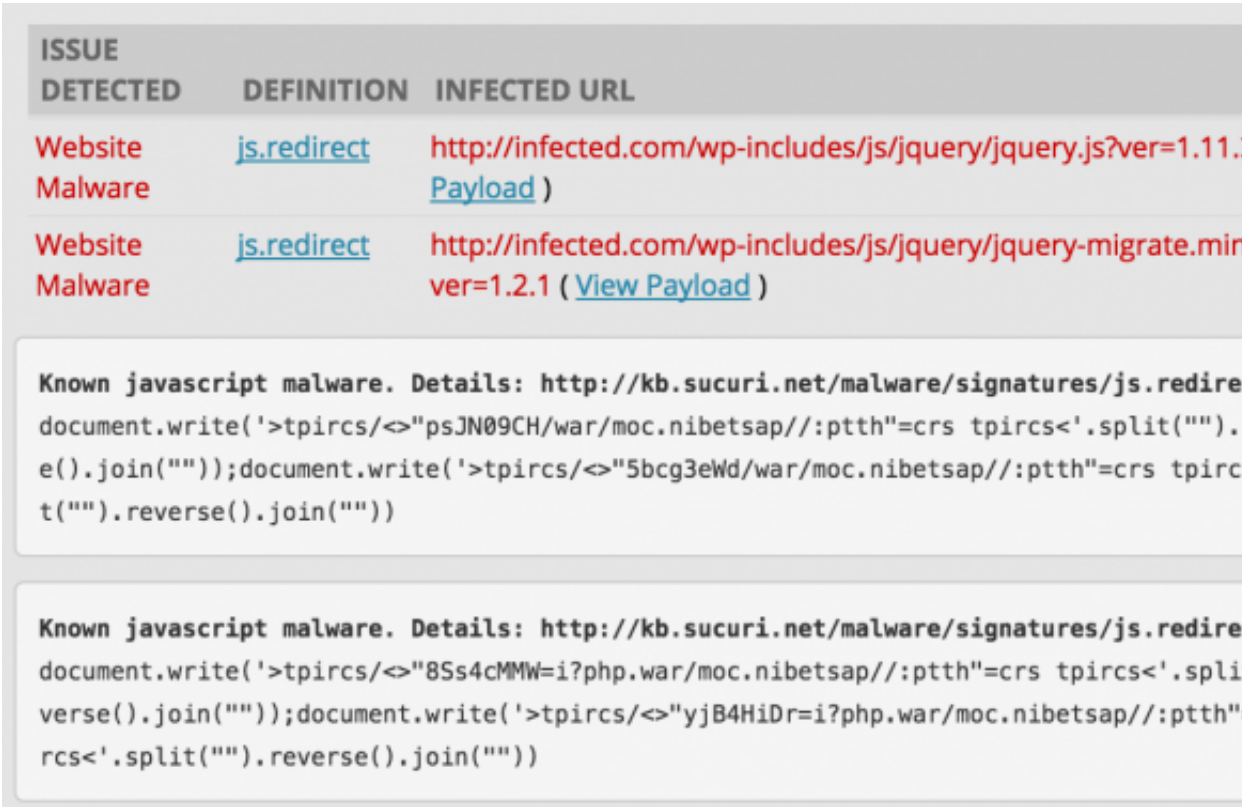
Malicious Pastebin Replacement for jQuery

By Denis Sinegubko on January 6, 2016 . + 4 Comments

Website hackers are always changing tactics and borrowing ideas from each other. One of t
website security is staying on top of those threats as they evolve. We wrote in the past abou
scripts and how hackers use Pastebin.com to host malware. This time, we will show you an
combines both of these techniques to spread malware using a fake jQuery Pastebin file.

Reversed URL Detected by SiteCheck

A couple of weeks ago SiteCheck began detecting WordPress sites with reversed JavaScrip
includes/js/jquery/jquery.js and **/wp-includes/js/jquery/jquery-migrate.min.js** files. As y
URL is written backwards inside the payload.



ISSUE DETECTED	DEFINITION	INFECTED URL
Website Malware	js.redirect	http://infected.com/wp-includes/js/jquery/jquery.js?ver=1.11. Payload)
Website Malware	js.redirect	http://infected.com/wp-includes/js/jquery/jquery-migrate.mir ver=1.2.1 (View Payload)

Infected jQuery detected by SiteCheck

When the code is reversed (e.g. ***war/moc.nibetsap//:ptth*** – is – ***http://pastebin.com/raw*** – backwards), it injects external scripts that load code directly from Pastebin. Previously, we s on infected Magento sites. There are strong signs that these two attacks are related, but this infection is interesting on its own, so let's look closer at these Pastebin links.

Pairs of Pastes

Both **jquery.js** and **jquery-migrate.min.js** are core WordPress files. Hackers gain access t replace the content of these files with their own short code.

In the case of **jquery.js** the attackers inject scripts from:

- **hxxp://pastebin .com/raw/HC90NJsp**
- **hxxp://pastebin .com/raw/dWe3gcb5** (or **hxxp://pastebin .com/sE8cX1Pi**)

… and in the case of **jquery-migrate.min.js** they inject:

- **hxxp://pastebin .com/raw/WMMc4sS8**
- **hxxp://pastebin .com/raw/rDiH4Bjy**

Now we have some interesting questions about these pairs of Pastebin links.

… Why do they inject two scripts?

… Why do they remove the legitimate code from WordPress core files?

… Wouldn't it break the infected sites?

We get answers to all these questions when we check the referenced pastes.

Referenced Pastebin Content

Let's first break down the content of each pair of Pastebin links.

- The paste **HC90NJsp** is actually the real source code of **jQuery** (v1.11.3)
- Its pair, **dWe3gcb5** is an obfuscated malicious script that redirects visitors to **hxxps://g**
- The paste **WMMc4sS8** is the real code of the **jQuery Migrate** (v1.2.1) library
- Its pair **rDiH4Bjy** is an obfuscated malicious script that redirects visitors to either **hxxps** or **hxxp://get .adobe.com .flashplayer .frogsland .com/flashplayer_20ga/**

Now we know that in each infected WordPress jQuery file, the first injected Pastebin script c removal of the original jQuery code (by loading the same code from pastebin.com) and the s injects the malware.

It's not clear why the attackers decided to remove existing code and then load it from Pasteb makes infection and reinfection easier. Instead of checking whether a **.js** file is already infec replace its whole content with code that is guaranteed to be correct. Since the jQuery code i be embedded in their attack scripts, they replaced it with a short external call to the same jQ on Pastebin. Why not? It works.

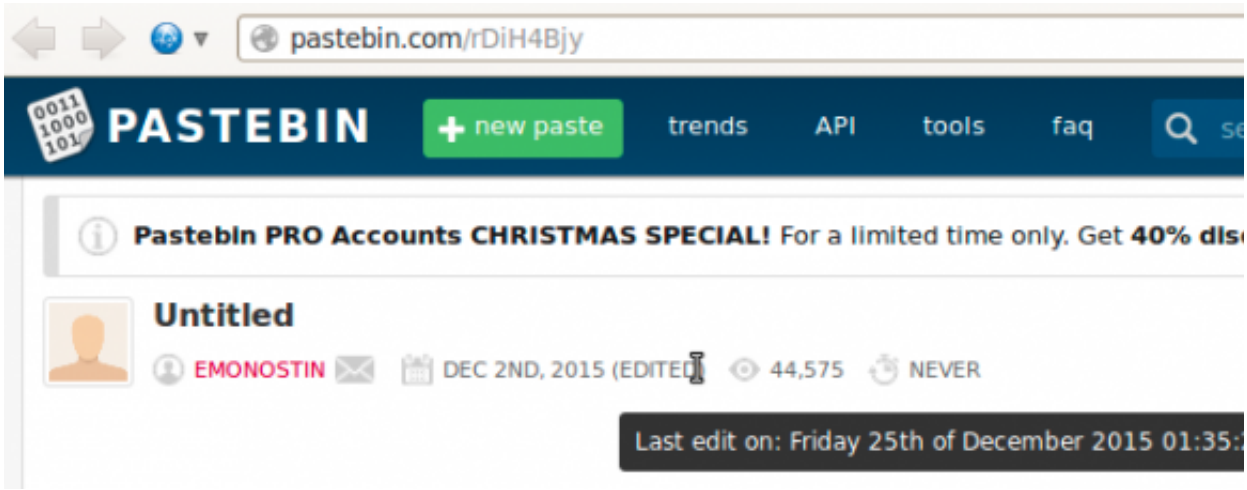
Pastebin User Info

The malicious pastes are not anonymous. There are two user accounts associated with ther

- Emonostin – created on Dec 2nd, 2015
- Jstoolshope – created on Dec 17th, 2015

Both users have only two pastes. Emonostin's pastes are the ones injected into **jquery-mig** Jstoolshope's are the ones from the infected **jquery.js**.

Why create malicious pastes under some user account if anonymous pastes can be equally injections? The answer is **flexibility**. Users can modify their own pasted content whenever t Anonymous pastes can't be modified. If the hackers need to change the URL they redirect tr just change the code of their paste and the URL will remain the same. As we can see in the these guys actually use this feature (the last modification was made on Dec 25th, 2015).



Malware modification date on Pastebin.com

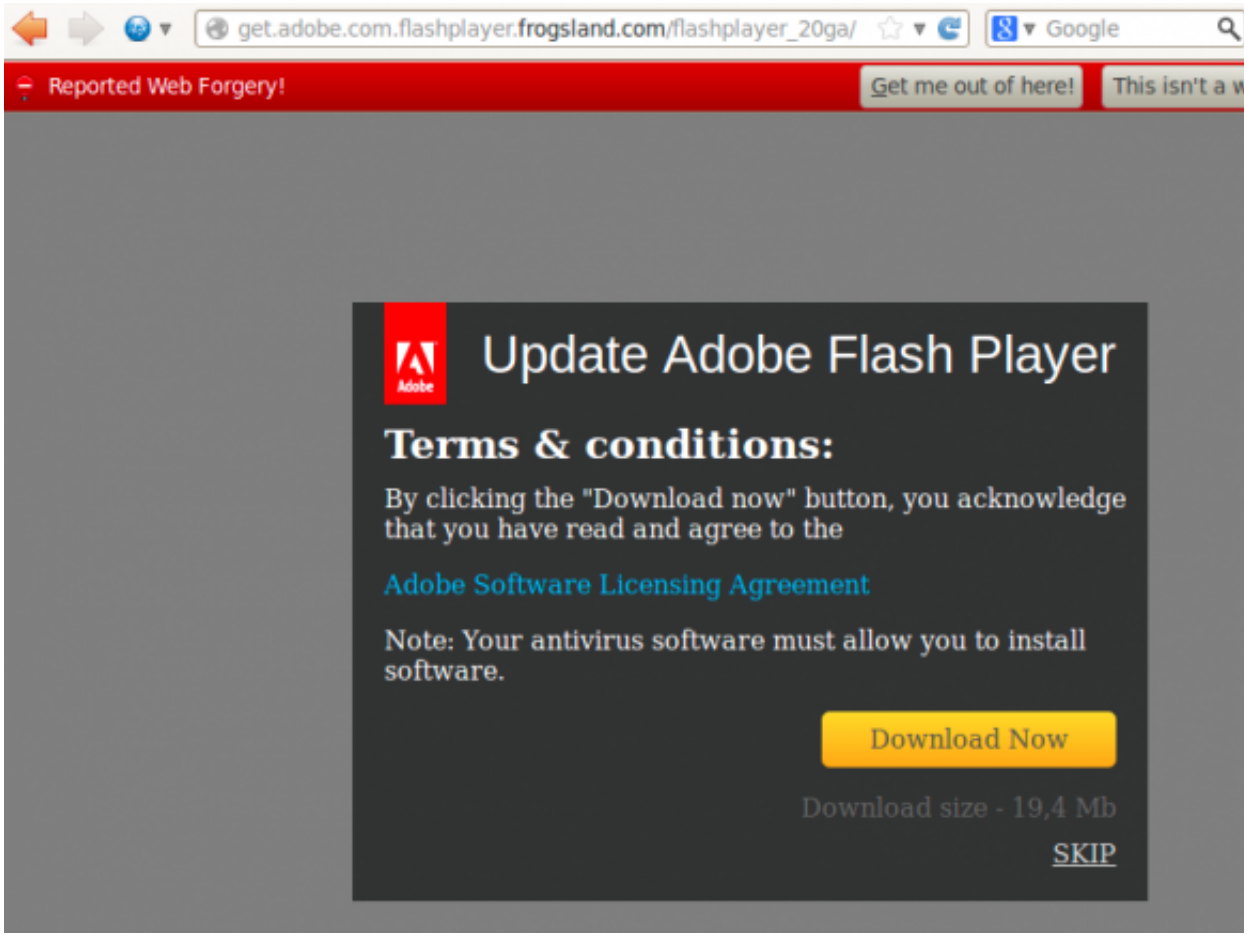
Pastebin also provides information about the number of views to each paste. Pastes from **jq** **20,000+ views**, and pastes from **jquery-migrate.min.js** have around **40,000 views**. At the t statistics look plausible since both pastes in the pairs have similar numbers of views — the i loads both at the same time. However, the Pastebin FAQ says that they do NOT include "*hit the RAW version of pastes*" and we know that infected sites load RAW versions of the paste counter may not represent real statistics for this attack. For more reliable statistics, we look l redirect.

Malicious Code

Now let's get back to the malicious code. It checks for presence of the "**tmid_no_session**" ("**tmid_no_check**" (in another version) cookie. If this cookie is set to "**1**", nothing happens (re Otherwise the script sets this cookie for **3** days and redirects the visitor to third party sites.

At this point the script from **jquery-migrate.min.js** redirects Windows users to **hxxp://get .a .flashplayer .frogsland .com/flashplayer_20ga/** and the rest of users go to **hxxps://goo .g** script from **jquery.js** redirects both Windows and non-Windows users to **hxxps://goo .gl/54**

The Windows redirect URL is self explanatory. You can see that it pretends to be a Flash pla It is already blacklisted by Google as phishing



Fake Flash player update page

Here's the VirusTotal analysis of the file this site pushes under disguise of a flash update: D
53

HFA (Hacked for Advertising)

The alternative redirect goes to "**hxxps://goo .gl/54Miz5**" which points to "**hxxps://go .pads
.com/afu.php?id=473791**". This is an affiliate link of some ad network.

Redirecting traffic from hacked sites to ad network links was one of the prominent trends of
more and more attacks that monetize compromised sites by pushing unwanted ads. The ad
such attacks, in turn, usually get money from advertisers. These advertisers pay to drive traf
sites or sites that trick visitors into installing malicious and potentially unwanted software (Uv
software hijacks their browsers and shows even more low quality scammy ads (do you see a

Ads and malware come hand in hand. In case of this "*jquery pastebin*" attack, they have two
branches: one for unwanted ads and one for malware. The Magento variant of this attack als
browser either to an exploit page or to some ad page — ads basically help monetize "unexp

You might know the MFA ("Made for Advertising" or "Made for AdSense") term, which is a bl
term that describes low quality spam sites created with the sole purpose of tricking people ir
clicking their ads. Now hackers adopted a somewhat similar approach that can be called HF
Advertising.

Goo.gl Link Statistics

Goo.gl links have a nice feature – you can see usage statistics of any shortened link. For ex
usage data for the redirect link during December https://goo.gl/#analytics/goo.gl/54Miz5/mor

Malware campaign statistics provided by goo.gl

We can see that hackers began using the"**hxxps://goo .gl/54Miz5**" redirection on Decembe
average number of redirects is more than **10 thousand per day** with a peak on December 2
thousand redirects. These numbers represent mostly unique redirected visitors since we k
sets a cookie that prevents redirection of known visitors.

Mitigation

In terms of mitigation, this attack has both upsides and downsides. The downside is if you si
malicious code from the **.js** files your site may stop properly working as the jQuery library file
now, so be careful. The upside is that those are core WordPress file so you have multiple ea
options:

1. Restore your site from the latest clean backup copy.
2. Update or re-install WordPress.
3. Restore only infected **.js** files. You can get canonical versions here (links for WordPres
    - http://core.svn.wordpress.org/tags/4.4/wp-includes/js/jquery/jquery.js
    - http://core.svn.wordpress.org/tags/4.4/wp-includes/js/jquery/jquery-migrate.min.j

As always, removing the malicious code is never enough. You should also scan your server
close the security holes that hackers used to break into your site in the first place. Make sure
website security detection system in place so you can be alerted if your website is targeted b

filed under: website security, wordpress security, magento security • tagged with: flash, jquery, malvertisi
hfa

About Denis Sinegubko

Denis is the founder of Unmask Parasites and a Senior Malware Researcher at Sucuri. F
at @unmaskparasites.

4 Comments Sucuri Security

Recommend 1 Share

Join the discussion…

Dustin Hein • a day ago

i was recently hired to update a website that was affected by this attack. i was able to re
code quite easily (many thanks to you folks for writing this article). so far my fixes have r
the cms and plugins were dramatically out of date, so i have everything updated and i ha
securi plugin, which is also very helpful. interestingly, it has reported 65 failed login atter
wordpress back-end. somewhat unnerving but very good to know. i have locked down t
question that they are trying to access. i am also considering password protecting the w
with a htaccess password... do you guys have any recommendations for how to deal wit
attempts? i guess they aren't so frequent that they would qualify as "brute force" but is t
similar? 65 password guesses in 8 hours or so? thanks!

Reply • Share ›

Leo F • 3 days ago

Thanks for the report, the reverse code was interesting! That's a varied mixture of techni

Reply • Share ›

Chris Q. • 7 days ago

I'm still having issues with the first jQuery round from the last post - I can't seem to loca
checked both my core jquery.js and jquery-migrate.min.js files against known clean cop
identical. I can remove the code from header.php but it always comes back within a cou
ideas of what I'm missing?

Reply • Share ›

Denis Sinegubko ↗ Chris Q. • 6 days ago

Hey Chris,

These two infections are different. You need to find and remove backdoors and c
to prevent reinfections.
https://blog.sucuri.net/2011/0...

Unlike the visitor-facing part of the infection, vulnerability and backdoor part may
different sites so it is hard to tell where exactly you should be looking for them.
Here's some general steps you should take to keep your site clean:

Here's some general steps you should take to keep your site clean:
https://kb.sucuri.net/remediat...

Reply · Share ›

ALSO ON **SUCURI SECURITY**

jQuery.min.php Malware Affects Thousands of Websites

15 comments • 2 months ago

Borja Cosar — i have this problem, but when i clean my joomla of encoded files like:' $j56="43dn_/}q …

Using WPScan: Finding WordPress Vulnerabilities

12 comments • 2 months ago

Canuckistani — For your average WP user installing this is beyond them - and they are the ones that need it most. Needs an installer for wider use.

Massive Magento Guruincsite Ir

28 comments • 3 months ago

Yinette — Hmm, I got the feeling back of the shoplift attacks. Loo sellers finally got a bidder.

Vulnerability Details: Joomla! Re Execution

10 comments • a month ago

Daniel Cid — There is quite a fev the web. We won't be sharing fr

Subscribe Add Disqus to your site Add Disqus Add Privacy

Blog Search

Search this website … Search

We love to socialize, let's connect..

Join 20,000 Subscribers!!

* indicates required

Email Address *

First Name

Subscribe

Categories

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:

dipaksaraf on WPScan Intro: WordPress Vulnerability Scanner

Phil Taylor, The Joomla Expert on Ransomware Strikes Websites

Dustin Hein on Malicious Pastebin Replacement for jQuery

Leo F on Malicious Pastebin Replacement for jQuery

financialhelp on Critical Persistent XSS 0day in WordPress

Toby Salmon on Critical 0-day Remote Command Execution Vulnerability in Joomla

seonewtool on My Website Was Blacklisted By Google and Distributing Email Spam

Denis Sinegubko on Malicious Pastebin Replacement for jQuery

allan on Payday Loan Spam affecting Thousands of Sites

Tony Perez on WordPress Plugin Alert – LoginWall Imposter Exposed

Recent Posts

Ransomware Strikes Websites

Malicious Pastebin Replacement for jQuery

Fake Media Download Sites

Using WPScan: Finding WordPress Vulnerabilities

Vulnerability Details: Joomla! Remote Code Execution

Critical 0-day Remote Command Execution Vulnerability in Joomla

Website Malware – Evolution of Pseudo Darkleech

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?