Application-aware Acceptable Use Policy for Enterprise Security

Allot CloudTrends Report Q2/2015

Allot communications

Contents

Executive Summary

Enterprises face numerous security threats that come in through many doors and take various formats, some well-known and others less obvious. As enterprise mobility becomes widespread and the migration to hybrid and public clouds continues, the security challenge is growing and changing. These trends disrupt the boundaries of traditional security solutions and allow online threats to jeopardize business productivity and viability more than ever.

In this report we analyzed the web security challenges of the modern enterprise, including application visibility, Acceptable Use Policy (AUP), malicious web traffic and cloud applications. The data in this report has been collected from large enterprises and from Communication Service Providers (CSP) who provide security services to enterprises and hundreds of Small and Medium Businesses (SMB).

Key Findings

- 92% of blocked web traffic in large enterprises is due to a well-defined Acceptable Use Policy – not due to detected malicious traffic.
- Enterprises have anonymizer traffic on their networks though they may not be aware of it. "Anonymized" web traffic is blocked 3 times more often than overall web traffic due to malicious content.
- Even when Acceptable Use Policy is in place, there are numerous attempts to access “risky” applications.
- On average, enterprise users try more than 6 times per day to access social networks, half of which are going to Facebook.
- On average, traffic from Instant Messaging applications is blocked 10 times more often than overall web traffic due to malicious content.
- 90% of blocked malicious traffic was caused by malware (malicious software). Spyware constituted about 8% and viruses about 1% in the organizations we researched.
- 30% of blocked malware comes in the form of JavaScript files, making it the most commonly used attack vehicle.
- 20% of blocked malware comes in the form of image files that most users would not suspect (jpg, png, gif, ico).

Our findings clearly indicate that enterprises must develop a well-communicated and enforceable AUP that is granular and specific. Simple filtering of online threats is not enough. It is also clear that the 'A' in AUP should be used for *Applications*, since going forward, Application Use Policy will become more important. A comprehensive approach combining application visibility, AUP for websites and applications, and protection against online threats is needed to secure the modern enterprise.

Enterprise Security Concerns

As critical business applications migrate to the cloud, cyber-criminals no longer need to breach the traditional IT perimeter to seriously paralyze an enterprise. Just last year high-profile cloud/SaaS providers such as Salesforce.com, ServiceMax and Basecamp were taken out by cyber-attacks. If you happen to outsource any of your mission-critical tasks to these vendors, you were effectively shut down. With the cloud becoming more popular, web browsers are becoming more vulnerable to security holes.

While there have been many high profile attacks, no enterprise, large or small, is immune to cyber-crime. Whether for profit or just malicious intent, cyber-criminals, will continue to exploit every potential weakness in enterprise IT security.

The Cost of Inaction

While the prospect of dealing with a multitude of security threats seems daunting, the cost of inaction far outweighs the investment in planning and preventive measures. The damage and implications of cyber-attacks or other IT security breaches can go far beyond the cost of downtime. For example, the attack on Target in late 2013 resulted in many unforeseen consequences summarized in Figure 1. Regardless of the motivation, cyber-security breaches can have devastating consequences in the short term, as well as unanticipated effects on long term business viability. Examples like these demonstrate how important cyber-security is for enterprises.

Not only high-profile or large companies are in the cyber-criminal's cross-hairs. As these large firms beef up their security budget, cyber-criminals are moving to smaller businesses in search of easier prey. According to PwC's recent *Global State of Information Security Survey 2015*, "We found that small firms, with annual revenues less than $100 million, cut security spending by 20% in 2014, while medium – those with revenues of $100 million to $999 million – and large companies increased security investments by 5%."

In a recent survey, Kaspersky Labs estimated the cost of security threats, even to SMBs, can be tens of thousands of dollars, reaching well into hundreds of thousands of dollars for mid-size enterprises. (IT Security Threats and Data Breaches *http://media.kaspersky.com/en/business-security/Global-IT-Risks-Report-2014-Threat-Security-Data-Breaches.pdf?icid=en-GL:ent-carousel*)

Figure 1:

Implications of the Target security breach

Cost of a Security Breach

TARGET

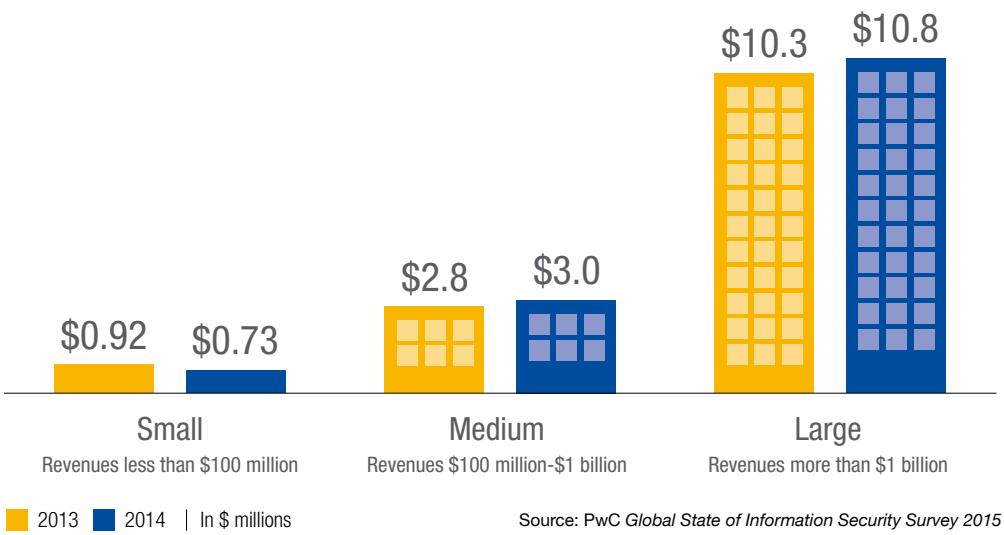
What we know/see:

- 100 million customers affected
- 2013-2014 total: $252 million, minus $90 million insurance receivable
- Exec team restructure (CEO resigned, new CIO, hired 1st CISO)
- Downgraded credit rating by S&P
- Ongoing litigation

Source: see References

Figure 2

Information Security Budget by Company Size



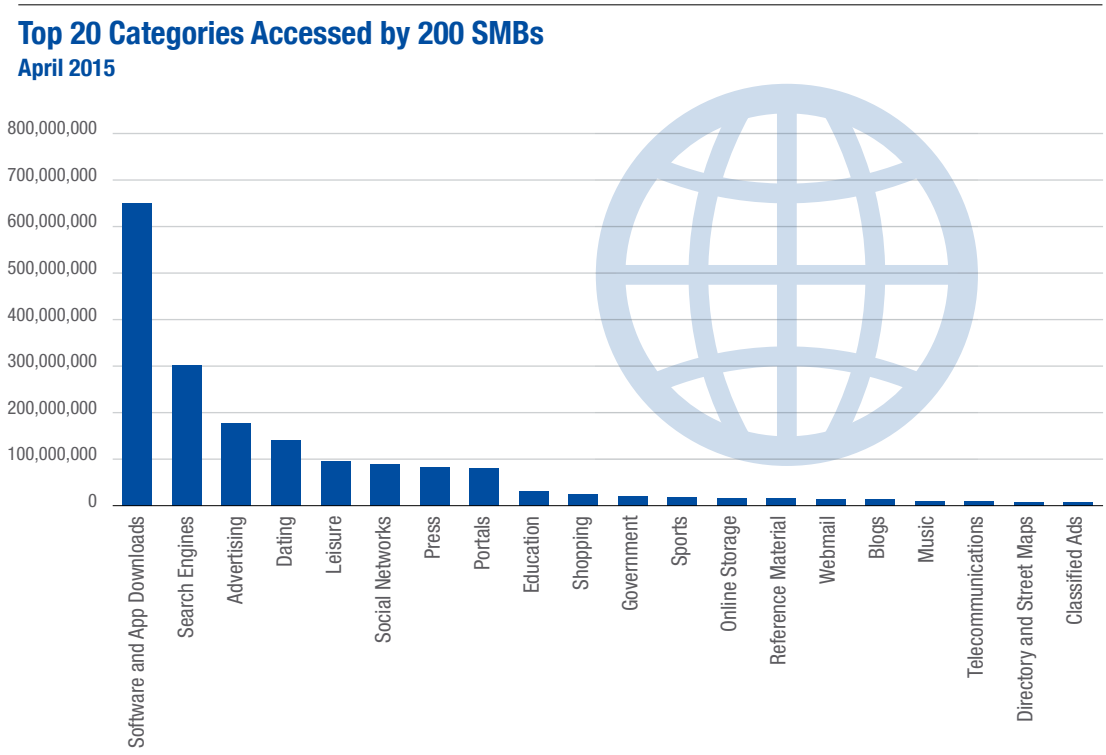
Source: PwC *Global State of Information Security Survey 2015*

While the high-profile hacking, DDoS and other cyber-attacks we read about are very real and devastating, there are many more common and no less potentially destructive risks. This report highlights some of the less obvious cyber risks that today's enterprises face.

Figure 3 shows web traffic for a one-month period broken down by content category. The data for this particular graph was aggregated from over 200 SMBs. The results show that many non-business and "high-risk" websites are accessed by employees through the corporate Internet connection. Cyber-criminals often attempt to disguise their illicit attempts as legitimate traffic, relying on the unwitting assistance of employees to carry out their aims. Employee lack of awareness and caution is often a key factor in security breaches.

In most companies, employees are expected to use the Internet responsibly and productively. An Acceptable Use Policy (AUP) combined with stringent user training is always the right first step to create the awareness and vigilance that will help mitigate much of the cyber risk. However, IT security departments must think outside the box when it comes to web/cloud security and be prepared with an AUP that includes application control.

Figure 3



AUP Enforcement is Essential to Threat Prevention

Adherence to and enforcement of a corporate Acceptable Use Policy can eliminate many potential threats. The graph below shows that over a period of five months in a security-aware enterprise, 92% of the blocked web traffic was due to the enforcement of policy, while just 8% of blocked web traffic was due to its identification as malicious traffic. The implications are clear. Strict enforcement of an AUP can dramatically reduce the amount of potentially harmful traffic entering (or exiting) the enterprise.

Malicious traffic represents many types of threats to employees and to the organization. While hacking attempts often capture news headlines, malware and spyware are a more pressing threat, comprising 90% of all malicious traffic in the organizations we studied.

Figure 4a

AUP Blocking vs. Malicious Blocking
11/2014 - 04/2015

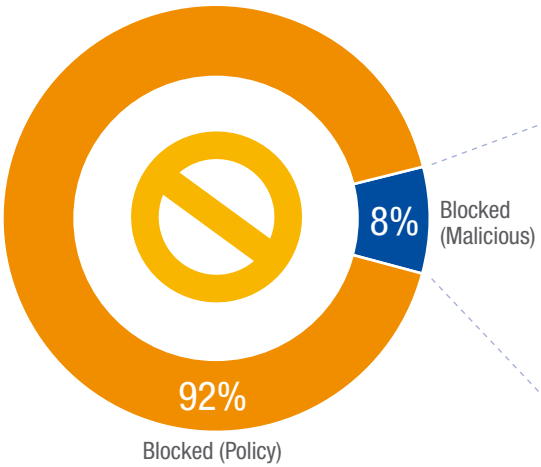
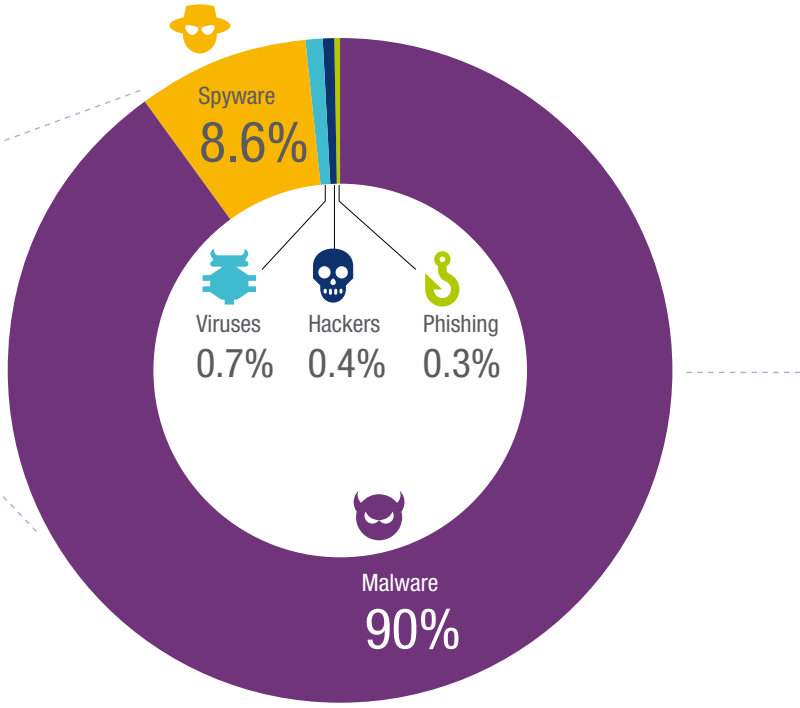


Figure 4b

Types of Malicious Traffic
11/2014 - 04/2015



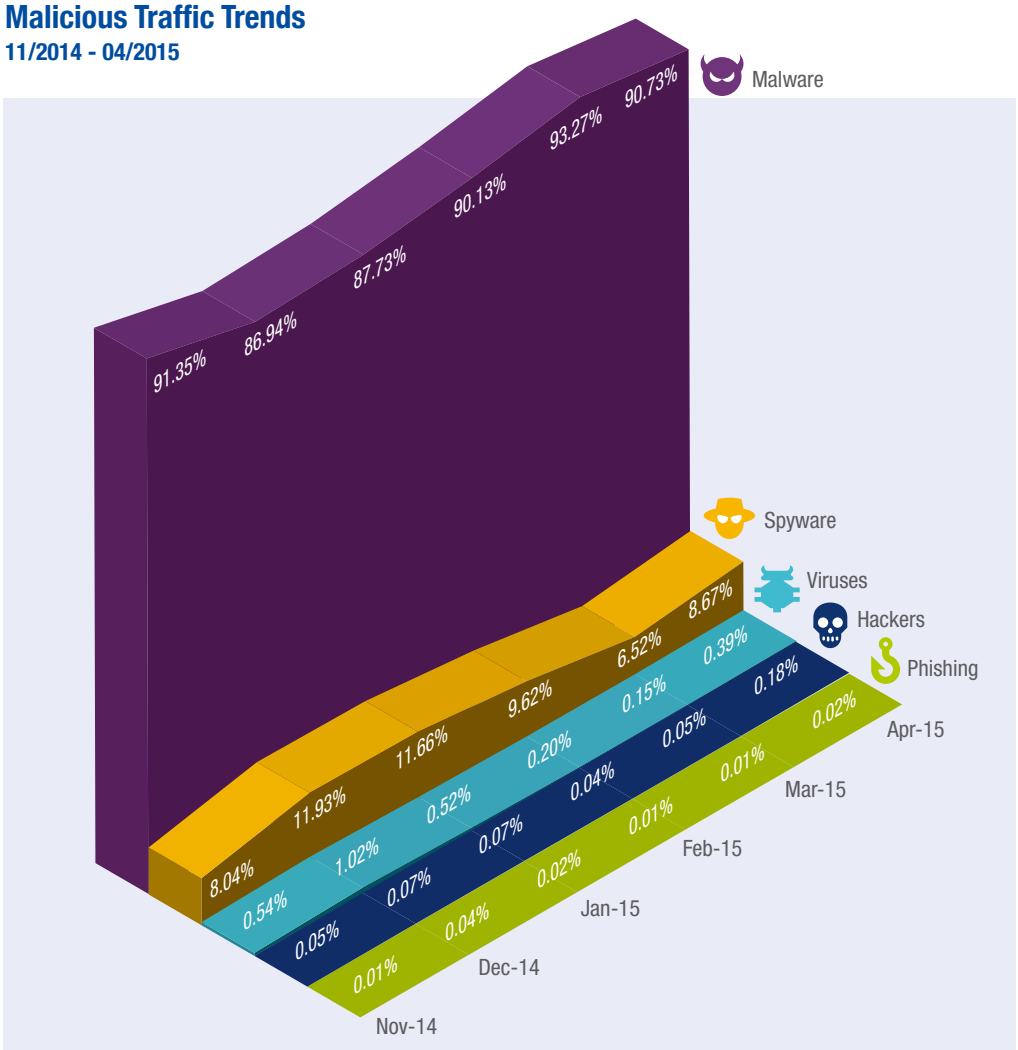
Trends

Figure 5 shows a detailed breakdown of malicious traffic over a six-month period (11/2014 – 04/2015). Malicious programs are dangerous because they can perform actions that have not been authorized by the user. Here are some examples of such actions which demonstrate the level of risk:

- Redirection of web browsers
- Initiation of scripts or programs to gain user credentials, customer information, financial data or other sensitive/ confidential information
- Installation of botnets
- Destruction of data

Figure 5

Malicious Traffic Trends
11/2014 - 04/2015



As mentioned earlier, cyber-criminals often disguise their illicit attempts as legitimate traffic, and rely on the unwitting assistance of employees to carry out their aims. Enterprise and SMB employees are popular targets for persistent attacks that often wax an wane as they attempt to exploit vulnerabilities. Figures 6-10 show the breakdown of individual malware targets over a six-month period.

Figure 6

Malware Attempts Blocked per Month per User
11/2014 - 04/2015

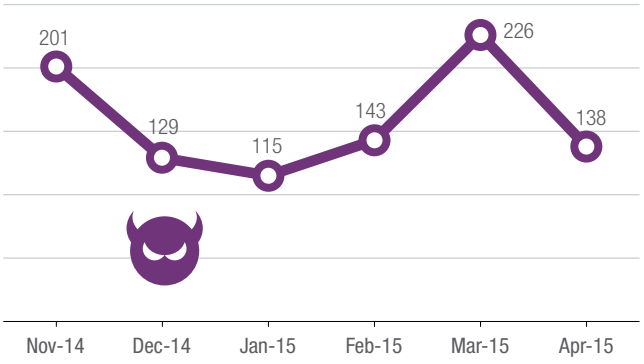


Figure 7

Spyware Attempts Blocked per Month per User
11/2014 - 04/2015

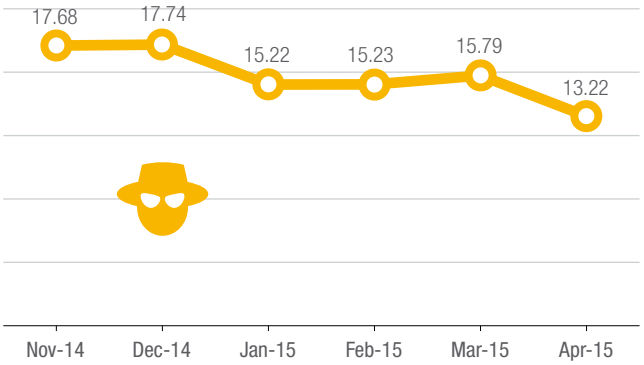


Figure 8

Viruses Blocked per Month per SMB
11/2014 - 04/2015

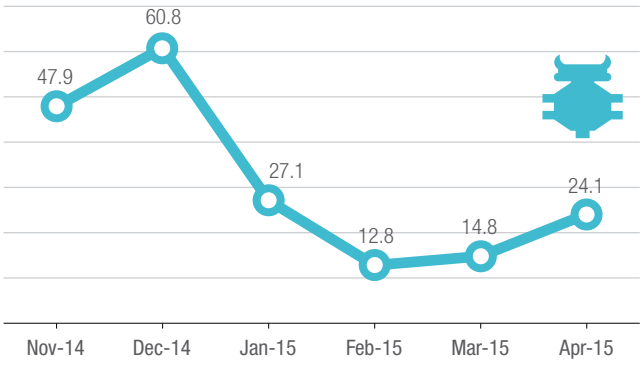


Figure 9

Hacking Attempts Blocked per Month per SMB
11/2014 - 04/2015

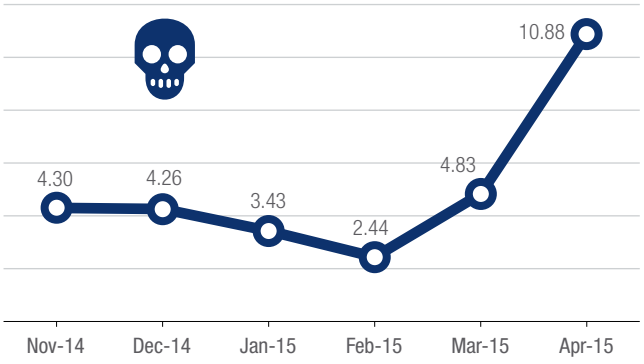
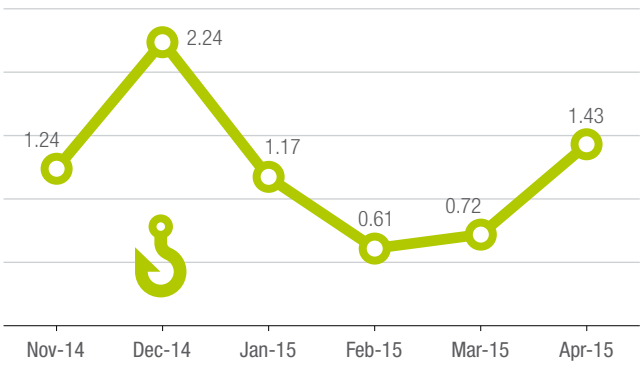


Figure 10

Phishing Attempts Blocked per Month per SMB
11/2014 - 04/2015



Malware, viruses and other threats are often disguised as regular content files. Figure 11 shows the file types blocked due to malware. The js (Java Script), aspx (Active Server Page Extended File Group) and php files are all server-side scripting languages. More commonly used file types are also being exploited. For example, images whose file extensions (jpg, png, gif, ico) are familiar to most Internet users comprise more than 20% of the blocked traffic. Threats like these come into the organization through seemingly harmless emails, Internet sites or social media and are very difficult for even the best trained and cautious employee to identify.

Viruses and worms tend to be self-replicating and very hard to purge once the infection takes hold. They too can install scripts to initiate dangerous attacks. The graph below shows the common types of viruses that were identified and blocked during the period we researched.

Figure 11

Common File Types Used by Malware

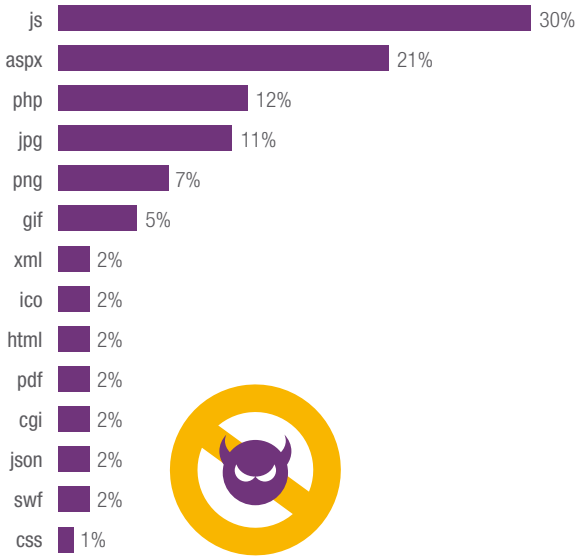
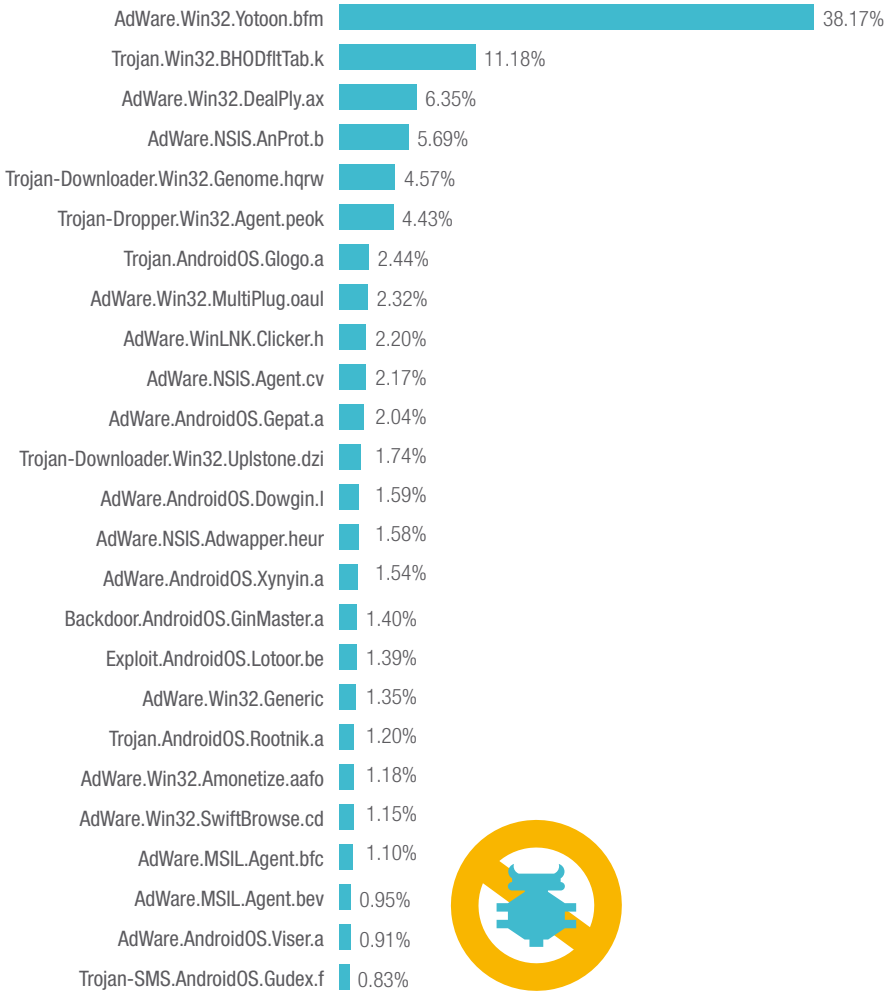


Figure 12

Top Viruses Blocked
11/2014 - 04/2015



Are social networks, gaming and instant messaging just productivity distractions?

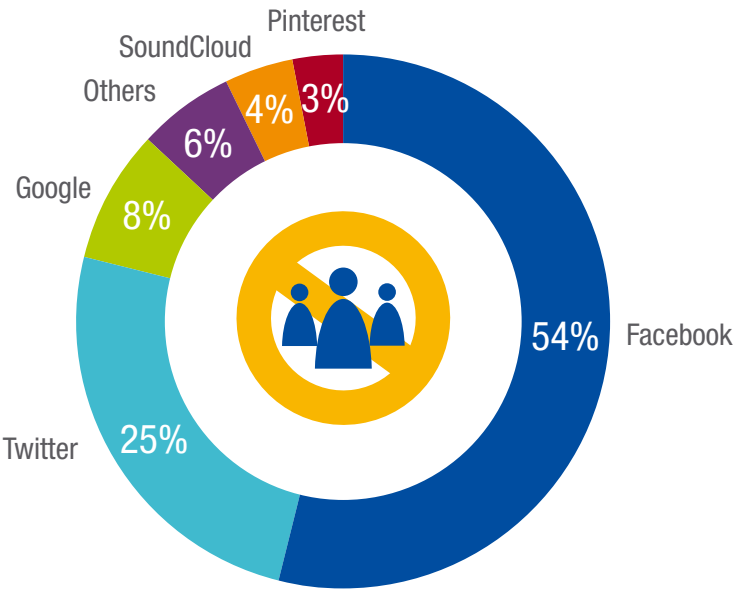
One of the large enterprises we focused on restricts the use of social networks and social media at the office. This policy and the reasons for it are clearly explained in the company's Acceptable Use Policy. The company enforces the AUP by blocking employee access to social networking sites. Our findings show that even though the company's AUP is well established and known, on average an employee makes 6.2 attempts per day to access social networking sites. Of these, 3 per day were attempts to reach Facebook as detailed in Figure 13. What is not known is whether these attempts were on purpose, or the result of being redirected by other websites or ads, or hidden links.

Social networks can distract employees during work hours and affect productivity. Moreover, they can also be the conduit for malicious traffic to penetrate through an organization's defenses. Some hackers go right to the source, injecting malicious code into the internal advertisements or third-party apps on a social networking site, waiting for unsuspecting users to click. On Twitter, shortened URLs (popular due to the 140-character tweet limit) can be used to trick users into visiting phishing sites that can extract personal and corporate information if accessed through a work computer. Twitter is especially vulnerable to this method because it's easy to retweet a post that may eventually be seen by hundreds of thousands of people.

Seemingly other harmless distractions such as playing online games, exchanging instant messaging and catching up on gossip provide a foothold for attackers to enter an enterprise and wreak havoc.

Figure 13

Social Networks Blocked
11/2014-04/2015



Anonymizers are dangerous

An anonymizer is a proxy that hides a user's real IP address – in this case, your company's IP address – from the Internet. It is attained by installing software on the client that creates a virtual proxy that links to a proxy network or to a public proxy server. There are hundreds of public proxies listed on the web, some of which anonymizers are tuned to call. There are approximately 58 attempts to use anonymizer applications per SMB per day. Of those, 2 attempts include malicious traffic that needs to be blocked.

When compared to overall Web traffic, "anonymized" traffic is blocked 3 times more often on average due to malicious content.

Anonymizers can be misused to evade corporate firewalls and Acceptable Use Policy, defeating your efforts to stop employees from accessing webmail accounts and engaging in inappropriate and sometimes illegal web surfing.

Email Spam and Phishing

Email spam and phishing are frequent causes of malware infections. A simple innocent looking email can mask a potentially major threat. Filtering corporate email is a standard response, but as we have already seen, phishing attempts can come through webmail, instant messaging and social networks, all affording malware a backdoor into the company.

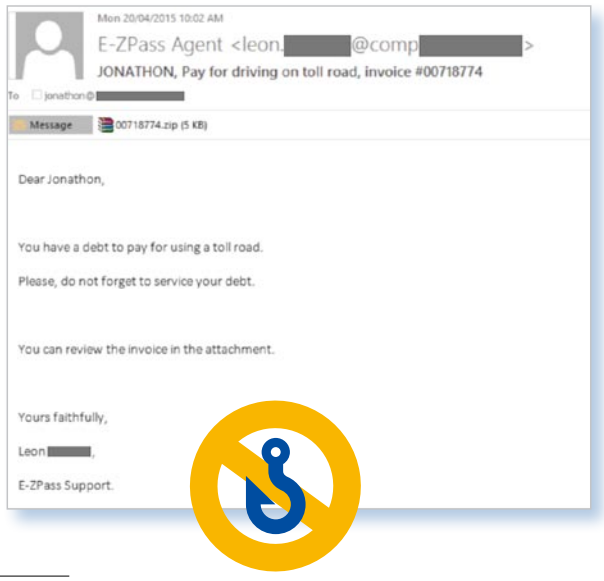
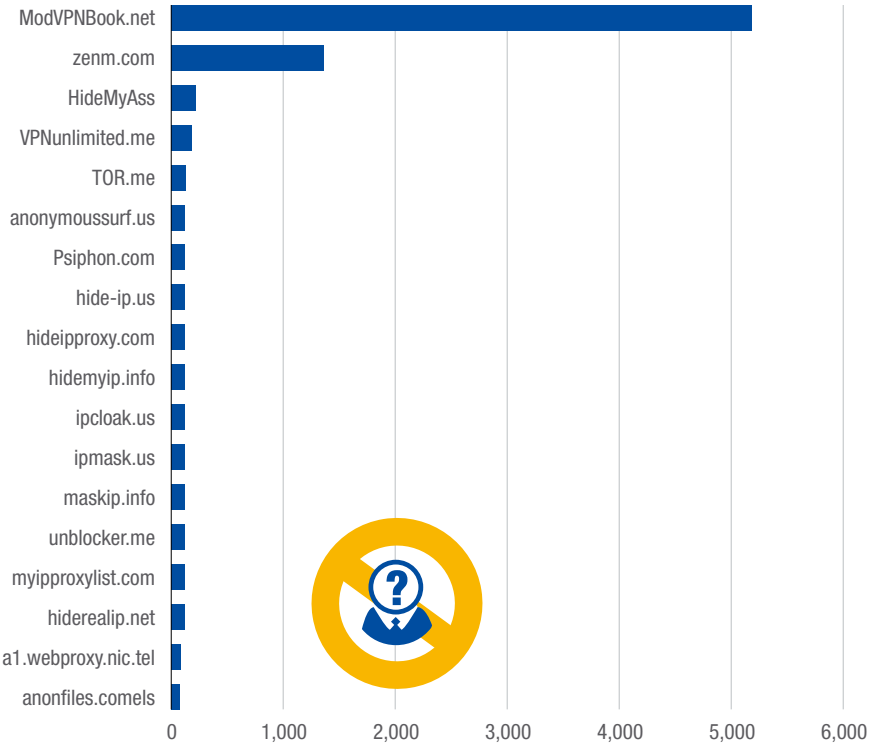


Figure 14

Top Anonymizers Blocked
11/2014-04/2015

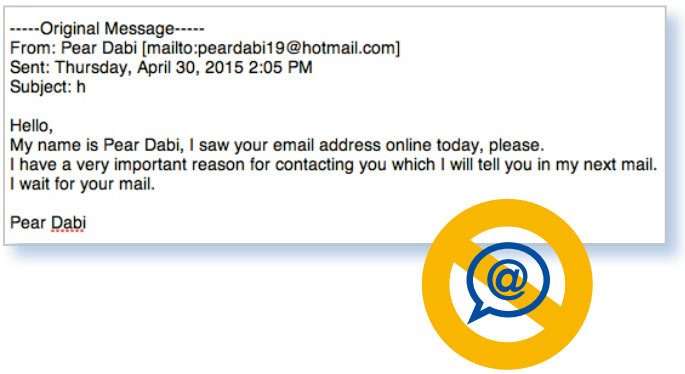


Webmail and Instant Messaging

Webmail and Instant Messaging pose a similar security challenge because they allow files to be attached and sent out of the company. In one large enterprise, employees on average made 5.5 attempts to access webmail and Instant Messaging sites and were blocked per the company's AUP. Moreover, we found that on average, traffic from Instant Messaging applications is blocked 10 times more often than overall web traffic due to malicious content.

Popular sites include:

- mail.google.com
- hotmail.com
- mail.live.com
- outlook.com
- mail.yahoo.com
- www.gmail.com
- www.whatsapp.com
- talk.google.com
- skype.com
- messenger.msn.com



Inappropriate Content

Accessing inappropriate content in the workplace can not only result in embarrassment, it may have severe consequences for both the employee and the company. Potential legal liability or negative publicity (issues of sexual harassment or racial intolerance) are too costly to ignore. Filtering out this type of content should be a priority in the workplace. Our findings show that employees at large enterprises attempt to access inappropriate content 1.5 times per day on average. Types of inappropriate content include:

- Bombs
- Dating Sites
- Drugs
- Glamour
- Hackers
- Models
- Pornography
- Weapons
- Violence

Online Storage - a major security hole?

Are cloud hosting and cloud storage websites a friend or foe to the security-conscious enterprise? These services are becoming increasingly popular for both corporate and personal use. Aside from the benefits such services bring to the corporate environment, there are inherent security challenges when they are used on an ongoing basis. Since it puts company data beyond the security perimeter of the enterprise, the information may not be properly secured, which could lead to unwitting leakage of confidential data. Dropbox already experienced a well-publicized problem with the security of their accounts and data. In short, your data may not be safe there. A Dropbox[1] sync glitch resulted in lost data for some subscribers and Dropbox blames other services for a claimed 7 million password hack.

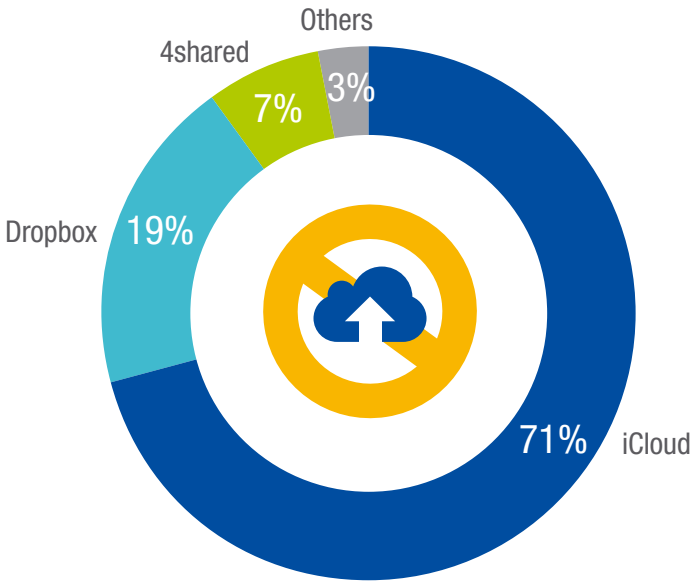
Online storage makes it very easy to transfer confidential or proprietary information out of the organization. An increasingly mobile workforce, coupled with the lack of company-approved, user-friendly file sharing tools, has led employees to use risky means to easily distribute files. The use of content-sharing applications in public clouds is common and easy but can be insecure and often a nightmare to IT security staff. When files leave the safety of the company's managed infrastructure, they are very difficult to track, and if that data lands in the wrong hands, it can result in a data breach.

Figure 15 shows that iCloud is overwhelmingly the most routinely blocked site for online storage. Apple's iCloud is not typically considered an enterprise application.

Cloud hosting and storage websites such as Dropbox, Google Drive, and iCloud – Friend or Foe?

Figure 15

Top Online Storage Sites Blocked
11/2014-04/2015



[1] *http://blogs.wsj.com/digits/2014/10/14/dropbox-blames-security-breach-on-password-reuse/*
http://www.independent.co.uk/life-style/gadgets-and-tech/nearly-seven-million-dropbox-passwords-hacked-pictures-and-videos-leaked-in-latest-thirdparty-security-breach-9792690.html
http://www.cnet.com/news/hackers-hold-7-million-dropbox-passwords-ransom/
http://techcrunch.com/2014/10/14/dropbox-pastebin/

Application Visibility and Control

Application awareness and control is crucial to securing your enterprise and SMB and maintaining productive use of Internet and network resources. Malicious traffic will often disguise itself as legitimate application traffic, effectively fooling many of the safeguards put in place. In addition, as demonstrated in this report, while not all traffic is malicious in intent, certain applications can become vehicles for intrusions and attacks.

Creating a productive environment can mean granting preferences to business-critical applications (VoIP, Salesforce, and Office 365) or curbing/blocking the use of non-productive applications such as social media, games and online shopping. In addition, application awareness is critical to plug security holes such as the use of anonymizers, online storage, webmail, and other "risky" web applications.

Application awareness and control gives enterprises and SMBs the flexibility and granularity to create and enforce their own specific AUP from the very simple to most sophisticated, according to business needs.

Conclusion

Safeguarding enterprises and SMBs from external and internal threats requires an enforceable Acceptable Use Policy with real-time network intelligence and application-level controls and that allow organizations to conclusively detect and prevent security breaches.

The cost of inaction is enormous. Organizations adopting such practices would benefit from a secure and more productive work environment and would also be able to more effectively use cloud applications and resources.

Methodology

Deep Dive Data Sets

The data in this report has been collected from enterprise customers and Communication Service Providers in order to give the most accurate representation of threats and points of concern. The Deep Dive data set is collected from a large North American enterprise with over 10,000 users and multiple locations, and a large European enterprise with about 20,000 users. Data was collected at the web/cloud access point.

Big Picture Data Set 1

The “Big Picture” data set was collected from Service Providers who provide Internet connectivity, hosting and cloud services to enterprise customers. As enterprises become more reliant on CSP and cloud service providers, they will demand more security from these providers.

Big Picture Data Set 2

Real-time data was collected and aggregated from several Communication Service Providers providing connectivity, security and other services to hundreds of SMB customers. The aggregated data has been anonymized to protect the identity of the service provider and their customers. The data was collected from over 200 SMBs.

References for Figure 1

http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/
http://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951/op-1
http://www.securityweek.com/target-data-breach-tally-hits-162-million-net-costs
http://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/
http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0
http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/

Allot CloudTrends Report

Q2/2015

About Allot Communications

Allot Communications Ltd. (NASDAQ, TASE: ALLT) empowers service providers to monetize and optimize their networks, enterprises to enhance productivity and consumers to enjoy an always-on digital lifestyle. Allot's advanced DPI-based broadband solutions identify and leverage network intelligence to analyze, protect, improve and enrich mobile, fixed and cloud service delivery and user experience. Allot's unique blend of innovative technology, proven know-how and collaborative approach to industry standards and partnerships enables network operators worldwide to elevate their role in the digital lifestyle ecosystem and to open the door to a wealth of new business opportunities.

www.allot.com info@allot.com

- **Americas:** 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA · Tel: (781) 939-9300 · Toll free: 877-255-6826 · Fax: (781) 939-9393
- **Europe:** NCI – Les Centres d'Affaires Village d'Entreprises 'Green Side', 400 Avenue Roumanille, BP309, 06906 Sophia Antipolis Cedex, France · Tel: 33 (0) 4-93-001160 · Fax: 33 (0) 4-93-001165
- **Asia Pacific:** 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104 Tel: +65 67490213 Fax: +65 68481015
- **Japan:** 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 · Tel: 81 (3) 5297-7668 · Fax: 81(3) 5297-7669
- **Middle East and Africa:** 22 Hanagar Street, Industrial Zone B, Hod-Hasharon, 4501317, Israel · Tel: 972 (9) 761-9200 · Fax: 972 (9) 744-3626

P/N D265039 Rev.1

Allot communications