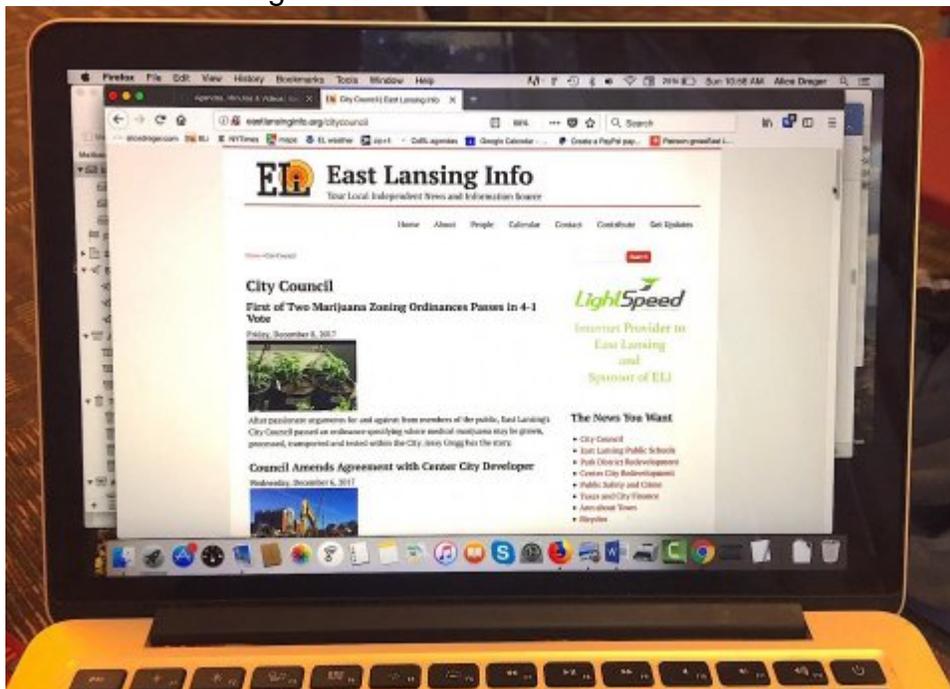Home > Hacker Attacks on ELi's Website Keeping Our Techs Busy

Hacker Attacks on ELi's Website Keeping Our Techs Busy [1]
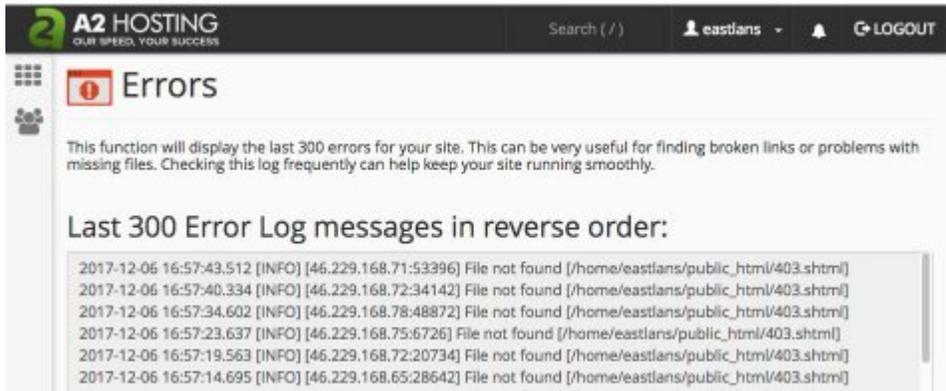
Monday, December 18, 2017, 7:32 am
By:
Lisa Lees and Morgan Lees

ELi?s Publisher, Alice Dreger, has asked us?the ELi tech management team?to explain why a site like ELi, that looks simple on the surface, in fact requires substantial tech management. She?s also asked us to explain why ELi really has no choice but to do a very labor-intensive software upgrade in 2018, assuming ELi meets its sustainability goal and continues through 2018.

The Internet is a dangerous place, filled with wandering robots, hooligans and downright villains. The news repeatedly reports on websites that have been hacked, with information stolen. Because ELi does not ask readers to subscribe with user logins, our site contains no personal data, but that doesn't mean it isn't under attack just as much as every other website.

Below: A screenshot showing robots hitting ELi?s site over and over.

Errors

This function will display the last 300 errors for your site. This can be very useful for finding broken links or problems with missing files. Checking this log frequently can help keep your site running smoothly.

Last 300 Error Log messages in reverse order:

2017-12-06 16:57:43.512 [INFO] [46.229.168.71:53396] File not found [/home/eastlans/public_html/403.shtml]
2017-12-06 16:57:40.334 [INFO] [46.229.168.72:34142] File not found [/home/eastlans/public_html/403.shtml]
2017-12-06 16:57:34.602 [INFO] [46.229.168.78:48872] File not found [/home/eastlans/public_html/403.shtml]
2017-12-06 16:57:23.637 [INFO] [46.229.168.75:6726] File not found [/home/eastlans/public_html/403.shtml]
2017-12-06 16:57:19.563 [INFO] [46.229.168.72:20734] File not found [/home/eastlans/public_html/403.shtml]
2017-12-06 16:57:14.695 [INFO] [46.229.168.65:28642] File not found [/home/eastlans/public_html/403.shtml]

Robots attempt to hijack our forms to send malicious email, they attempt to hack the site and capture it for use in a bot net, and not a few robots and people wander the net simply trying to destroy whatever they can. (ELi has only been successfully hacked once, because of a serious core security hole in the software we are using, and that was quickly detected and fixed.)

How often is ELi accessed by a robot or other non-human activity? It's not once a day, or once an hour, or even once a minute; it's several times each second, all day long, every day. Actual humans make up only a tiny fraction of the accesses to ELi and indeed of the enormous traffic on the Internet.

Below: Screenshot illustrating that most of the logged activity on the site isn?t an ELi staff person trying to do something ELi-intended.

Because of the reality of today's internet ecosystem, strange things happen sometimes to our system, without warning, requiring immediate tech attention. Recently a mistaken change to one line of one file on the server side of the site revealed a problem with one part of one module in the main software part of the site.

It turned out that this module was being relentlessly targeted by bots, and now began generating thousands of empty files each day in a temporary directory. This caught the attention of the tech team, leading to a search for the problem, and the implementation of more effective ways of keeping bad bots off the site and cleaning up after them.

You might use internet sites like Facebook without ever thinking about stability and security.

That?s because at commercial online systems like Facebook?which are using your participation to make a profit?tech managers provide stability and security without you ever realizing it.

For a nonprofit site like ELi, which is highly interactive, maintains sizable archives, and is a fully independent site, we have two tech managers on call to provide stability and security. That you don?t see problems at ELi is the result of that necessary tech management.

Here?s a deeper look behind the scenes, to give you a sense of what we do and why it requires funds to manage:

Eastlansinginfo.org (ELi) is a website created using the Drupal content management system (CMS). Drupal was chosen over other CMS packages such as Joomla and Wordpress because of its reputation for supporting customization and fine-tuning. Drupal is widely used for large, high traffic sites (such as whitehouse.gov), and is arguably the best 'free' CMS package, though it is often said that Drupal requires the highest level of technical skill to manage properly.

The ELi site was originally created in July 2012 on hosting provider Dotster, then moved in August 2014 to hosting provider LiquidWeb, and finally (we hope) moved at the end of August 2016 to hosting provider A2 Hosting. The hosting moves were made to improve site performance and our control over the server-side management of the site.

Beginning with the reboot of ELi as a non-profit corporation in May 2014, the ELi management team met with its tech team and discussed what they wanted in terms of changes in site appearance and features. The tech team then proposed several ?themes? from which to choose as starting points. (A theme determines the site's basic features, such as colors, number of columns, header and footer areas, location of navigation bars, slide show, and so on.)

Below: A screenshot showing the ?backstage? management of ELi?s webpage structure.
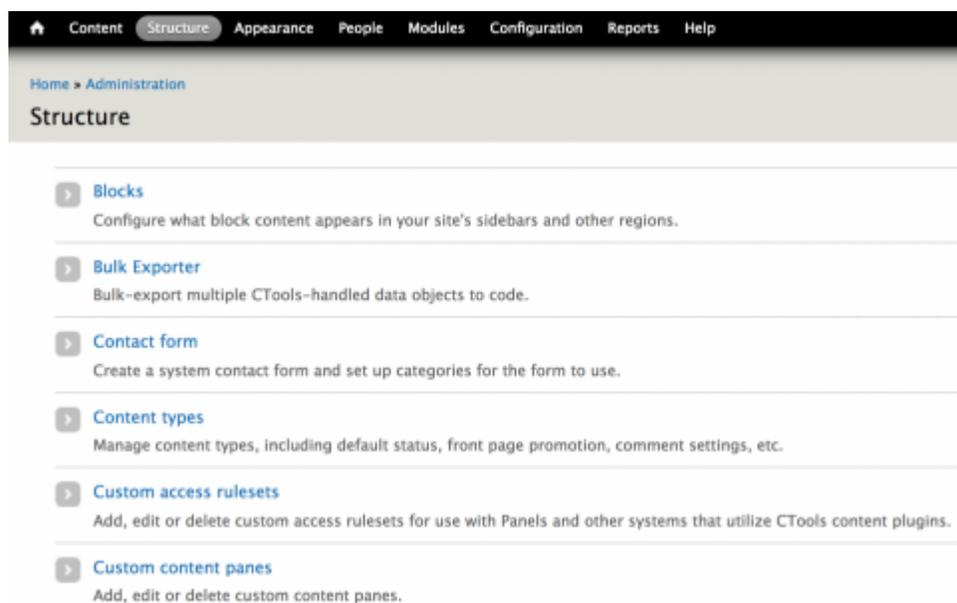
Once a theme was chosen, the tech team proceeded to configure and modify the theme. Over the past several years, the theme has been changed once again, and extensively modified at the

code level.

A number of other changes have been made in the way articles are named and organized in order to help readers find what they want. The original slide show was eventually replaced with the current map, using pins for links to articles. A system was put in place to allow articles to be published in the future (written on one day to not be visible until a future day). The Top Story feature was added. In other words, ELi has been a rather dynamic site in terms of features and organization.

To support the modeling and testing required by all these changes to the ELi production website, the tech team operates a duplicate test version of ELi on a different but identical A2 Hosting account (this expense is donated by the tech team because it makes their life easier and less stressful), and each member of the tech team has also set up their desktop computer to run a copy of the ELi site locally.

Drupal is a complex and marvelous system, but as with any computer-based system, it is in some ways extremely fragile. A single character out of place in a module or system file is enough to prevent the site from working at all, resulting in a stark, blank screen. This is why testing must be done on other than the production site, and why the tech team is obsessive about making file and database backups, so that the production site can be rebuilt if something goes wrong.

Below: This screenshot shows how most of ELi and all of its content lives in databases managed by the tech team.
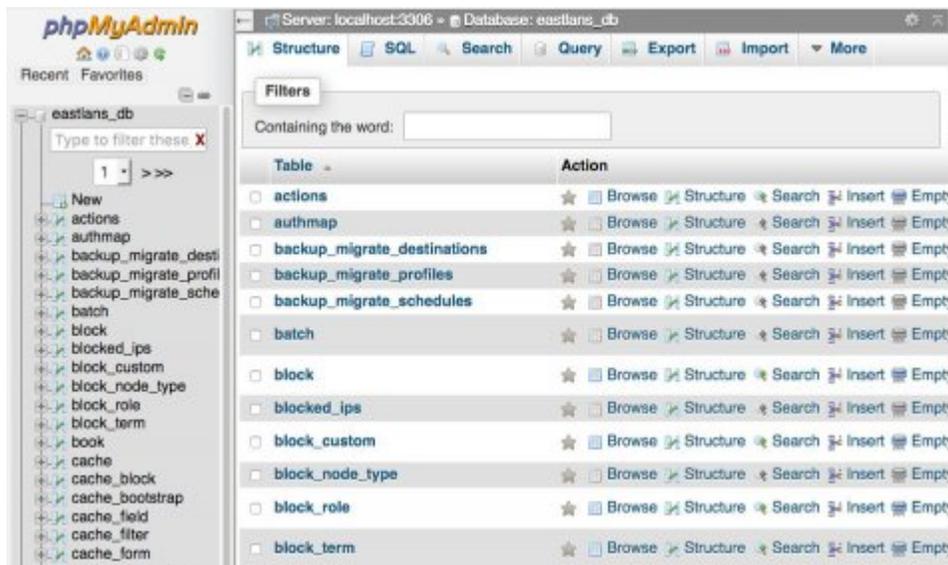
One member of the tech team is on the Drupal security email list, and finds out each week whether any parts of Drupal have been flagged with security errors. Drupal consists of a core set of code plus many add-on modules. Modules are easy to update, from within the Drupal back end, but updating Drupal core code is more difficult. Any module update is tested first on the test version of the site; core updates are tested first on a desktop version of the site, then on the test site.

The tech team monitors and backs up ELi every day, logging into the back end of the site to

check error logs, looking for trouble. We also keep an eye on the server side of things, outside Drupal, to check on resource usage, block bad robots and perform checks and backups on non-Drupal aspects of ELi such as its mail system.

At the time of site creation, we were using Drupal 7.14, relatively early in the Drupal 7 life cycle. We are now at Drupal 7.56, near the end of the Drupal 7 life cycle. We are beginning to work on plans to migrate the site to Drupal 8 (now early in its life cycle at 8.4.2).

In 2018, the move to Drupal 8 will be necessary, as Drupal 7 will cease to receive security updates when it reaches end-of-life (once development on Drupal 9 begins). This move will not be simple. With the increase in major version number, the Drupal developers are free to change anything about the internals, including the database layout and the scripting language used to write modules and themes.

ELi has published over four thousand articles, containing many thousands of photos and PDF files. These all must be moved to a differently structured database and file system. The number of articles requires that this process be automated. The tool used to do this will have to be modified to fit our needs, and repeated runs made until the end result is as good as possible. It is likely that further tweaks to content by hand will then be necessary.
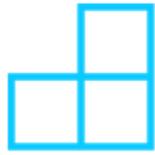
And, of course, the move to Drupal 8 provides a chance to change ELi's appearance and features, so some redesign will probably take place as a prelude to the move. This will all need to happen while the Drupal 7 version of ELi continues to operate for you, so there will need to be an entire set of Drupal 8 version ELi test sites also. The final migration probably will require a period during which the Drupal 7 site is frozen while the content is migrated, checked and tweaked. The entire process will take weeks, or more likely months.

Though mostly invisible to you, the intended user of ELi, tech support for an active website is a necessary and continuous task. There have been dozens of times in its life that publishing at ELi would have come to a halt because of one technical problem or another without an on-call technical staff.

Related Categories:
Your ELi [2]

ELi is a member of INN and LION Publishers

This news is brought to you by our financial supporters!