S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

May, 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 May 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.

Five questions to ask your outsourcer

20.05.2014

Many companies today rely on outsourcing trusting sensitive client data to be processed and stored at outsourcing provider's premises. Big amount of recent data breaches have shown, that companies should ensure, that outsourcing provider had implemented necessary security controls, has and is following all required information security policies and procedures.

These are the questions you should be asking your supplier in order to determine that:

1. ***Who are your customers, am I the first?*** This helps identify potential risk if you're hosted next to an interesting government department. Make sure that you're not at risk of an attack bouncing back on you when you're not the target.
2. ***What's the software that's in use?*** You only have to look at the recent Heartbleed issues to realize your provider needs to be using appropriate proprietary software, so make sure you ask them if they're up-to-date with their patching, and ask them about their evaluation regime.
3. ***Where do you keep the data and how do you protect it?*** It's important to know where it is, how it's supported, and where the first, second, third and fourth line of support comes from.
4. ***What sort of response time can I expect?*** You need to be aware of incident response time. If your portal is under attack, or the website is suffering a DDoS attack, how quickly will it be noticed? And how quickly will the defenses swing into action?
5. ***How do you handle protective monitoring?*** And what are you doing with the logs once you've got them? Data from logging is great, but it must be filtered for relevance so you and your supplier can focus on the threats that matter most.

Read more at: http://letstalk.globalservices.bt.com/en/security/2014/05/five-questions-ask-outsourcer/

Contents

Metadata possess a security risk

Recent events in the information security area demonstrated, that metadata is widely used for user tracking, collecting information and even targeted social engineering attacks, and presents a security risk for the users who do not protect themselves from such threads.

Metadata is an additional information embedded into browser cookies, Microsoft Office documents, images, PDF and other files, which describes different information, like who is author, when and where the document or a file was created.

In order to minimize this security risk use the following recommendations:

1) Use "Private Browsing" feature and No Script plugins in your browser to ensure that it won't keep any browser history, temporary internet files or execute unexpected scripts. While this measures doesn't prevent to track computer by an IP address it will be not possible to distinguish which user is currently using the web browser.

2) Use special software to erase all metadata before uploading images or other files to the Internet. The examples of such software are: Metadata Anonymisation Toolkit, Exiftool, RHDTool.

"I still believe cybersecurity — and by extension, privacy — is a state of mind and very much dependent on the context of any given situation to be effective." - Richard F. Forno, Ph.D, Chief Security Officer for at Network Solutions

Protect your privacy while surfing the Internet

19.05.2014

Many information companies collect private information of their subscribers.

Each time a user surfs the Internet his browser executes a part of code embedded into the visited web page, which transmits statistics information to a third party company who is partner to a web resource owner. It allows to form a decent idea of user's habits and interests. All collected data is aggregated to a huge subscriber database, which is later used for targeted advertising campaigns. If this bothers you, then it's time to take measures in order to protect your privacy.

The best way to achieve this goal is to install a “tracker blocker” – a web browser plugin, which prevents execution of third party scripts loaded from third party domains.

Conform data, provided by CBR, the best plugin designed for this purpose is HTTP Switchboard. It allows to control where a browser is allowed to connect, what type of data it is allowed to download, and what it is allowed to execute.

Read more at: http://www.cbronline.com/news/security/should-you-download-adblock-plus-ghostery-or-disconnect-4271294

Cyber threat trends for 1Q of 2014

13.05.2014

According to the latest report, provided by TrendMicro Inc., cyber threats continued evolving in the direction more targeted attacks.

The review of the trends is presented below:

- ***New attack targets***. Today’s cybercriminals are aiming at previously nontargeted entities to carry out malicious deeds. Proof of these include the US$480-million digital heist Bitcoin exchange, MtGox, suffered from and recent attacks against large retailers via point-of-sale (PoS) terminals.
- ***From mining to stealing***. In the past, attackers compromised systems and used them to mine for the valuable digital currency; today, Bitcoin exchanges and wallets are targeted for theft. This March, for instance, BitCrypt an addition to the ransomware scene, stole various cryptocurrency wallets, including Bitcoin wallets.
- ***Ransomware Continued to Go Regional***. In February, a CryptoLocker-like ransomware variant victimized users in Hungary and Turkey. Last time it was targeted users in Italy, Spain, France, and the United Kingdom.
- ***New Zero-Day Exploits***. Various zero-day exploits were found this quarter for a mix of browser, browser plug-in, Microsoft Office 2010, Internet Explorer, Adobe Flash and other software vulnerabilities.
- ***Threats Migrated from Computers to Mobile Devices***. Mobile malware has grown from 1.5 M in JAN 2014 ot 2.1 in MAR 2014. Top Android Malware families: "OPFAKE" - 9%, "SMSREG" - 9%, "GINMASTER" - 8%. Threat Type Distribution: Adware - 47%, Premium service abuser - 35%, Data/Information Stealer - 19%, Malicious downloader - 9%, Unauthorized spender - 2%.
- ***New PoS Malware***. Cybercriminals infected PoS terminals (device which reads credit card information in the super markets) in South Korea with malware to steal sensitive information.
- ***New Social Engineering Techniques.*** Cybercriminals took advantage of the hype to lure users to watch fake videos, regarding missing flight MH370, on Facebook forcing them to share the videos and spreading by this way links to phishing web sites.

Read more at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cybercrime-hits-the-unexpected.pdf

Review of malware underground market in Russia

28.04.2014

Trend Micro Inc., a Japanese security software company, has published a report, which describes current situation, prices and trends of Russian's malware underground market.

The report reviled that Russian underground today are now highly specialized. A cybercriminal with ties to the right people no longer needs to create all his attack tools himself; instead he can buy these from sellers that specialize in specific products and services.

Sellers and buyers meet in underground forums. To ensure both of their safety, sellers and buyers use escrows — third parties who get and keep the buyers' money until the purchase is finalized. This protects the sellers because escrows make sure the buyers have the money to pay for the products or services sold. Escrows also test the products or services sold by the sellers to make sure the buyers get what they paid for and will not become victims of false advertising. Escrows usually get 2–15% of the sales price for their services. Forum members use all kinds of tricks (e.g., use VPNs, SOCKS proxies, or the TOR network) to hide their GeoIPs but they still need to be identified by unique nicknames and ICQ numbers, as that is how they can be distinguished from others. This allows them to stay anonymous but somewhat recognizable.

Conform the same report Russian malware industry mostly specializes in selling Traffic Distribution Systems (TDS), which is designed to forward users to a specific malware-contained web-site based on: version of user's operation system, type of web-browser or local language; and Offering Traffic direction and Pay Per Installation (PPI) services, which allows a malware author, who doesn't have its own malicious web-sites, to distribute its malware among affiliates which receives money from him based on the number of computers they infected.

Here is some malware price statistics (comparing to prices of 2012):

- Trojans (ex. ZeuS, SpyEye, etc) - price droped from 120$ - 790$ to 0$ - 35$;
- Crypters (Basic static, Poymorphic, etc) - price droped from 10$ - 100$ to 10$ - 65$;
- Proxy server host lists (per 300 IP addresses) - price grown from 3$ to 6$;
- Scanned fake documents (per 1 document) - price droped from 2$ - 5$ to 1$ - to 2$;
- Stolen credit card credentials (per card) - price droped from 2.5$ - 7$ to 1$ - 5$;
- Server hosting - price droped from 70$ - 450$ to 12$ - 190$;
- DDoS attack (1 hour) - price grown from 4$ - 10$ to 2$ - 60$;
- Spamming (per 10 000 messages) - price droped from 13$ to 4$ - 5$;
- Pay per Installation service (per 1000 installations) - price droped from 190$ - 400$ to 50$ - 200$;
- SMS flood (per 1000 messages) - price droped from 15$ to 8$;
- Landline phone flood - price droped from 35$ to 25$;
- Hacking (Facebook , Twiter, Gmail and other accounts) - price droped from 74$ - 200$ to 50$ - 100$;

Read more at http://blog.trendmicro.com/trendlabs-security-intelligence/the-russian-underground-revisited/

Security best practices

16.05.2014

For Business:

- **Know your data**. Protection must focus on the information – not the device or data center. Understand where your sensitive data resides and where it is flowing to help identify the best policies and procedures to protect it.
- **Educate employees.** Provide guidance on information protection, including company policies and procedures for protecting sensitive data on personal and corporate devices.
- **Implement a strong security posture**. Strengthen your security infrastructure with data loss prevention, network security, endpoint security, encryption, strong authentication and defensive measures, including reputation-based technologies.

For Consumers:

- **Be security savvy**. Passwords are the keys to your kingdom. Use password management software to create strong, unique passwords for each site you visit.
- **Be vigilant**. Review bank and credit card statements for irregularities be cautious when handling unsolicited or unexpected emails and be wary of online offers that seem too good to be true.
- **Know who you work with.** Familiarize yourself with policies from retailers and online services that may request your banking or personal information. As a best practice, visit the company's official website directly (as opposed to clicking on an emailed link) if you must share sensitive information.

Read more at:

http://techday.com/the-channel/news/symantec-new-era-of-mega-breaches-signals-bigger-payouts-for-cyber-criminals/184538/

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**.

Real life scenario of free Wi-Fi network attack

07.05.2014

Many hackers these days start by hanging out at the coffee shops or other free-WiFi hot spots near the offices of companies they want to infiltrate. Using easy to carry hardware, hackers can impersonate a free WiFi network and invite a user to join. It looks and feels like free Internet, and few people ask many questions if their browser works.

What next? A relatively easy next move, the cyber security version of the "the man in the middle" scam: create a mock login page for a site that's likely visited by the hacker's target–the Facebook login page, for instance. Or, a company's Intranet login page. Many of these are easily downloadable from IT specialty sites that build them to test their vulnerability. The unsuspecting user logs in as usual, giving away username and password details. Since many people use the same details across platforms and sites, it's often easy pickings for hackers from there.

Once the hacker has a password for one account, even a personal one carefully segregated from an employee's work account, the hacker can start trying to gain access into their victim's other accounts, any of which may have corporate data worth mining: Gmail, Yahoo, Hotmail, or go right for their corporate intranet and email.

The hacker now has access. Let the real trouble begin. What would you do if you received this email: "Hi, it's Peter from IT. We've got a security update we need you to run, can you run it for me please? Just double click the attachment. Thanks." According to Sophos' Deacon, many employees do as they're told when they see an email which looks like it came from their company's IT department. What's been unleashed? One threat is a Trojan Horse malware program. It sits unseen on a company's server and can be used to pilfer data like passwords and internal communications.

Be careful and control websites you visiting while using free public Wi-Fi.

Read more at: http://blogs.wsj.com/five-things/2014/05/07/5-ways-hackers-exploit-our-bad-byod-habits/

Philippine branch of Anonymous hacks Chinese govt sites

Close to 200 Chinese government websites have been defaced by a Philippine branch of the hacktivist collective Anonymous. The group took to its Facebook page at 18.05.2014 to share links to each of the sites hacked. Based on the context of the message used on the defaced sites, as well as recent events regarding territorial tensions between Beijing and Manila over the South China Sea, the hacktivists are not pleased with China's actions.

Read more at: http://www.scmagazine.com/philippine-branch-of-anonymous-hacks-chinese-govt-sites/article/347773/

Disclaimer: