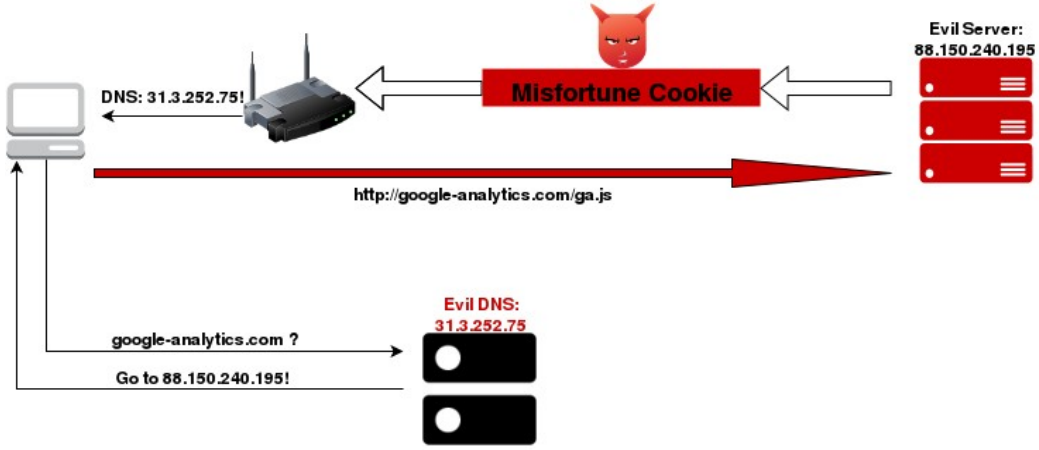
Cyber Threat Intelligence Report
“Mass-fortune Cookie”

The following report intends to share evidence founded in the investigation of a multistaged cyber-attack which I prefer to call “Mass-fortune Cookie Attack”. Aforementioned attack is aiming router devices online and exploits a vulnerability called `Misfortune Cookie (CVE-2014-9222)` which affect atleast 200 different models (*).

Title: Mass-fortune Cookie Attack
Investigator(s): Robin Dimyanoglu
Report Date: [17/01/2016]

Background
Discovery of this attack occurred in a sequence of events as I mentioned in my blog (*) earlier *-post in Turkish-*. As a result of my research it is clear that this attack pose a serious threat since the vulnerability provides privileged access to router devices, which may result in attacker intercepting the entire traffic of victim network. Fortunately this is not the case at the moment, but it is only a matter of the attacker's will.

Infrastructure



The infrastructure consist of two elements. A probe/web server (attacker uses the same server for both scanning* and as a web host*) and a DNS* server. First stage of the attack is exploiting Misfortune Cookie vulnerability to bypass login screen and acquire admin access to router's management panel. Following with a 2nd stage, attacker alters the router's settings in order to enforce devices in the network to use his own DNS server. The 3rd stage begins when someone queries the domain “google-analytics.com”. Attacker's DNS responds to that query with his own web server's IP address so that he can embed his own obfuscated JavaScript code (which will prompt the pop-up's) into the visited page instead of Google's.

Key Questions and Answers:

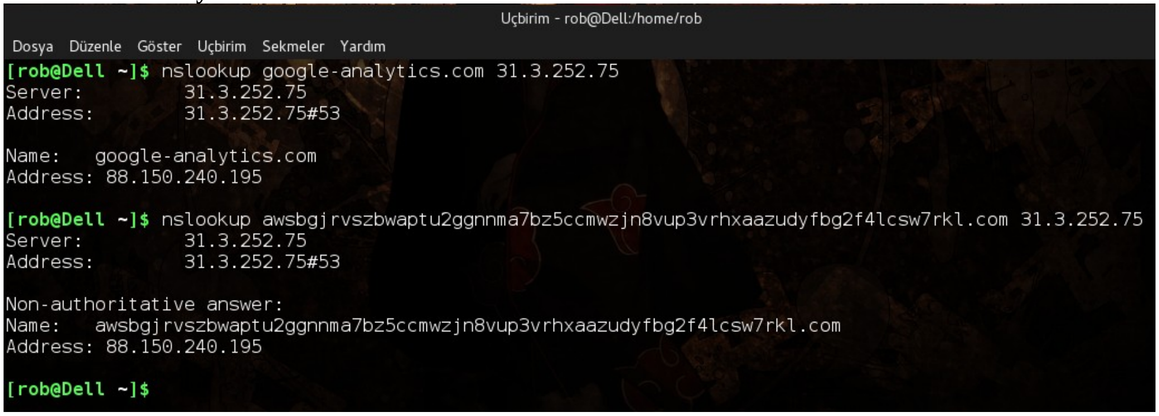
- How did the infection occur?
  Most probably by an automated script mass-scanning the internet for router devices.
- When did the malware infection occur?
  It reached my network on May 2015 but evidence shows that it started atleast a year ago.
- What vulnerabilities allowed the infection to occur?
  CVE-2014-9222
- What is the motivation behind this attack?
- Financial. The JavaScript code embedded into web pages appears to be prompting a pop-up ad. No other malicious behavior was detected.

Indicators

If one of these indicators appears to be present in your network, it's highly possible that you're also affected from the attack. You can also submit this data to your IDS/Firewall product to prevent a future attack.

IPv4:	31.3.252.75
IPv4:	88.150.240.195
IPv4:	104.28.28.127
Domain:	awsbgjrvszbwaptu2ggnnma7bz5ccmwzjn8vup3vrhxaazudyfbg2f4lcsw7rkl.com
Domain:	hidcptqmerifcusymaqddcomolsujibeptsmycmqsrwgrcmywshgnfpjhcc.com
CVE:	CVE-2014-9222
File-SHA1:	722a97b5ead1b089321f7af1e1e24279c9ec6cdb

Evidence and Key data elements



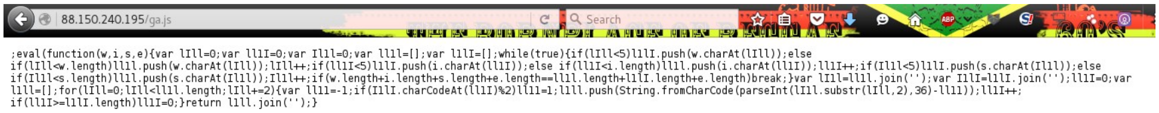
```
[rob@Dell ~]$ nslookup google-analytics.com 31.3.252.75
Server:         31.3.252.75
Address:        31.3.252.75#53

Name:   google-analytics.com
Address: 88.150.240.195

[rob@Dell ~]$ nslookup awsbgjrvszbwaptu2ggnnma7bz5ccmwzjn8vup3vrhxaazudyfbg2f4lcsw7rkl.com 31.3.252.75
Server:         31.3.252.75
Address:        31.3.252.75#53

Non-authoritative answer:
Name:   awsbgjrvszbwaptu2ggnnma7bz5ccmwzjn8vup3vrhxaazudyfbg2f4lcsw7rkl.com
Address: 88.150.240.195

[rob@Dell ~]$
```



```
;eval(function(w,i,s,e){var lIll=0;var ll1I=0;var Il1l=0;var ll1l=[];var l1lI=[];while(true){if(lIll<5)l1lI.push(w.charAt(lIll));else
if(lIll<w.length)ll1l.push(w.charAt(lIll));lIll++;if(ll1I<5)l1lI.push(i.charAt(ll1I));else if(ll1I<i.length)ll1l.push(i.charAt(ll1I));ll1I++;if(Il1l<5)l1lI.push(s.charAt(Il1l));else
if(Il1l<s.length)ll1l.push(s.charAt(Il1l));Il1l++;if(w.length+i.length+s.length+e.length==ll1l.length+l1lI.length+e.length)break;}var lI1l=ll1l.join('');var I1lI=l1lI.join('');ll1I=0;var
l1ll=[];for(lIll=0;lIll<ll1l.length;lIll+=2){var ll11=-1;if(I1lI.charCodeAt(ll1I)%2)ll11=1;l1ll.push(String.fromCharCode(parseInt(lI1l.substr(lIll,2),36)-ll11));ll1I++;
if(ll1I>=l1lI.length)ll1I=0;}return l1ll.join('');}
```

* De-obfuscated JavaScript code

Followup Actions and Lessons Learned

If your organization suffer from this attack do as the following;

1. Restore your router to factory settings and do a re-installation. Exploitation techniques used by this attack cause memory corruption and thus prevents you from re-accessing the interface.

2. After installation, update your router's firmware to latest version.

3. Clear DNS-cache and browser cache of all devices which was connected to the network.