S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

April, 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 April 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.

"Heartbleed" vulnerability found in TLS protocol implementation allows an attacker to steal sensitive information.

11.04.2014

A security bug called "Heartbleed" was found in the open-source OpenSSL cryptography library, widely used to implement the Internet's Transport Layer Security (TLS) protocol. This vulnerability results from a missing bounds check in the handling of the TLS heartbeat extension.

Normally Heartbeat Extension is used to test TLS/DTLS secure communication links by allowing a computer at one end of a connection to send a "Heartbeat Request" message, consisting of a payload, typically a text string, along with the payload's length as a 16-bit integer. The receiving computer then must send the exact same payload back to the sender.

Using a malformed heartbeat request with a small payload and large length field to the server in order to elicit the server's response, permitting attackers to read up to 64 kilobytes of server memory that was likely to have been used previously by OpenSSL.

This allows an attacker to retrieve: private keys, user data, usernames and passwords, which allows him to launch man-in-the-middle attacks and/or to hijack the identity of the user whose credentials were compromised.

The affected versions of OpenSSL are OpenSSL 1.0.1 through 1.0.1f (inclusive).

To address this issue it's recommended to upgrade OpenSSL to version 1.0.1g, to generate new certificates, to change all user passwords.

Web service http://filippo.io/Heartbleed/3 allows you to check whether your web site is vulnerable to "Heartbleed" attack.

Read more at: http://en.wikipedia.org/wiki/Heartbleed

Contents

Watch out malicious Firefox add-ons

17.04.2014

A Metasploit developer Joe Vennix published three new modules for Metasploit application which allows to steal browser cookie, history and saved passwords from Firefox users.

A hacker is able to exploit Firefox web browser either by convincing the user to install an untrusted add-on or by finding a privilege escalation exploit in Firefox itself.

It's recomended to users to avoid installing untrusted addons and to update their Firefox installations to latest available version.

Read more at: https://community.rapid7.com/community/metasploit/blog/2014/04/17/weekly-metasploit-update

Did you know?

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

"Every organization should make security awareness training part of its defense in depth strategy." Craig Kunitani, COO with Security Mentor.

Google patches android icon hijacking vulnerability

15.04.2014

Researchers at FireEye have identified a vulnerability affecting Google Android that could be exploited to lead users to malicious sites.

The issue allows a malicious app with 'normal' protection level permissions to target legitimate icons on the Android home screen and modify them to point to attack sites or the malicious app itself without notifying the user. The issue has been acknowledged by Google, which has released a patch to its OEM partners.

To address this vulnerability it's recommended to upgrade your Android device to latest version of firmware.

Read more at: http://www.securityweek.com/google-patches-android-icon-hijacking-vulnerability

Viber is vulnerable to man-in-the-middle attack

25.04.2014

Researchers from the University of New Haven were able to intercept mobile data send through Viber — including images, videos, doodles and locations — with relative ease, using a PC that was setup as a wireless access point for the phone. Attackers could do the same by setting up malicious wireless access points, or with other so-called man-in-the-middle network intercepts.

The study also showed that Viber stored user data publicly on its servers for at least a week. "The data is stored on Viber's server in an unencrypted manner," one of the researchers said in the clip. "There is also no authentication method used, so anybody who has access to these links can look at this data, retrieve this data, and do whatever they want with it."

Demonstration of exploitation of vulnerability is posted at YouTube: www.youtube.com/watch?v=kqgn-HF4gKg

"The key here is to let the people know about these things so they can make an informed decision about using these applications until they are patched," Ibrahim Baggili.

Read more at: http://www.news.com.au/technology/viber-sends-video-images-without-encryption-researchers-warn/story-e6frfrnr-1226895488744

New Zero Day Internet Explorer Bug

Microsoft Internet Explorer users may be vulnerable to targeted attacks, after Microsoft published a security advisory about a new zero-day bug. Users of all versions of IE are vulnerable. Microsoft will be issuing a patch for supported operating systems, but Windows XP users will need to find another way to stay secure, as the operating system is no longer supported by Microsoft. It is recommended to switch to an alternate browser, while Microsoft will release a security update.

Read more at: http://community.norton.com/t5/Norton-Protection-Blog/New-Zero-Day-Internet-Explorer-Bug/ba-p/1127768

DDoS statistics for first quarter of the 2014

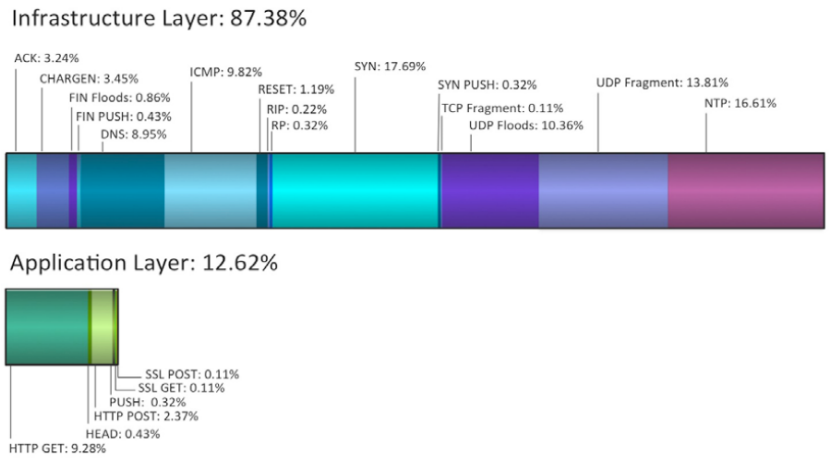
16.04.2014

According to the latest global DDoS report prepared by Proxlexic Technologies in Q1 2014 continued the trend of increasing botnet construction and decreasing traditional malware infection. This is a result of the widespread availability of reflection-based DDoS toolkits for malicious actors to build and deploy botnets for DDoS attacks.

Comparing the first quarter of the year with the same period in 2013, the report showed:

- 9% decrease in average attack bandwidth;
- 21% decrease in application (layer 7) attacks;
- 47% increase in total DDoS attacks;
- 50% decrease in average attack duration: 35 vs 17 hours;
- 68% increase in infrastructure (layer 3 & 4) attacks;
- 133% increase in average peak bandwidth: 4.17 Gbps vs 9.7 Gbps;
- 690% increase in peak packets per second: 2.87 Mpps vs 19.8 Mpps.

As presented at picture 1, infrastructure-based attacks, also known as volumetric attacks which seek to consume as much bandwidth as possible, constitute 87.38% of all DDoS attacks. The most commonly abused protocols are CHARGEN, NTP, DNS.



***Picture 1** – DDoS attack vectors and their relative distribution in Q1 2014*

Application-based attacks, which seek to cause specific application to fail or to become unresponsive to legitimate users, constitute 12,62 % of all DDoS attacks. The most frequent types are HTTP GET floods and, recently discovered, reflected application DDOS attack, which uses vulnerability CVE-2007-0540 in WordPress websites.

Conform the same report the most targeted industries are:

- 49,80% Media & Entertainment
- 16,53% Software & Technology
- 11,55% Security
- 8,97% Financial Services
- 6,57% Gaming
- 2,99% Internet & Telecom
- 2,19% Education
- 1,40% Public Sector

Read more at: http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q1.html

Photo by SC3 Security Training

More than half of enterprise employees receive no security training

10.04.2014

According to the research, performed by Enterprise Management Associates, 56% of 600 surveyed employees do not get security or policy awareness trainings.

As a result, conform the same research:

- 59% of the survey's participants said they store work information in the Cloud;
- 58% have sensitive information on their mobile devices
- 35% said they have clicked on an email link from an unknown sender;
- 33% said they use the same password for both work and personal devices;
- 30% also admitted to leaving mobile devices unattended in their vehicles.

"While today's organizations continue to harden their infrastructure to protect against the latest cyber threats, this report reveals that they too often fail to arm their employees with the critical information needed to avoid a data breach, prevent phishing, or report a possible security incident," said Craig Kunitani, COO with Security Mentor.

Read more at:

http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds

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**.

How to enable the “Kill Switch” on your iPhone or iPad, right now!

21.04.2014

A Kill switch is a feature designed to deter the growing problem of mobile phone thieves. Many smartphones already include the ability to let users remotely wipe their lost devices, ensuring that sensitive data doesn’t fall into the wrong hands. But that doesn’t stop a determined criminal from doing a “factory reset,” and selling the device on as though it were newly purchased from the local store.

From iOS 7, Apple’s “Find my iPhone” feature has incorporated a new technology called “Activation Lock,” which is effectively Apple’s version of the Kill Switch.

This is how it works:

1) User turns on "Find my iPhone" feature.
2) When the phone is lost or stolen user should immediately put it into "Lost Mode" by means of icloud.com/find website. Which alows also to wipe personal data, view place on the map and date when the lost phone was detected last time, and, to display custom message like "This iPhone has been lost. Please call me (373) 444-2323".
3) Once Lost Mode has been enabled, your device’s screen will be locked and demand that whoever finds it enter your Apple ID and password before they can do anything with it.

To enable the Kill Switch, you have to:

1) Go to Settings on your iPhone, iPod Touch or iPad.
2) Tap iCloud.
3) Sign in with your Apple ID, if necessary.
4) Turn on Find My iPhone.

Some important things to consider

- Activation Lock is only going to help if you have enabled it.
- Make sure that your Apple ID password is not easy to guess, and that you are not using the same password anywhere else on the Internet.
- Also, you should have a passcode protecting access to your phone. You can configure the passcode for your iPhone, iPad, or iPod touch using Settings > Passcode Lock.
- Never forget to wipe all of the content and settings off your iPhone or iPad before you sell it or pass it onto someone else as a gift. You can do that by going to Settings > General > Reset.

Read more at http://www.intego.com/mac-security-blog/how-to-enable-the-kill-switch-on-your-iphone-or-ipad/