-date. Then using segmentation principles, restrict access to both the DNS resolvers and SMB services only to internal network and/or trusted users, implement an up-to-date IPS and next-generation endpoint protection software, and create a blacklist for the malicious IP addresses.

HOW MANY APPLICATIONS ON YOUR NETWORK USE SSL?

Palo Alto Networks provides the ability to decrypt SSL based on application-level policy. This feature provides a view into the applications that are capable of using SSL in some way, shape, or form. Based on this ability we were able to determine that 34% of all applications we found within the 5,500 network traffic assessments can use SSL to communicate in the dark. Surprisingly, these

applications span nearly all of the 26 application subcategories. The most commonly used ones are shown in figure 5. The use of SSL brings the benefit of privacy, but also the risk of hiding malicious activity and, of equal concern, the risk of compromise via Heartbleed, the recently exposed OpenSSL vulnerability.

FIGURE 5: Top 10 categories with the highest concentration of applications that can use SSL.



THREATS USING ENCRYPTION: HIDING IN PLAIN SIGHT?

SSL and tcp/443 are well known to cyber criminals as the easy way to bypass a port-based firewall and recent high profile attacks have shown their effectiveness. One example is the Trojan. POSRAM, a variant of the BlackPOS Trojan used recently to steal the credit card data and personal information of roughly 100 million Target customers. In this particular attack, the cyber criminals were able to gain access to the entire network, and install their malware in key locations. The credit card and personal information was collected, encrypted using SSL, and moved around via netbios shares, then stolen via FTP. The use of any of these applications was not unusual as they were found on more than 90% of the networks we analyzed, but the location or where they were used was and would have raised a red-flag had it been discovered in a timely manner.

In an example of “what’s old is new,” the Ramnit bot has been updated and was seen within the threat traffic we observed. The Ramnit bot initially infects a user machine with HTML files that have an appended VBScript. Another infection vector is through Microsoft Office OLE document files with .doc, .docx, or .xls file extensions and contain a macro which will attempt to run when the document is opened. Once installed, the bot will download a module that is encrypted using RC4. It will remain encrypted on the endpoint, and when executed, will load as a .dll, hiding in plain sight using two different techniques.

The Ramnit bot is known to steal FTP, banking credentials, and browser cookie information as well as enable remote access on the victim’s machine (via VNC, a remote access tool found on 52% of the networks we analyzed) thereby providing the attacker with the ability to do just about anything. Finally, there is a new module that appears to do a better job at evading end-point protection mechanisms such as antivirus, personal firewall and automatic updates by disabling them via Windows registry modifications.

HAS THE HEARTBLEED RISK COME AND GONE?

Up until now, the Heartbleed impact has been focused on the compromise of HTTPS-enabled websites and web applications, such as Yahoo!, Google, Dropbox, Facebook, online banking, and the thousands of other vulnerable targets on the web. These are of huge impact, but those sites will all be updated within the next few weeks. The media frenzy will die down and the world will move on, believing Heartbleed is behind us.

For security professionals, however, this is only the tip of the iceberg. The Heartbleed vulnerability puts the tools that were once reserved for truly advanced cyber criminals into the hands of the average attacker – notably, the ability to breach organizations and move laterally within them. Most enterprises of even moderate size do not have a good handle on what services they are running internally using SSL encryption, much less those that the end-users have brought into the network. Without this baseline knowledge, it is extremely difficult for security teams to harden their internal attack surface against the credential and data stealing tools that Heartbleed enables. Suddenly, all footholds for the attacker with an enterprise network are of equal value.

Proof-of-concepts that take advantage of Heartbleed are no doubt in the works. We believe it is only a matter of time before an automated internal scanner is developed that finds vulnerable services on the local network and exploits them with a single click. The challenges that presents to organizations is significant – once you know how many internal applications may be using OpenSSL, how difficult will it be to update them? If it is a business critical application, the effort is not small.

Organizations must determine which applications are capable of using SSL, both the business applications and those in use by employees. Then determine which of them use OpenSSL. The primary risk to end-user introduced applications using OpenSSL is the endpoint. The secondary risk is what is on that endpoint machine in terms

of company data. Knowing which applications are using SSL, who is using them, and what network resources the person has access to will allow you to gauge your exposure.

ADDRESSING THE HEARTBLEED RISK

Even though the Heartbleed ramifications will be felt for some time, there are known steps you can take to mitigate these risks and get on with your business.

- **Exert tighter control over those applications that can use SSL:** as shown in figures, there are many more applications that use SSL than you would think, or you possibly need within your organization. Many are end-user focused and may not be updated quickly, or end-users may not follow best practices thereby introducing possible security risks to the organization.
- **Identify and patch your affected systems:** as obvious as this sounds, don't assume you know everything; given that more than a quarter of the applications we found can use SSL. Run local scanners across your network to discover any OpenSSL instances that might have popped up without your knowledge. Both client and server applications that utilize OpenSSL need to be updated.
- **Contact any of your cloud application providers to see where they are in the cleanup process:** salesforce.com is one cloud provider that already announced that its systems are unaffected by this vulnerability. But you are probably using a handful of other cloud providers for other tasks like HR, payroll, ERP, etc. Make sure you know who they are and ensure they are cleaning up the same way that you are. Utilize reputable resources such as Filippo Valsorda's site (<http://filippo.io/Heartbleed/>) to check for vulnerable systems.
- **Get new keys:** acquire new key certificates, revoke your old ones, and install the new ones. Because of the way the vulnerability works, attackers who have compromised your servers through this Heartbeat vulnerability may have

stolen your private keys. Even after you patch your systems, attackers would still have your private keys. Get a new set of keys.

- **Inform your customers:** this is critical. Your customers should already be asking you if you have been affected (see No. 3), but there will be some that have not and will just assume you're working on it. As a matter of trust, you should be transparent about your cleanup efforts. Do not shy away from this. Since this vulnerability is widespread, you will not be alone in your efforts and maybe you can help some other organization that is not as clear-thinking as you are about how to do this cleanup. Customers always remember who acted swiftly and professionally in times of crisis.
- **Change your passwords:** once you have patched your systems, changed your keys, ensured that your cloud providers also accomplished those tasks, then it is time to change the passwords for all users on those systems. But wait on this until everything else is done, because attackers who are hanging out on systems that have not been patched or systems where the keys have not been changed can still read your new password. It does not make sense to change your password until the other tasks are completed.
- **Beware of the inevitable phishing campaigns:** soon you will start to see phishing email messages telling you that you must immediately change your password in order to protect yourself from the Heartbleed vulnerability. They will most likely have a link embedded in the message pointing you to a site that looks very much like your ERP, HR, or payroll site, but, in fact, will be a site cleverly designed to collect your credentials. Be wary of all communications related to Heartbleed.

If there's a long-term consideration here, it's to install perfect forward secrecy as Twitter did last year (<http://phys.org/news/2013-12-secrecy.html>). That ensures that a session key derived from a stolen private key and a collected public key in the future will not be compromised.

SUMMARY

Globally, the findings were somewhat surprising in that common sharing applications delivered nearly one third of all threats – and 19% of all code execution exploits. Yet their threat activity was disproportionately lower than expected, particularly when compared to the other two categories. When applying the standard attacker practice of using multiple steps to perpetrate the end-goal, this pattern makes sense. The same pattern of exploits, not malware, was found within the internal applications that act as critical pieces of the infrastructure. Within these applications, brute force activity was significant. Here too, the concept of being part of a multi-phased attack may help explain the reason why. Malware, specifically a range of botnets were found hiding in plain sight within UDP and a few other applications. The use of SSL and encryption, once a benefit as a privacy and security feature is now a significant risk both in terms of hiding malicious activity and placing the business at risk via the Heartbleed threat.

RECOMMENDATIONS

The traffic and associated threat patterns discussed within this report exemplify how cyber criminals are opportunistically hiding in plain sight, yet there are some fairly straight forward steps that organizations can take to minimize or eliminate the hiding places within the network.

- 1.** Deploy a balanced safe enablement policy for common sharing applications. First determine which applications are in use and by whom. Then in collaboration with the business groups, determine the business use case, and establish security policies that enable the required applications while blocking others. Key to the success of this recommendation is documentation of the policies, education of your users, periodically reviewing and updating the policy.
- 2.** Control the unknown traffic, isolate and segment business services and applications. Every network unknown traffic – it is small in volume, averaging roughly 10% the bandwidth observed, but it is high in risk. Controlling unknown UDP/TCP will allow you to quickly eliminate a significant volume of malware. As an extension of controlling unknown traffic, your business applications and services should be isolated, applying zero-trust principles based on the applications and users that require access.
- 3.** Determine and selectively decrypt the applications that use SSL. The use of SSL has become a double edged sword. Privacy and protection on one hand, masking threats and exfiltration of data either directly or indirectly via the Heartbleed exploit on the other. Selective decryption, in conjunction with enablement policies outlined above can help you uncover and eliminate potential hiding places for cyber threats.

APPENDIX A: REGIONAL OBSERVATIONS

At a regional level, the traffic and threat patterns mimicked the global patterns discussed above. This is not too surprising, given that the data set is generated within enterprise networks, all of which have access to the web, and the applications therein. Internal applications follow a similar pattern – enterprises use similar applications from leading vendors worldwide; and these applications rely on network services that are commonly targeted by cyber criminals. Any differences from region to region are very subtle, and do not significantly modify the general statements made about the global traffic patterns.

REGIONAL DATA SUMMARIES

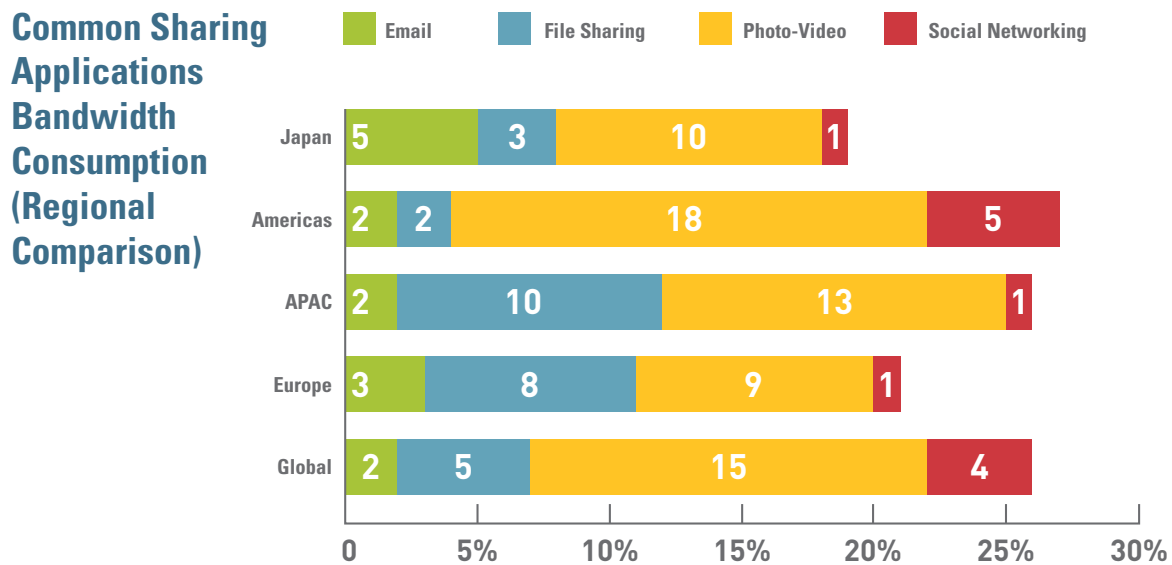
- The **Americas and Canada** dataset represents 2,203 organizations distributed across 17 countries (up from 11 in 2013) in North, South, and Latin America. The United States, Brazil, Canada, Mexico, Colombia, Costa Rica represented (in order) 93% of the participating organizations. 1,676 applications were found along with 4,623 threats.
- The **European** dataset represents 1,499 organizations in Europe, the Middle East, South Africa, Russia, and the Baltics. 73% of the participating organizations were in (in order) Germany, UK, France, Spain, Netherlands, Italy, Russia, Finland, Austria, and Norway. 1,707 applications were found along with 4,744 threats.
- The **Asia Pacific** dataset represents 1,325 organizations distributed across 20 countries with 91% coming from (in order): Taiwan, China, Australia, Thailand, Korea, India, Philippines, Hong Kong, Malaysia, Singapore, and Vietnam. 1,576 applications were found along with 4,623 threats.
- The **Japanese** dataset represents 404 organizations with 1,178 applications detected and 1,314 threats found.

COMMON SHARING APPLICATIONS – REGIONAL OBSERVATIONS

Observations on common sharing application threat delivery and associated activity (Figure 6):

- **File sharing:** The **Americas and Canada** file sharing application bandwidth consumption was the lowest of all the regions at 2% while Asia Pacific and Europe consumed the highest volume.
- **Video:** Video application usage within the **Americas and Canada** was the highest of all the regions at 18%.
- **Social media:** At 5% of bandwidth consumed, social media in the **Americas and Canada** was 5 times greater than the other regions.
- **Email:** Email traffic in **Japan** consumed more the twice as much bandwidth than the other regions at 5%.

FIGURE 6: Regional comparison of bandwidth consumption for common sharing applications.

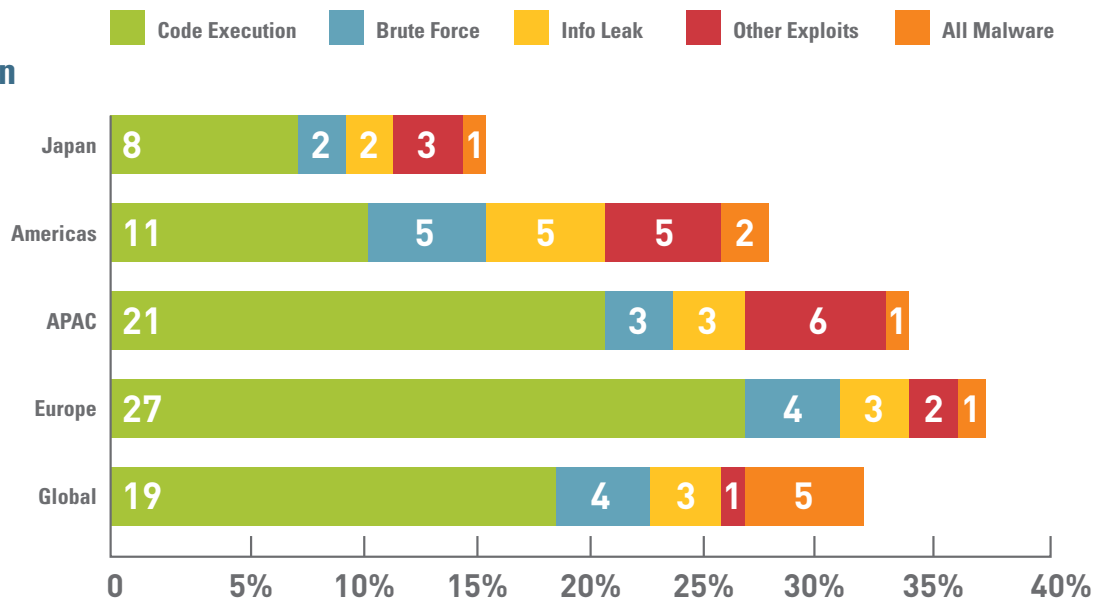


Observations on common sharing application threat delivery and associated activity:

- The number of threats delivered across common sharing applications for the **Americas and Canada** was lower than the other regions while Europe was the highest at 37% of all threats delivered.
- Code execution exploits delivered across common sharing applications in **Europe** were higher than other regions at 27%.
- **Japan** had the lowest overall volume of threats within these applications and the lowest percentage of code execution exploits at 8%.
- In terms of outbound threat activity within common sharing applications, all of the regions saw roughly the same volume at 5% of total.

FIGURE 7: Regional comparison of threat types found within common sharing applications.

Threat Types Within Common Sharing Applications (Regional Comparison)



BUSINESS APPLICATION THREAT ACTIVITY – REGIONAL OBSERVATIONS

- Malware activity across UDP in **Japan** was nearly non-existent, possibly because of the fact that ZeroAccess was not found within the Japanese organizations. Nearly all malware activity in **Japan** was observed in web-browsing.
- The **Americas** displayed the highest volume of DNS threat activity and the lowest volume of SMB related threat activity.
- Threat activity observed in SIP traffic was lowest in **Europe** and highest in **Japan**, while SMB exhibited a higher volume than other regions in **Europe**.

SSL USAGE – REGIONAL OBSERVATIONS

Regionally, there was little variance in the number of applications that are capable of using SSL, nor were there any significant differences in the application categories in use.

- Globally, 34% (539) of the 2,076 applications observed are capable of using SSL.
- In **Asia Pacific**, 498 out of 1,576 (32%) applications are capable of using SSL.
- **Japan** had the highest percentage of SSL usage at 36% (425) of the applications found (1,178). This may be partially attributed to the lower overall application count and the smaller sample size.
- In **Europe**, 511 out of 1,707 (30%) applications found are capable of using SSL.
- In the **Americas and Canada** 539 (32%) of the 1,676 applications observed are capable of using SSL.

DEMOGRAPHICS AND METHODOLOGY

The latest edition of the Application Usage and Threat Report summarizes more than 5,500 traffic assessments performed worldwide. The distribution of the participating organizations is distributed fairly equally across three geographic regions: Americas (including Mexico and Canada), Asia Pacific, Japan, and Europe. The findings within this report focus solely on the global view of application traffic with any regional specific variations in usage patterns discussed separately.

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 and 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 Threat Report.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business

operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.



PALO ALTO NETWORKS • 4401 GREAT AMERICA PARKWAY • SANTA CLARA, CA 95054

www.paloaltonetworks.com



Copyright ©2014, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks and the Palo Alto Networks Logo are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.