S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

March, 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 March 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.

Windows XP Security: Hype or a Real Threat?

3.04.2014

After 12 years of service and the releases of the less popular Windows Vista and Windows 8, Windows XP is still the preferred OS of many users and runs on 30% of all PCs connected to the Internet, about 400 million computers. On April 8th, Microsoft will stop supporting these devices with new security upgrades. Is the last minute hype around XP security risks warranted?

Fact #1. Microsoft will continue updating its XP malware engine for another year, until July 14, 2015. While no antivirus program can completely replicate or replace manufacturer security updates, it will still remain difficult for malware to take advantage of your system's vulnerabilities.

Fact #2. Only a handful of compromises discovered over the past few years. These attacks were primarily Denial of Service (DOS) attacks. DDOS attacks do not steal data, but only interrupt service.

Fact #3. Upgrading to the latest version of XP will reduce security risks. Many security attacks succeed by studying security vulnerabilities patched in prior updates. Now that new research into vulnerabilities is not being carried out, attackers will lose this advantage over users running the most updated version. Organizations that install the most recent Windows XP service pack can mitigate security risk for this reason.

Fact #4. Attacks are never one-dimensional. A single operating system vulnerability may not be enough to cause a security incident. Research has shown that most attacks require multiple touch points to be carried out successfully.

Verdict: You're going to be okay. For now. Unless a massive vulnerability is discovered, Windows XP should still have at least one more year in it.

http://www.doctrackr.com/blog/bid/381580/Windows-XP-Security-Hype-or-a-Real-Threat

Contents

Hackers from across Europe flocked to Geneva to test their ethical hacking skills.

22.03.2014

The sixth annual Insomni'hack ethical hacking competition, organized by IT security firm SCRT, drew over 300 hackers from Ukraine, Spain, Germany, France and other countries, who battled for hours to solve a range of fiendish computer security challenges.

Three of the best hacking teams in the world were present, including the winners of another famed competition, "Dragon Sector", who are mostly from Poland. Attendees faced about 30 tests in almost all security areas.

The Geneva competition is held for fun, but many of the competitors make a living from their hobby.

http://www.securityweek.com/european-hackers-test-their-skills-geneva

Did you know?

According to research from Incapsula, almost one in every three network-based DDoS attacks is above 20Gbps.

Read more at: http://www.infosecurity-magazine.com/view/37714/ddos-attack-volume-skyrockets-in-q1-/

"Just as nuclear was the strategic warfare of the industrial era, cyber warfare has become the strategic war of the information era." U.S. Secretary of Defense, Leon Panetta

Tor network – a safe haven for illegal services

5.03.2014

Conform research performed by Kaspersky Lab expert, Tor network more and more used by cybercriminals to hide their illegal activities.

The researcher found approximately 900 hidden services online. Some of them used to deploy C&C servers of botnets - the most recent found examples: Zeus with Tor capabilities, ChewBacca and the first Tor Trojan for Android. Hosting C&C servers in Tor makes them harder to identify, blacklist or eliminate.

Another example of broadly used hidden services are Tor underground marketplaces. It all started from the notorious Silk Road market and evolved to dozens of specialist markets: drugs, arms and, of course, malware. Some of them are public, some are private and you need the approval or an invitation from an existing member or need to be a respected personality in underground scene.

http://www.securelist.com/en/blog/8187/Tor_hidden_services_a_safe_haven_for_cybercriminals

Relying on password security? The truth about what employees are (not) doing

26.03.2014

Many organizations today rely on passwords as the foundational layer of security for access to sensitive business data. With the rapid growth of smartphones and tablets, expanding use of cloud services, and nearly ubiquitous mobile workforce, passwords make for a shaky foundation. Highly sophisticated attackers target these categories of users to take advantage of vulnerable passwords and holes in security, which could result in a costly breach for your company.

According to the Symantec's research, 49% of people participate in bring-your-own-device (BYOD) programs, using their personal devices for work-related activities. Almost half of them do not protect it with a password or other basic security measures. About 30% of parents let kids play, download, and shop on their mobile work device. These facts together with broad range of functions, embedded in modern smartphones, and variety of malware spread, even through trusted web store, transforms them into an excellent platform for advanced persistent threats and cyber espionage.

Why is security so lax? – Complexity – companies make security measures too difficult for employees to comply with; – Password fatigue – the average user has 26 password-protected accounts, but only five different passwords; – Resistance – 38% of people surveyed would rather clean a toilet than come up with a new password.

To protect against specified threads enterprises require the following:

- Two-factor authentication solution that is easy for employees to use and mobile-friendly;
- Unified solution that can provide employees with secure access to applications and networks.

http://www.symantec.com/connect/blogs/relying-password-security-truth-about-what-employees-are-not-doing

Authorities arrest infamous hacker "Diabl0" in Bangkok

Farid Essebar, a hacker from Morroco, also known as Diabl0, was arrested in Bangkok last Tuesday due to charges levied against him in Switzerland for hacking bank computer systems and resulting in $4 billion worth of damage to victims in Europe.

Read more at: http://www.scmagazine.com/authorities-arrest-infamous-hacker-diabl0-in-bangkok/article/338982/

Kaspersky Lab launches worldwide interactive cyber threat map

27.03.2014

Kaspersky Lab has launched an interactive cyber threat map that visualizes cyber security incidents occurring worldwide in real time.

The types of threats displayed include malicious objects detected during on-access and on-demand scans, email and web antivirus detections, as well as objects identified by vulnerability and intrusion detection sub-systems.

Information about cyber-attacks is collected using cloud-based infrastructure "Kaspersky Security Network" (KSN). Internal KSN mechanisms summarize the data sent automatically from thousands of protected devices whose users consented to share information about any suspicious programs they encounter. After comparing the behavior of the file on different computers, checking it against a database of hundreds of thousands of legitimate applications and using heuristic algorithms, the system issues a preliminary verdict on whether or not the object is malicious. If it is malicious, access to the object is promptly blocked for all other Kaspersky Lab users, thus preventing an epidemic.

KSN possesses the very latest information about security incidents, which is added to a map of the world in real time so that anyone can view the wide variety of threats, and the speed at which they spread.

The interactive map of the cyber world is available at http://cybermap.kaspersky.com. To be displayed correctly, the browser must support WebGL.

http://www.kaspersky.com/about/news/virus/2014/Real-Threats-in-Real-Time-Kaspersky-Lab-Launches-Worldwide-Interactive-Cyberthreat-Map

Hackers could take control of Philips ‘smart TVs’ and broadcast their own ‘shows’ to watching families.

28.03.2014

The recent firmware released by Philips for their 2013 models of SmartTV (6/7/8/9xxx) have the WiFi Miracast feature enabled by default with a fixed password and no PIN or request of permission for new WiFi connections.

A hacker within Wi-Fi range of any 2013 Philips Smart TV can replace the image on screen with video or images of his choosing steal browser cookies and read files on USB devices attached to the set.

While company develops a fix for this issue, Philips Smart TV users advised to disable Miracast function using the following procedure: Press the HOME button – navigate to Set up – select Network Settings – Select Miracast – set to OFF.

http://www.welivesecurity.com/2014/03/28/channel-cybercrime-bug-allows-hackers-to-hijack-screen-of-philips-tvs/

Five Security Myths Unmasked

26.03.2014

Myth #1. Passwords must be overly complex and impossible to remember. While this advice is still good in theory you should consider that the length of your passwords is just as important and makes them unbreakable, not just the complexity - ensure your passwords are at least 15 characters in length and the same password is never used on any two websites or systems;

Myth #2. Only email attachments that are executable files are dangerous to open. Wrong! ALL types of e-mail attachments can be dangerous. Recent and very dangerous examples have been Adobe PDF documents and Microsoft Word documents. If you are not expecting an attachment from someone, delete the e-mail to be sure.

Myth #3. Popup messages asking you to update could be fake. A number of years ago there were quite a few examples of “fake” software upgrade popups tricking people into installing malware. This epidemic appears to have left many users jaded with the perceived risk and the inconvenience of installing updates at seemingly random times – but updating is one of the most important tasks you should be doing.

Myth #4. You should never write a password down. As long as you secure any written passwords and keep them somewhere safe, like in a locked drawer, the risks of them being compromised are quite limited.

Myth #5. Your Internet banking credentials are the most important thing to keep safe. Fraudsters are able to exploit poorly protected e-mail accounts in a number of ways, and this can directly affect your family and friends who may be targeted with scams.

http://blogs.avg.com/lifestyle/security-myths-unmasked/

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**.

Watch out for photos containing malware

27.03.2014

Cybercriminals use images in a number of ways to infect your computer. In most cases, the photo itself is harmless; it's just a trick to get you to do something stupid. However, a ".jpg" file itself can contain malicious code.

An image can harm in a few ways:

1) An email can contain an image clicking on which will lead the user to malicious web site.

2) Another trick is the double extension. If a file is named “image.jpg.exe”, most Windows computers will display it as “image.jpg”. Most users, therefore, will think it a harmless image file, even though it's really an executable program. Moreover, when you run the program, it probably will show you a picture...while it infects your PC.

3) And finally, a ".jpg" can easily contain additional bits interwoven within the image, without noticeably effecting the image's appearance. That additional data can include code, which is encrypted to make it harder to identify. Luckily, such an altered image cannot do much by itself, however the information hidden in a picture could contain instructions useful to another piece of malware on your computer, for example "Zeus".

To protect yourself from "bad" images the following can be useful:

1) Don't click on images in suspicious emails

2) Keep your operating system, browser, and antivirus software up-to-date.

3) And finally, have Windows show you file extensions so you will not be fooled.

http://www.pcworld.com/article/2105408/3/watch-out-for-photos-containing-malware.html

WinRAR vulnerability exposed

Danor Cohen, an Israeli security researcher, discovered a vulnerability that allows an individual to create a ZIP file that appears to contain one thing when compressed, but actually houses something different altogether.

All versions of WinRAR, including version 5.1 are affected.

Read more at: http://www.scmagazine.com/winrar-spoofing-vulnerability-being-exploited-in-malware-campaign/article/340135/

Disclaimer: