S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

June, 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 June 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.

Why every enterprise should have a honeypot?

- Because they can bring great advantages to companies' information security, like:

1. ***High chance of intrusion detection*** – in comparison with antivirus software, production honeypots have higher chances of intrusion detection, because virus authors always test their malware against top antivirus products, which allows malware to stay undetected before signature is released. In counter side, production honeypots are machines that no legitimate user should be accessing, and any connection attempt should be considered malicious.
2. ***Able to confuse attackers*** - because attackers have a much more difficult time predicting their use and countering the defenses, which gives possibility to information security personnel to detect an intrusion before attacker will be able to reach valuable data.
3. ***Little maintenance time*** - unlike research honeypots, which assumes deployment of a vulnerable operating system on the Internet and studying attackers' behavior, production honeypots, emulate web server, workstation, database or anything which has value to the company and after installation the security team has to worry about it only when the honeypot triggers an alert.
4. ***Help train your security team*** - Research honeypots can be useful for studying new intrusion techniques.
5. ***Widely accessible*** - There are many freeware effective honeypots ready to deploy.

Read more at http://www.darkreading.com/vulnerabilities---threats/5-reasons-every-company-should-have-a-honeypot/d/d-id/1140595

Contents

FIFA 2014: World Cup's Wi-Fi password leak

Luiz Cravo Dorea, head of international cooperation at the Brazilian Federal Police

A photograph made for Correio Braziliense, an online version of Brazil newspaper, exposed the password and SSID used for Wi-Fi network of World Cup's security center.

On the photo is presented head of international cooperation at the Federal Police – Luiz Cravo Dorea standing in the security center. The password "b5a2112014" and SSID "WORLDCUP" were exposed behind him, in the lower corner of the screen.

Although the password used meets minimum password length criteria, it lacks complexity requirements. In particular it doesn't contain uppercase letters and non-alphanumeric characters and, according to the Microsoft password checker www.microsoft.com/en-gb/security/pc-security/password-checker.aspx, has 'Medium' password strength.

Another important aspect to consider from this incident – all the information leaving the organization should be properly sanitized.

For the moment there wasn't made any official statement regarding this issue.

Read more at:
http://www.infosecnews.org/want-to-know-the-wifi-password-for-the-brasil-world-cup-security-center/

"A lot of traditional defensive technologies don't have a lot of value against advanced attackers, because the bad guys have the means and the resources to ensure that their attack is going to work," - John Strand, senior security analyst/principal of BHIS.

How to recognize a phishing email?

Phishing attacks continuously evolving to be more attractive and trustworthy to their targets. Therefore it is very important to recognize a phishing attack before it can harm your organization.

The following points can help to distinguish a phishing email from a legitimate one:

1. ***Generic Greeting*** - Usually companies address to their customers by name. If an email begins with "Dear XYZ-company customer" – it is a bad sign;
2. ***Fake link address*** - what can be seen by eyes not always correspond to the actual link address. Always check the link, before click on it;
3. ***Request for personal information*** – it is not normal for companies to ask for personal information if the service is already provided. Contact your provider by phone to verify the email;
4. ***Urgency*** – it is a sign that something is wrong. Do not trust such email unless you verify it;
5. ***Poor spelling*** - a reliable indication of phishing

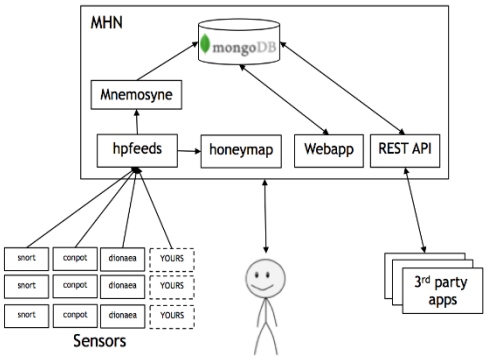
Read more at:
https://www.globalsign.eu/resources/white-paper-phishing-attacks.pdf

Automation of the setup and management process of enterprise honeypots

19.06.2014

The Modern Honey Network (MHN) – is a free software, created by ThreatStream, which automates the process of setting up and monitoring honeypots.

The architecture of MHN is presented at picture 1.



Picture 1 – The architecture of MHN

MHN main components:

- ***HPfeeds*** – protocol for delivery sensor data;
- ***Mnemosyne*** – indexes sensor data and adds it to MongoDB;
- ***Honeymap*** – visualizes sensor data in real time;
- ***Sensors*** – currently supported: Dionaea, Conpot, Snort.
- ***Rest API*** – allows integration with 3rd party software.

Adding a new honeypot is as simple as copy a link from MHN web interface and paste it into the console of the server to which a honeypot has to be installed.

The Honeymap enables to view all active threats in the real time. The Honeymap is presented at picture 2.

Picture 2 – Honeymap

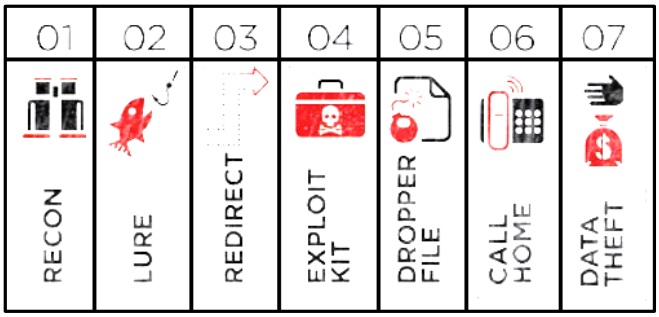
The latest version of Modern Honey Network can be obtained from https://github.com/threatstream/mhn/

Cyber-attacks analysis using "kill chain" model

Websense Security Labs in its 2014 Threat Report demonstrated how to apply the seven-stage “kill chain” model to analyze cyber-attacks.

The "kill chain" - is an attack model, which splits all activities, performed by cybercriminals in an attack, into different categories. Each category has specific characteristics, which allows clearly identifying purpose, providing general description, discovering possible ways of execution and recommending suitable countermeasures against a malicious action. This helps to evaluate the risk related to an attack and to review security posture applied in order to prevent such attacks in the future.

There are seven categories, or stages, in the "kill chain" attack model, which are presented in the picture 3.



Picture 3 – Stages of the “kill chain” attack model

Short description of the “kill chain” model’s stages is provided below:

1) ***Recon*** - at this stage attackers research their intended victims using personal, professional and social media websites and other public-facing content in order to create trustworthy "lures" that lead to compromised websites under their control or discover other ways to infiltrate into an organization.

2) ***Lure*** - Using information collected in the recon stage, on the black market or via other attacks, cybercriminals create socially engineered web pages and email lures that can cause users to act in ways that seem in their self-interest but in reality lead them astray. Lures are used to encourage users to enter their credentials or other personal information, which cybercriminals can then use in later attack stages or sell on the black market.

3) ***Redirect*** - In their lures, cybercriminals may use links that point users to safe-looking or hidden web pages that then “redirect” users to sites containing exploit kits, exploit code, obfuscated scripts or other malicious content. Cybercriminals use redirects not only to obscure their identity, but also to hide the attack apparatus from those who could create defenses.

4) ***Exploit kit*** - Once a user has clicked on a link to a compromised website, software known as an exploit kit scans the victim’s system to find known and zero-day vulnerabilities. Cybercriminals seek weaknesses that can become open doors for delivering malware, key loggers or other advanced tools that enable them to further infiltrate networks and steal data or compromise systems. They also seek to bypass static defenses by adapting their exploits and keeping ahead of the latest security updates.

5) ***Dropper file*** - The dropper file is the object that, once delivered and installed on a system or endpoint, enables the attacker to persist and advance an attack.

6) ***Call home*** - Once the dropper file infects the target system, it “calls home” to a C&C server to download additional programs, tools or instructions.

7) ***Data theft*** - the end-game of most modern cyber attacks, the theft or destruction of data completes the kill chain. Cybercriminals steal intellectual property, personally identifiable information or other valuable data for financial gain, for use in other attacks or sometimes to destroy.

Read more at: http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf

Cyber espionage attack against Vietnamese government failed

27.06.2014

According VietnamNet Bridge Vietnamese government’s Ministry of Natural Resources and Environment (MONRE) became a target of coordinated cyber espionage attack. The target of attackers was "East Sea database", which contains sensitive to national economic and strategic information about "cow's tongue" region - exclusive, according UN convention 1982, economic zone between China, Philippines, Vietnam, Taiwan, Malaysia, and Brunei.

Attackers used phishing emails, with infected Microsoft Word document, to penetrate into MONRE's network. As soon as document has been opened the malware, disabled Bach Khoa Anti-Virus - software used by MONRE to defend its computers. After that it started a Windows command shell “%system%\cmd.exe” with input/output redirected to the command-and-control (C&C) server located in the U.S.

Nguyen Huu Chinh, director of the Information Technology Agency insisted that the hackers could not have stolen information from the latest attack, because the infected personal computers were not authorized to connect to server, where sensitive information is stored.

The key points to remember from this story are:

- Educate your employees don't open emails from untrusted source;
- Ensure your partner's emails are digitally signed in ordered to prevent spoofing;
- Encourage employees to report to the IT staff any suspicious computer activity, connection requests, email, or behavior;
- If you have to open the attachment ensure your OS, antivirus is up to date and you contacted the sender using phone, text or in person to authenticate the email.

Read more at: http://english.vietnamnet.vn/fms/science-it/106128/monre-claims-malware-damage-minimal.html

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**.

New Android malware's abusing techniques

13.06.2014

Recent McAfee Labs Threat report revealed new methods used by Android malware to abuse platform vulnerabilities, applications and services.

Usually mobile malware abuses the official features provided with the platform in the way like: it can make calls without the user's permission, send premium SMS message or GPS data, intercept communications and so on. Newfound malware started abusing features provided by legitimate applications and services installed on a device.

Examples of such malware are:

- ***"sijaja7mnmn"*** - a suspicious android application, already removed from Google Play app store, that asked user, upon installation, to authorize usage of various Google services and after acceptance of the request it could automatically download, install, and launch other applications without user permission, which is usually required when manually installing apps from the Google Play;
- ***"Adobe Flash Player"*** - a malware disguised as an update for Adobe Flash Player or another legitimate utility app. It hides from the home screen after installation. In the background, the malware checks whether the device user has a Visa QIWI wallet account and whether there is a balance in the wallet, intercepts the confirmation response, and finally sends the money transfer to the attacker's server;
- ***"BalloonPop"*** - this malware disguises itself as a game app. It exploited weakness of an encryption method in the popular messaging app "WhatsApp" and stole user's conversations, pictures stored on the device and secretly sent them to the criminal's remote server to decrypt, and later to disclose them to public on the attacker's website.

As can be concluded from these examples - protecting only the underlying platform is no longer sufficient. A number of activities should be performed to overcome this issue:

- Applications should be designed in the way to prevent any unauthorized usage;
- App stores should ensure that all data access comes from only authenticated and authorized client apps;
- Users should not grant excessive or unfamiliar permission requests at installation and runtime.
- Users should also update their apps to fix security issues once vulnerabilities are found, and should avoid any suspicious apps.

Read more at: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf

Disclaimer: