zscaler
Secure. Everywhere.

The Zscaler 2014 Security Cloud Forecast

DNS AND SSL MOVE INTO THE SPOTLIGHT

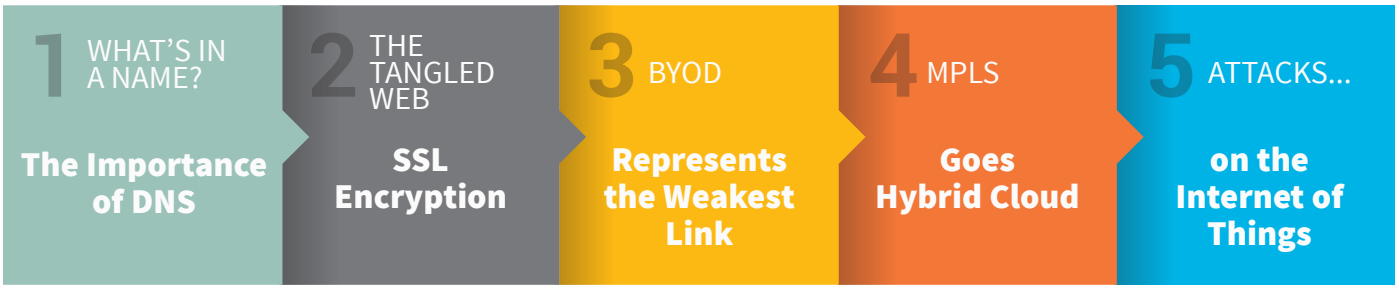
Contents

Introduction

As 2013 comes to a close, we have witnessed a number of significant cyber security stories, issues and trends pushed to the forefront of mainstream media, including attacks on the very mainstream media itself. Reports of well-organized Advanced Persistent Threats (APTs) abound from abroad, underscored by dozens of botnets constantly mutating into new permutations to evade detection. It has become evident that signature-based anti-virus is not enough to provide proactive protection against these advanced threats.

Fundamentally, the way we conduct business continues to radically change; between work PCs, personal PCs, smartphones and tablets, each employee is accessing corporate assets from as many as four distinct devices. Coupled with the rise of cloud applications, the enterprise network has become increasingly complex and heterogeneous, making it very difficult to maintain visibility and control of corporate assets.

In 2014, Zscaler sees these two major trends – the evolution of advanced threats and the complexity of cloud and mobile environments – increasingly intersect. In particular, here are five areas that information security practitioners should be considering as they plan for the New Year.



1 What's in a Name? The Importance of DNS

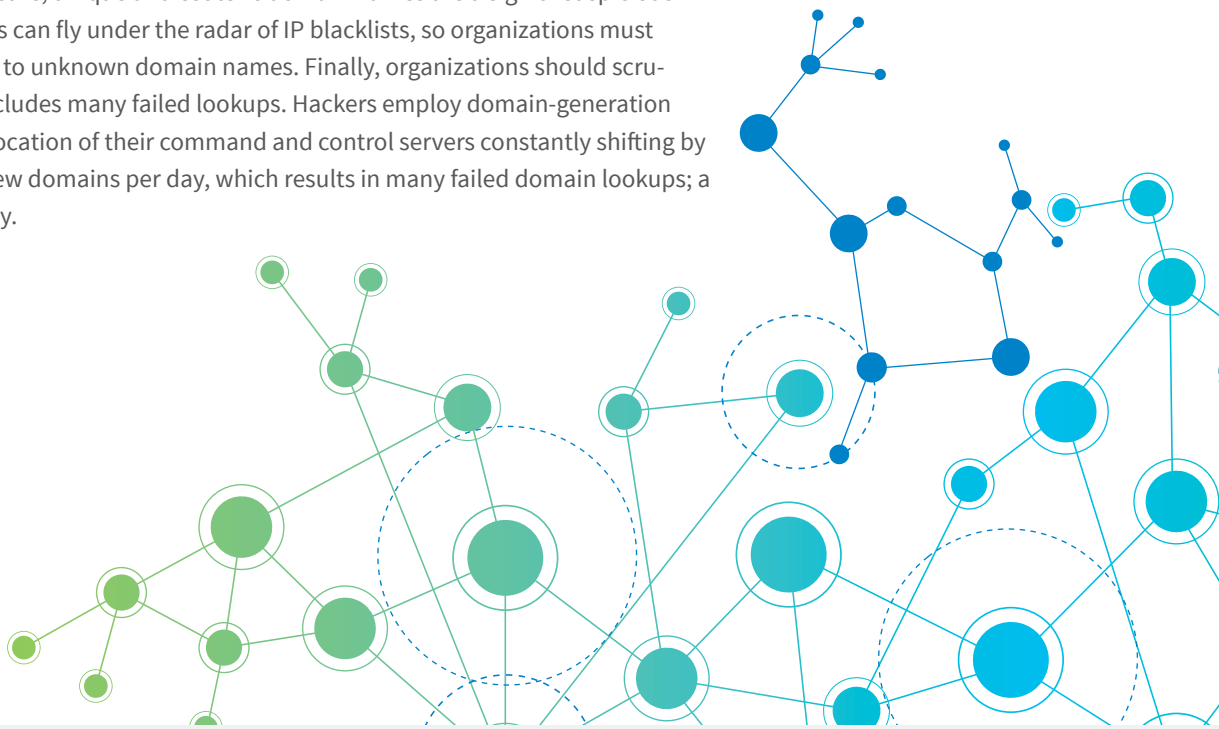
Attacks that leverage DNS servers are on the rise. These attacks take advantage of the fact that many organizations have no visibility into their DNS servers and that tens of thousands of DNS servers on the Internet are unsecured.

It was not a fluke that the largest distributed denial-of-service (DDOS) attack to date, which reached 300 Gb/s against Spamhaus, was achieved by exploiting DNS to magnify the attack. Attackers are using DNS techniques that mimic load balancing to move their servers in and out of view very quickly, a technique known as fast flux. In this way, malware is utilizing DNS to hide command and control networks.

Why DNS you may ask? There are several contributing factors. Its protocol is easy to use and powerful, it is an area of the network that is not typically monitored and it is foundational. Literally every device on the Internet is using DNS. Additionally, DNS can lower the cost of attacks since it can act as an amplifier for traffic.

DNS security practices are of critical importance moving into 2014. Much can be learned from analyzing patterns in DNS characteristics, such as age, obscurity and lookup failures, which all can provide significant indications of malicious activity, compromise or other threats. There is so much to be learned simply by analyzing DNS traffic. Young domains (recently registered) often can be a suspicious sign of malware infection.

Companies should monitor and investigate DNS traffic to domains that are less than a day or a week old; potentially even creating a policy to block access to any site less than 24 hours old. Likewise, obscure, unique and esoteric domain names are a sign of suspicious behavior. These domains can fly under the radar of IP blacklists, so organizations must monitor for connections to unknown domain names. Finally, organizations should scrutinize DNS traffic that includes many failed lookups. Hackers employ domain-generation algorithms to keep the location of their command and control servers constantly shifting by creating thousands of new domains per day, which results in many failed domain lookups; a sign of suspicious activity.



2 The Tangled Web: SSL Encryption

There is a dark cloud on the horizon: organizations are increasingly deploying cloud services, yet cloud services are increasingly reliant on HTTPS and SSL to encrypt traffic. Encryption protects traffic in transit but makes it difficult for IT departments to manage. Historically, Secure Socket Layer (SSL) encryption has been achieved by exchanging 1024-bit keys. However, in order to strengthen encryption, the industry standard will transition to 2048-bit keys by the end of 2013. Visibility into encrypted streams is important to secure corporate assets, but such visibility becomes five times more difficult with the move to 2048-bit keys. This holiday season, the process of upgrading SSL certificates for appliance-based solutions will be time consuming and expensive for organizations that continue to rely on outdated security hardware.

However, this implementation of stronger SSL is only half of the issue. It is equally important to note that major Web sites, such as Facebook and Google, have extended SSL encryption beyond its login pages for password security to protect all of its pages and communication. Expect SSL to be enabled by default with many major Web services in 2014.

This trend will not cease. It is compounded by the proliferation of mobile devices and public networks that make it trivial for an attacker to intercept and exploit unencrypted sessions. Unfortunately, these attacks are predominately targeting end users and using them as beachheads into corporate networks. As a result SSL is a must for any secure web application. It's only a matter of time before the majority of Internet-bound traffic is encrypted. To that point, recent discussions of HTTP 2.0 have suggested adoption of HTTPS as a default standard.

However, SSL traffic inspection can be very challenging, which creates a blind spot in a network that is consequently ignored. Inspecting encrypted traffic almost always results in performance degradation because the process must transparently decrypt traffic, inspect it and then re-encrypt it as it continues through the network. In a moderately sized network it simply may not be possible to enable SSL interception "as is" because the performance hit will be too great. This can apply even if that network's infrastructure is up to date. Modern firewalls and next-generation firewalls are not immune – they can see a performance hit of 5X or greater simply by enabling SSL inspection on web traffic.

The challenge of maintaining visibility and control of encrypted traffic will accelerate in 2014, making it a ripe attack vector for hackers. Attackers will increasingly use encryption in their botnet callbacks to command and control servers, which can be hard to detect without specific IP addresses. Without the ability to inspect encrypted traffic, botnet callbacks will continue to hide in the sea of encrypted traffic.

3 BYOD Represents the Weakest Link

A few short years ago, corporate users had a corporate PC and perhaps a personal laptop at home. Today, these same users also have a smart phone and a tablet – all of which connect to corporate assets – yet 3G wireless and public WiFi connections make it difficult to gain visibility and control into this traffic.

Mobile malware is still nascent, focused largely on phishing, adware and fake/cloned apps; however, the impact of mobile malware is potentially huge because mobile devices are the new weak point. As enterprises move corporate data to the cloud and its users connect through mobile devices, there is no traditional security appliance between the data and the device. Recall that the incursion point for the TJX data breach, in which 170 million credit card numbers were stolen, was through its wireless network, where no traditional security appliances existed at the time.

While both Apple and Android devices sandbox apps, they also each grant permissions in different ways. As a result, Zscaler expects to continue to see mobile attacks via email, Web and malicious third-party apps that are a hybrid of phishing and adware.

4 MPLS Goes Hybrid Cloud: Network-Delivered Security

Traditionally, large organizations have deployed a hub-and-spoke network model to manage and secure traffic through a central point. However, backhauling all of this traffic from numerous remote offices on a wide area network (WAN) through costly fiber connections and multiprotocol label switching (MPLS) is expensive and detrimental to performance.

In the past 10 years, WAN traffic ratios have turned upside down. Today, many networks are now carrying more Internet-bound traffic than internal traffic. Increasingly, enterprises are employing cloud-based technology, yet remain married to outdated paradigms of appliance-based security. It remains challenging to manage and protect much of this traffic, but this appliance-based model persists.

As organizations continue to grow globally and increasingly turn to the cloud, it can become time-consuming, inefficient and expensive to layer new cloud-based solutions on top of outdated network topologies. In 2014, Zscaler expects to see organizations move from securing its users through private networks into a public or hybrid cloud, rethinking their networks to reduce or eliminate backhauling by enabling users to connect direct-to-cloud.

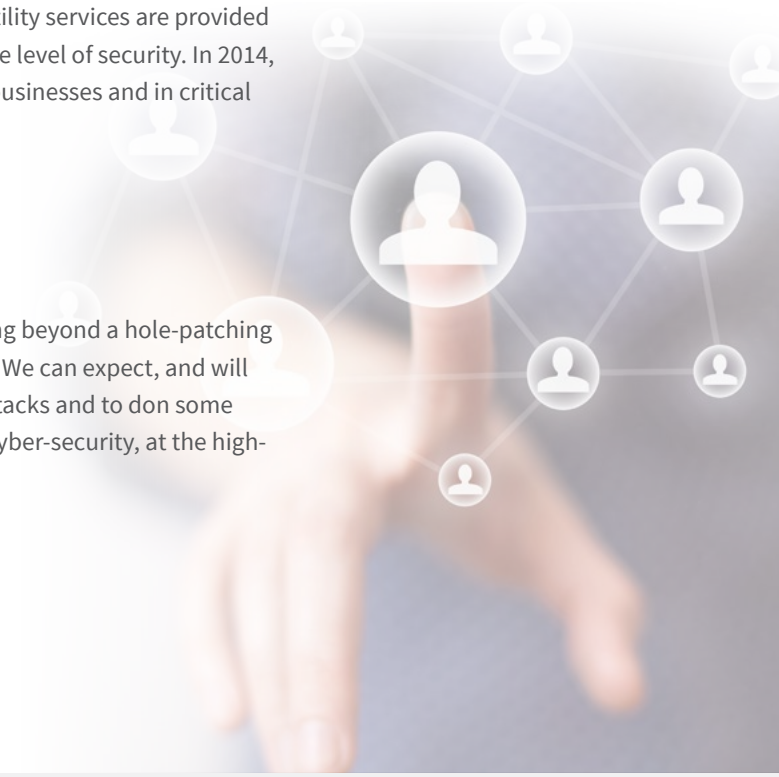
The corollary to this trend is a shift from the hardware-based security used with MPLS to network-delivered security needed for a direct-to-cloud network. Large and distributed organizations also struggle with routing and MPLS costs, yet never stop to consider that the same service provider delivering its network can also deliver its security.

Zscaler expects to continue to see mobile attacks via email, Web and malicious third-party apps that are a hybrid of phishing and adware.

5 Attacks on the Internet of Things

One of the most-lauded possibilities of IP networking is the ability to remotely control and monitor the activity of just about any device that uses electricity. The optimistic view of this is called the Internet of Things, a "smart network" that will obviate the need for meter readers and will allow people to see what's in their refrigerators from their phones. Many people already have several dozen items in their own home that can be remote controlled or monitored. The smartphone has in effect become the remote control for people's lives. Beyond this, virtually all the major water, power and communications equipment also has an IP address.

Herein lies the problem. Typically hardware vendors do not take Internet security into account – the Internet of Things has a security maturity level approximately equivalent to the World Wide Web in 1995. That means someone who can hack a wireless signal or steal a smartphone can open garage doors, turn off cameras, disable security systems, and the like. Most government-owned heavy infrastructure, such as that owned by the military, has some degree of protection, but in countries like the U.S., where public utility services are provided by private companies, there is no universal minimum required base level of security. In 2014, attackers will make attempts on the Internet of Things in homes, businesses and in critical pieces of infrastructure.



Conclusion

In 2014, we will turn our eyes toward protecting privacy and moving beyond a hole-patching approach to security to a more strategic and integrated approach. We can expect, and will need to prepare for previously underused forms and venues for attacks and to don some serious thinking and prioritization of strategic objectives around cyber-security, at the highest level.

CONTACT US

Zscaler, Inc.
110 Baytech Drive, Suite 100
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/groups/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com

zscaler
Secure. Everywhere.