S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

August 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 August 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

Fundamental security flaw was detected in the Universal Serial Bus (USB)

The Berlin-based researchers Karsten Nohl and Jakob Lell from Security Research Labs reverse-engineered the firmware that controls USB functions, including controller chips that connect a USB to a PC and discovered that this firmware can be reprogrammed with malicious code, which is practically impossible to detect. This security weakness has been dubbed "BadUSB".

Universal Serial Bus is an industry standard developed in the mid-1990s. The main advantage of USB - the ability to connect devices without the need of rebooting the computer - made it the most used standard for portable equipment and peripherals of the most various kinds. That circumstance significally increased impact of detected vulnerability, since infected can be any device, which connects to a PC using USB, including keyboards, computer mice, as well as the USB drives used to charge phones and tablets.

A malware, which uses BadUSB, is able to emulate a keyboard and transmit signals in the way the operating system will consider them as activity of the user, such as commands for opening files or installing software. The infected device can also spoof a network card and change the computer's settings to redirect web traffic to certain sites.

"We demonstrate a full system compromise from USB and a self-replicating USB virus not detectable with current defenses.", Mr Nohl and Mr Lell added.

The researchers say that the best practice for the moment in preventing of infection, which uses BadUSB is caution of user, who should ensure that the device, which is going to be connected to a PC, is 100% trustworthy.

Read more at: http://www.dailymail.co.uk/sciencetech/article-2711802/Is-USB-drive-risk-Invisible-fundamental-flaw-lets-hackers-computers-discovered.html

Contents:

Amateur security enthusiasts from the United Kingdom participated in the cyber-security challenge "Assignment Flag Drive”

Assignment Flag Drive is one of a series of UK national online competitions and learning programs, organized by Cyber Security Challenge UK, and sponsored by Oxford-based security firm Sophos with the aim of identifying and inspiring of EU citizens resident in the UK to become cyber security professionals.

According to the scenario, the fictional terrorist group warned of a future attack on the UK by placing a video on Facebook. The police traced location of suspected terrorist group, but at the time they arrived the terrorists had left, leaving only encrypted hard drive. During the competition entrants had to use computer skills and logic to break into the suspicious hardware and discover to whom the drive belongs to.

Although the challenge lasted 15, 16 of August the results has not been released yet.

Read more at:
http://www.dailymail.co.uk/sciencetech/article-2715381/Could-YOU-crack-terrorist-s-hard-drive-Cyber-security-challenge-

"When it’s time to perform the time to prepare has passed." - Steven Roberts

The list of global cyber attack maps

Sandro Süffert an entrepreneur and founder of APURA Cyber Intelligence created at his blog a list of global cyber attack maps available in the Internet.

The list, inter alia, includes the following sources:

1. Cyber Warfare Real Time Map by Kaspersky http://cyberwar.kaspersky.com/
2. Top Daily DDoS Attacks Worldwide by Google http://www.digitalattackmap.com/
3. Cyberfeed Live Botnet Map by AnubisNetworks http://globe.cyberfeed.net/
4. IpViking Live Map by Norse http://map.ipviking.com/
5. Honeypots from the Honeynet Project http://map.honeynet.org/
6. Global Activity Maps by Arbor http://atlas.arbor.net/worldmap/index
7. DDoS Attacks by ShadowServer http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSMap
8. Internet Malicious Activity Maps by TeamCymru http://www.team-cymru.org/Monitoring/Malevolence/maps.html
9. Globe and WorldMap by F-Secure http://worldmap3.f-secure.com/

Read more at:
http://sseguranca.blogspot.com.br/2014/03/ten-sources-of-global-cyber-attack-maps.html

A closer look at Adware

Many of computer users are accustomed to use freeware for performing their day-to-day activities. Meanwhile more and more freeware developers begin to include in freeware installation packages additional software that was called "Adware". That can be toolbars and plugins, icons, wallpapers, advanced search engines, and other lifestyle widgets. Although by this means the developers earn some money for their products, as they are paid for each installation of that adware, the users became exposed to a security risk as that adware could potentially carry malicious programs to target their browsing behavior and spy on other online activities.

The adware can harm your computer in the following ways:

- Because adware covertly piggybacks on the freeware you download, you don’t know that your system is running adware when you begin to install these free programs.
- Adware can have various routines such as bombarding you with pop-up ads, leading you to harmful or fake websites, offering bogus adware removal or antivirus software or gaining full access to your computer.
- It can spy on your browsing behavior and gather private information about you to be sold to third parties or other cybercriminals.
- Adware could hijack clicks without your knowledge or without having to run the freeware you downloaded, prompting your computer to become unbearably slow and unstable.
- Additionally, adware also mines bitcoins which results in unexpected high electric consumption.

To protect yourself against adware use the following guidance:

- Think twice before immediately downloading and installing any software, particularly freeware.
- Read everything rigorously before digitally signing up or agreeing to terms and conditions to prevent the download of adware.
- Make sure to routinely check up your computer and regularly scan your systems.
- Take basic preventive measures like using a security solution software that will enable constantly updated protection.

Read more at:

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-exposed-part-2-when-adware-goes-bad-a-closer-look-at-adware/

Cyber espionage campaign revealed

Researchers from Russian computer security firm Kasperksy Labs claim to have discovered a massive cyber espionage campaign called "Epic Turla" that targeted government institutions in 45 countries.

The hackers were said to have collected spreadsheets, documents and emails that contained terms such as "NATO", "Budapest" and "EU energy dialogue." The revealed campaign targeted countries, which are predominantly from Europe and Middle East. The biggest number of victims was detected in France - 25 victims. In total were identified approximately 500 infected IP addresses.

The victims were infected by means of different methods, among them:

- Distribution of spear-phishing emails with malicious PDF file. Spear-phishing email is a malicious electronic message that is aimed to infect specific target;
- Social engineering to trick the user into running malware installers with ".SCR" extension, sometimes packed with RAR;
- Use of watering-hole attack. A watering-hole attack is a method of infection in which an attacker determines web sites which are often accessed by a victim, then he breaks into some of identified web-sites and installs malicious software, which infects computers of those users, whose profile present an interest for the attacker. In total were identified more than a hundred web-sites with malicious scripts installed on them, whose code contained exploits, which targeted different vulnerabilities in Java, Adobe Flash Player and Internet Explorer 6,7,8.
- In some cases attackers tried to trick users of hacked web sites by luring them to install an "update" for Adobe Flash Player.

After the malware installs on a computer of a victim it established a connection to Control & Command (C&C) server of an attacker for receiving instructions what it should do next. Among identified instructions were:

- Brute force accounts of computers installed in the same to the infected computer local area network;
- Create a file list with extension ".doc";
- Search in file names phrases: "*NATO*.msg", "eu energy dialogue*.*", "EU*.msg", "Budapest*.msg".

After instructions are received, the malware installs additional modules, such as key logger, windows administration utility and other. In some cases were noticed that the malware installs special module called "Carbon system", which represents a very comprehensive software used for hiding the presence of malware in the infected system as well as its communications with Control & Command server.

To prevent an infection use the following best practices:

- While using email client do not click on images or links in suspicious emails. An email can contain an image or link clicking on which will lead the user to a malicious web site.
- Configure your email client to show emails in a form of simple text, but not as html page. This measure prevents an attacker to trick you by substitution of the real link address of a web page displayed in your email client by a fake one.
- Ensure your partner's emails are digitally signed in ordered to prevent spoofing;
- Remember that not only executable files in an email attachment are able to contain a malware, but also PDF, Word or any other file.
- While using web-browser remember, that popup messages which are asking you to update "Adobe Flash Player", "Java" or whatever could be a fake. Always close such windows and install updates only from official web site of the developer.
- Never save passwords from your accounts in a web-browser. In case of infection, these are easily extracted by the malware.

Read more at:
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

Guide to Application Whitelisting

National Institute of Standards and Technology has published a draft of Special Publication 800-167 "Guide to Application Whitelisting".

The purpose of that publication is to assist organizations in understanding the basics of application whitelisting and planning for its implementation.

An application whitelist is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a system according to a well - defined baseline.

Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software. Unlike security technologies such as antivirus software, which block known bad activity and permit all other, application whitelisting technologies are designed to permit known good activity and block all other.

According to the Special Publication 800-167 the organization should use the following steps in order to plan and implement the application whitelisting technology:

1. ***Initiate the Solution***. The first phase involves identifying current and future needs like performance, functionality and security requirements.
2. ***Design the Solution***. This activity imply creation of whitelist management, cryptography policy, and security aspects of the solution itself.
3. ***Implement and Test a Prototype***. The next phase involves implementing and testing a prototype of the designed solution in a lab or test environment.
4. ***Deploy the Solution***. Once the testing is completed, deploy the solution in the production environment.
5. ***Manage the Solution***. Management process should include maintenance and support for operational issues.

Read more at:
http://csrc.nist.gov/publications/drafts/800-167/sp800_167_draft.pdf

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**

Like us on facebook

CSC
Centrul pentru Securitatea Cibernetică

Recommendations for performing a security assessment in an organization

Lenny Zeltser, an expert in information technology and security, gave recommendations regarding the steps that should be taken in order to perform security assessment of an organization.

According to provided recommendations, for performing of security assessment, security managers should use the following guidance:

1. ***Identify Key Data Flows*** to better understand the business processes of the organization:
   - Meet key people and hear their concerns. These folks can support your security improvement efforts later;
   - Try to understand where data comes from, where it goes and which infrastructure components process it;
   - Ask about any compliance or contractual requirements that may drive the company's need to protect data.
2. ***Understand User Interactions*** to determine how, with whom and which data people share internally, as well as with partners and customers:
   - Pay attention to the access individuals require to get work done: who only reads data, and who requires the ability to change it. This will affect the permissions that should be enforced to control access;
   - Assess what change controls are in place for prevention unauthorized modifications to the infrastructure and its data;
   - Remember that weak sharing practices have resulted in many information security breaches.
3. ***Examine the Network Perimeter*** to explore network egress and ingress paths:
   - Try to determine which weak places exists in the network perimeter;
   - Check what mechanisms exist to detect and block unauthorized access;
   - Analyze the situation when one of the perimeters components, say the border firewall, failed to block the attack in order to determine the possibility that your production environment would be wide open;
   - Examine your Internet connection, as well as any direct links to your partners and customers. Include both wired and wireless networks.
4. ***Assess the Servers and Workstations*** to detect missing patches or configuration errors:
   - Start with the servers accessible to external parties. Then, move onto your internal servers;
   - Don't forget to assess the state of your desktops and laptops, as attacks on client-side software, such as browsers and their add-ons, have been very successful.
5. ***Look at the Applications*** to determine the weaknesses which could allow an attacker to compromise the application's security mechanisms to access data without authorization:
   - Consider the vulnerabilities that may exist in custom applications accessible to third parties and internal users;
   - Pay particular attention to Web-based applications, which have been an attractive target in the recent years.

Read more at: http://zeltser.com/security-assessments/assessments-for-mid-sized-firms.html

Disclaimer:

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-GOV-MD assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.