S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

BE **WARNED**, STAY **PROTECTED**.

October 2014

Newsletter

Dear Colleagues,

Cyber Security Center CERT-GOV-MD is glad to announce its newsletter, as part of its proactive services. This newsletter compiles events of IT security for October 2014, and has the scope to inform you about the latest information security news, trends, tips and threads discovered. We hope this information will help you in your day-to-day activities, either if you are part of technical staff, dealing with sensitive information, or just a regular computer user.

BE WARNED, STAY PROTECTED,
CERT-GOV-MD Team

Contents:

Useful advices:

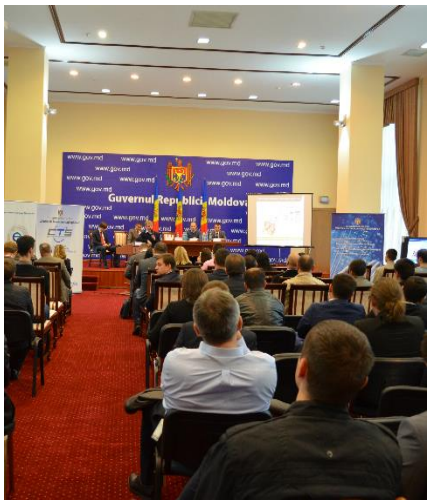
Drupageddon - the biggest challenge of 2014 for Drupal web sites

Drupageddon is a name used to designate a severe vulnerability discovered in the Drupal-based web sites. The term itself, apparently, was obtained by the way of combining the words "Drupal" and "Armageddon" to demonstrate catastrophic impact of the most dangerous, for Drupal content management system, software error of 2014.

There are a couple factors, in the discovered vulnerability, which left many system administrators without sleep for a couple of days or even weeks:

1) The ease of building and automating exploits, which make use of this error;
2) A quite limited time (~ 3-7 hours) to patch the announced vulnerability before Drupal web site should be considered compromised;
3) Time-consuming web site recovery procedures - system administrators had to recover the web sites from a backup and to restore all missing content, or - in case the backups were missing or damaged - to build affected web sites from scratch.

According to the Drupal.org it is estimated that between 100 000 and 800 000 of Drupal web sites became compromised as the result of automated attacks, which makes this vulnerability one of the biggest challenge of modernity for the Internet community.



Cyber security experts all over the world participated at the international conference "Cyber Security in Moldova: Challenges, Trends and Responses"

The international conference, organized by Cyber Security Center CERT-GOV-MD as a part of European Cyber Security Month initiative, took place on Wednesday, 15 October 2014, at the premises of Government of the Republic of Moldova.

Within the event specialists, researchers, engineers, scientists, developers of solutions and experts met together in order to discuss the current situation, trends, solutions and challenges that face the Republic of Moldova in the domain of cybersecurity.

Read more at:
http://cert.gov.md/noutati/international-conference-2014.html

"We don't see things as they are, we see them as we are." - Anaïs Nin

Insiders - an enemy within

Insiders represent a significant problem for IT security teams. To deal with it many organizations have built up a huge array of network security systems and controls, such as data loss prevention systems, encryption, firewalls, IDS and anti-virus packages – but these are failing to deliver total security since different insiders have differing motives, skill sets, risk profiles and access privileges.

While there is no way to address all possible attack scenarios the following approaches can minimize the risk of an insider thread:

- **Monitor user activity**. For example, if a certain user is accessing hundreds of documents that aren't reasonably justifiable as being within their remit, then the alarm should be triggered and the breach can be dealt with much sooner.
- **Set access rights based on user roles**. Ensure that only those employees that have a real need to access a given resource have the ability to do so.
- **Separate duties**. Separating duties prevents subversion or collusion, and avoids implicating personnel in activities in which they had no part.

Read more at:
http://www.information-age.com/technology/security/123458593/cyber-enemy-within-rise-insider-threat

Stay safe on the Web

While the Web is an essential part of our lives, it is important to understand the danger that might come from the underlying technology.

Cybercriminals are using various methods in order to penetrate into victim's computer. However, most of them have a single goal - to lure the victim into navigating to a malicious web site, which usually hosts an exploit pack - a collection of malicious scripts that targets browser, add-ons and third party software loaded by the browser.

Down below you will find attack techniques used by cybercriminals as well as countermeasures, which can help to avoid the infection.

Attack techniques:

1) ***Spam messages***. It includes messages sent by email, SMS and instant communications systems, via social networks, private messages on forums or a link to an infected site.
2) ***Malicious advertisements***. On-site advertisement, pop-ups, hidden banners can redirect the user to a malicious site. On occasion, these malicious banners can even penetrate into honest banner networks. Cases like this have affected the Yahoo Advertising banner network and even YouTube.
3) ***Promotion via search engines***. Modern users often go to search engines to find necessary information or services, so the easier it is to find a given site the more visitors it will get. Cybercriminals can use a collection of techniques in order to raise the position of a malicious web site in the results given by search engines.
4) ***Infected legitimate sites***. Sometimes cybercriminals infect popular legitimate sites in order to spread their programs. These might be high-traffic news resources, internet shops or portals and news aggregators.
5) ***Direct download by users***. Quite often cybercriminals don't need ingenious and expensive tools to insert their malicious programs onto users' computers. Users can simply be fooled into downloading and running malware themselves.

Countermeasures:

- Always pay attention to what you are doing on the Internet: which sites you visit, which files you download and what you run on your computer;
- Do not trust messages from unknown users and organizations, do not click on links and do not open attachments;
- Regularly update frequently-used software, especially software that works with your browser;
- Install up-to-date defenses and keep anti-virus databases current.

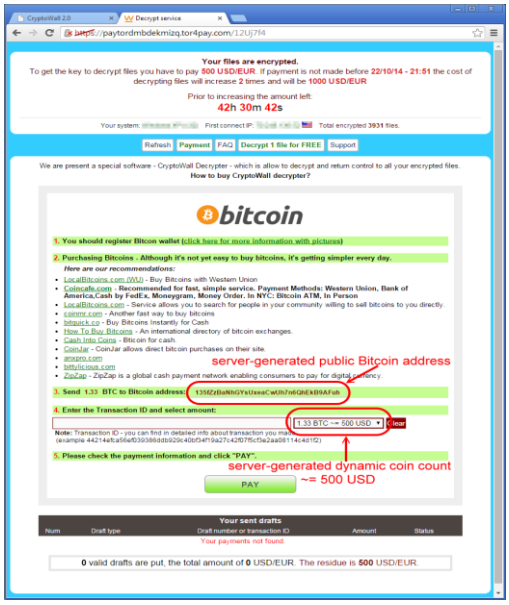
Read more at:
https://securelist.com/analysis/publications/66347/internet-predators/

Malvertising becomes more popular

Researchers at information security company "Proofpoint Inc" have detected numerous popular websites hit by a malvertising campaign. Among affected web sites were Yahoo!, AOL and Match.com. In total more than 3 million visitors per day were potentially exposed to this threat.

Malvertising is a term used to denote malicious variety of online advertisements generally used to spread malware through legitimate advertising networks luring the victims to visit a malicious web-site.

Proofpoint found that without having to click on anything, visitors to the impacted websites might have been stealthily infected with the CryptoWall 2.0 ransomware. The attackers using FlashPack Exploit Kit exploited a vulnerability in the Adobe Flash Player plugin and installed CryptoWall 2.0 on end-users' computers. Similar to the behavior of other "ransomware," CryptoWall then encrypted the end-users' hard drive and not allowed access it until the victim paid a Bitcoin fee over the Internet for the decryption key.



Since all Bitcoin translations are public, the researchers were able to study one of coin flows and found that for 5 days since it was active it received 24.35 BTC, which is roughly $9,354 USD. They estimated that on a daily basis, this campaign was generating at least 40 addresses, so for 30 days of the campaign, attackers may have generated a ransom amount of at least $750,000 USD.

It is recommended to use the following best practices in order to protect yourself against infection:

1) ***Regularly backup important data and keep it at the external storage device.*** It allows you to clean infected system and to recover all encrypted data from a clean backup without paying the ransom;
2) ***Keep your operating system, web browser and it's plugins up-to-date***;
3) ***Enable function "Click to Play" in your web browser***. By enabling Click to Play, web content that requires plugins such as Java, Flash, Silverlight, Adobe Reader, QuickTime, and more will be disabled by default. Users must manually Click to Play plugin content on any given web page in order for the content to load. This provides a useful security control, so that malicious content is not automatically executed by the browser.
   - ***In Chrome***. Open Settings -> Show advanced settings -> Privacy -> Content settings -> Plug-ins -> Choose "Click to play" -> Restart Chrome;
   - ***In Firefox***. Open FireFox -> Type about:config into the address bar and hit Enter -> Click the "*I'll be careful, I promise button to proceed*" -> In the search bar that appears at the top of the page, enter *plugins.click_to_play* -> Right-click the configuration setting and select Toggle. The value column should change from false to true -> Restart Firefox.

Read more at:
http://www.proofpoint.com/threatinsight/posts/malware-in-ad-networks-infects-visitors-and-jeopardizes-brands.php

Tor: Anonymity is not equal to Security

Tor is a computer network that makes possible to navigate over the Internet anonymously. The navigation process could be briefly described in the following way: a tor client securely transmits the data to the tor network; the tor network selects a random path and forwards the data; the last node in the Tor network the data go through (sometimes referred as "Tor exit node") decrypts the data and sends it to a final destination.

The researchers from Leviathan - an information security company - found an exit node that silently infected with a malware all binaries that were transmitted through it.

Further inspection showed that malware authors used sophisticated technique, which allowed them to bypass simple self-checking mechanisms of the original binary while keeping original icon intact.

It is recommended to use the following countermeasures in order to stay safe during the Tor usage:

- **Always check file integrity**. That is usually done by comparing hash string of a file from the web page you initiated the download with hash of received binary;
- **Verify digital signatures**. Ensure:
  1. That binaries you downloaded are signed
  2. The signer is trusted.
  3. The certification authority that authenticated the signer is trusted.
- **Keep your applications up-to-date**. Remember that not only binaries could be dangerous to open, but also regular files like PDF, Word or Excel.

Read more at:
http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries/

About us

Cyber Security Center CERT-GOV-MD is the governmental cyber emergency response team, created within S.E. Center of Special Telecommunications on 18.08.2010 upon the approval of the Government decision nr. 746 "Regarding the updated action plan Moldova - NATO".

Central point of contact

CERT-GOV-MD is the central point of contact for all cyber security problems for public administration authorities in the Republic of Moldova.

Alerting us about security incidents

By e-mail to info@cert.gov.md
By telephone on (+373 22) 820-900 (ask for the CERT-GOV-MD) on business days from 8:00 to 17:00

Find us on the Web:
www.cert.gov.md

BE **WARNED**, STAY **PROTECTED**

WordPress Security Tips

Chetan Soni, a cyber-security expert and penetration tester, has published security tips for protecting web sites, which are using WordPress platform as its content management system.

According to these security tips, in order to protect a WordPress web site the system administrator should use the following advices:

1. ***Secure the htaccess file.*** Hackers can use the .htaccess file to redirect the users to malicious sites. To restrict access to the .htaccess file add the following lines to the your htaccess file:

```
<Files .htaccess>
 order allow,deny
 deny from all
 </Files>
```

2. ***Disable the Theme/Plugin Editor***. That prevents hackers to makes significant changes to the WordPress website. In order to do it navigate to the *wp-config.php* file and add the following line of code:

```
define('DISALLOW_FILE_EDIT', true);
```

3. ***Protect the wp-config file***. Hackers try to access this file to destroy the whole website. Change the permissions of the file, so that only a Web server can access it;
4. ***Change Table Prefix***. The WordPress database consists of many tables, which have standard names like *wp_users, wp_options, wp_posts* etc. If a hacker knows where user details are stored, he will try to exploit this. It's recommended to change default prefix *"wp"* to something else. To do this, open your *wp-config.php* file, which is located in the WordPress root directory and change the table prefix line like this:

```
$table_prefix = 'wp_chetansoni123_';
```

5. ***Use WordPress Security Plugins***. Many different security plugins available, which address security issues of WordPress.
6. ***Change Security Keys***. Security keys are used as a salt for generating authentication cookies. If the site gets hacked, it is highly advisable to change these keys with fresh ones.
7. ***Always Update WordPress Themes and Plugins***. WordPress updates are often issued for the purposes of fixing potential security issues.
8. ***Prevent Directory Browsing***. Directory browsing allows anyone to list all of the files of site's directories. Add the following line to your .htaccess file:

```
Options -indexes
```

Make sure to add an empty line.

Read more at:
http://dl.packetstormsecurity.net/papers/general/8in1wordpress.pdf

Disclaimer: