S.E. CENTER OF SPECIAL TELECOMMUNICATIONS

CYBER SECURITY CENTER CERT-GOV-MD

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

November 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 November 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

Contents:

Useful advices:

Beware of STARTTLS downgrade attacks

Two engineers from the Golden Frog, an international IT service provider, discovered that some Internet service providers are stripping STARTTLS flag from email traffic that forces sending server to transmit plaintext email over the public Internet, where it is subject to eavesdropping and interception.

STARTTLS is a wildly used extension for plain text communication protocols, which allows to transmit email messages securely between sending and receiving servers. Under normal circumstances, before message transmission, the client inquires destination server whether it supports message encryption. If yes - a TLS session is initiated otherwise the message will be transferred in a plain text. A STARTTLS downgrade attack occurs when an attacker alters server response so that does not contain a STARTTLS option. The problem is that the user will not be notified that the message was sent unencrypted that jeopardizes its confidentiality and integrity.

While it is not always possible to prevent STARTTLS downgrade attacks, it is recommended to use Pretty Good Privacy (PGP) or Secure/Multipurpose Internet Mail Extensions (S/MIME) for email encryption and digital signing in order to stay safe in the Internet.

Read more at:
https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks

Members of OSCE's Informal Working Group met on 7 November 2014 to discuss the implementation of Confidence Building Measures (CBMs)

The meeting, organized by Swiss OSCE Chairmanship, took place at Vienna, Austria and brought together cyber-security experts and representatives from over 50 countries.

The CBMs are risk-reduction measures designed to enhance transparency, reduce misperception and escalation, and increase co-operation and stability between states in the domain of cybersecurity. The initial set of CBMs were adopted in 2013. The states also agreed to meet once a year in order to summarize the results and to discuss future steps of CBMs' development.

During the meeting, participants reviewed cyber-security efforts at the sub-regional level and negotiated the development of a second set of CBMs.

Read more at:

http://www.osce.org/cio/126475

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace." - Newton Lee, a computer scientist.

Case of CryptoPHP. System administrators are target of social engineering attack

A security research team from Fox-IT – an information security Dutch firm, discovered a thread, called CryptoPHP, which tricked system administrators into installing a backdoor on their web server.

Threat actors hosted several web sites in order to provide "free" for anyone access to pirated themes and plugins for Joomla, WordPress and Drupal content management systems. After malicious plugin or theme was installed, it established an encrypted connection to the command-and-control server in order to receive further instructions.

Currently the CryptoPHP is used for injection of links and text into the webpages of the compromised server. That allowed thread actors to increase rank rating of the injected web links in the popular search engines. It is estimated that CryptoPHP compromised more than 20 000 web sites.

Systems administrators are advised to use the following Python scripts in order to verify the presence of the CryptoPHP infection.

https://github.com/fox-it/cryptophp/tree/master/scripts

Read more at:
https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf

Wirelurker: A New Era in iOS Malware

Palo Alto Networks' research team discovered a malware that targets iOS devices from infected Mac computers. The malware was named "Wirelurker" as it spreads through a USB wire.

WireLurker was used to trojanize pirated Mac applications that were uploaded to the Maiyadi App Store - is a site known to host pirated premium Mac, iPhone, and iPad applications. Victims downloaded these applications, installed them on their OS X systems and ran them. On instantiation, WireLurker's entry code was transparently executed, dropping malicious executable files, dynamic libraries and configuration files prior to running the original pirated application. Upon installation WireLurker monitored any iOS device connected via USB with an infected OS X computer and installed downloaded third-party applications or automatically generated malicious applications onto the device, regardless of whether it is jailbroken.

The interesting is that the malware uses unseen before on iOS platform attack methods:

- It is capable to automate generation of malicious iOS applications, through binary file replacement;
- Can infect installed iOS applications similar to a traditional virus;
- Installs third-party applications on non-jailbroken iOS devices through enterprise provisioning.

The following are our recommendations to enterprises and users regarding prevention or mitigation of WireLurker or similar OS X or iOS malware threats:

- Employ an antivirus or security protection product for the Mac OS X system and keep its signatures up-to-date;
- In the OS X System Preferences panel under "Security & Privacy", ensure "Allow apps downloaded from Mac App Store (or Mac App Store and identified developers)" is set;
- Do not download and run Mac applications or games from any third-party app store, download site or other untrusted source.
- Keep the iOS version on your device up-to-date;
- Do not accept any unknown enterprise provisioning profile unless an authorized, trusted party (e.g. your IT corporate help desk) explicitly instructs you to do so;
- Avoid powering your iOS device through chargers from untrusted or unknown sources.
- Do not jailbreak your iOS device

Read more at:
https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

Review of malware underground market in Brazil

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

The report reviled that a malware underground market at Brazil usually represents a post at Facebook, YouTube, Twitter, Skype, or WhatsApp in which are offered for trade illegal products or services. It was also discovered that Brazilian underground today is mostly specialized in banking domain. Therefore there are many offers regarding different banking malware such banking trojans, credit card number checkers, crypters and other. Some offers include tools that were specifically created for attacks against products and services only available in Brazil. The Brazilian underground is also the only known market that offers training services for future cybercriminals.

A cybercriminal can buy the following products at Brazilian underground:

- ***Banking trojans***. These are intended to intercept bank client credentials and/or to redirect client payments to the cybercriminal. In order to do so banking trojans use techniques like Domain Name System poisoning, fake browser window or a specialized malware module called boware, which is able to modify bar code of a payment slip of a Brazilian online store in the way the payment will be transferred to the attacker instead of original seller. The prices are ranging from 155$for Bolware kits to 386$for banking trojan builders and more for banking trojan source codes;
- ***Crypters***. Crypters are special software designed to modify a malware in the way it cannot be detected by an antivirus. Crypters that can prevent all security products from detecting malware are considered “100% fully undetectable (FUD).” If they can only evade several security solutions, they are only sold as “partial” crypters. The prices for FUD cryptes are ranging from 19$to 39$for 1 month license.
- ***Credit card credentials and checkers***. A credit card checker is a special software that allows to debit small amounts of money from specified accounts in order to check if the card number is valid and is ready for illegal transactions. The average price for a valid credit card number varies from 31$to 135$in dependence on the card credit limit.
- ***Phishing pages***. Phishing page allows cybercriminal to steal personal data, redirect victims to the original page and send stolen information via email. The price for a phishing pages usually consist 39$
- ***Social media followers/views/likes***. As the number of followers/views/likes is one of the factors, which influences on the position of the tweet, video or a post in the search results Brazilian underground market sellers offer social media followers to anyone interested. The prices for Facebook likes vary from 8$for 1000 likes to 62$for 10 000 likes. Instagram followers cost at average 35$for 5000 followers. 200 YouTube subscribers cost 8$- the same price for 1000 YouTube views or 1000 Twitter followers.

Brazilian malware underground market is also offering different services. Among them:

- ***Malware checking against security software services***. Cybercriminals need to ensure that their malicious creations will not be detected by security solutions when used. Experienced fraudsters rarely use publicly available file scanners because these usually send scanned files to security companies for detection. Cybercriminals offer malware-checking services for as little as 12$for one month license.
- ***SMS-spamming services***. Some spammers outsource spam sending at prices ranging from 155$for 5,000 text messages to 1,159$for 100,000 messages.
- ***Training services***. What distinguishes the Brazilian underground from others is the fact that it also offers training services for anyone who wants to become a cybercriminal. The most of the trainings courses are focused on fully undetectable crypter programming and fraud training. The trainings are selling as how-to videos. The buyer can usually get training support services via Skype.

Read more at:
http://www.trendmicro.ca/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf

New advanced thread called "Darkhotel" targets hotel visitors

Kaspersky global research team has published a threat intelligence report, which revealed a new advanced persistent threat that targeted unsuspecting guests of several high-end and luxury hotels.

Attackers abused hotels' Wi-Fi networks to lure its victims into installation of fake GoogleToolbar, Adobe Flash player or Windows Messenger infecting their computers with spyware. The attack method involved hotel's Wi-Fi access login screen with a hidden iframe to identify guest's first and last names and to redirect its browser to a malicious webpage. It was also discovered that only specific guests, like government servants and defence industry staff, were attacked, what means that the attackers knew exact date and place of stay of its victim. Once attack succeeded all the traces of it were removed. It is estimated that the threat existed for more than five years, before it was discovered.

Use the following advices in order to stay safe while traveling:

- ***Before you travel***: decide ahead of time what device(s) and data you will actually need, and do your best to limit what you take; do not take with you in trip day-to-day devices; use temporary accounts and devices like an inexpensive laptop or a throw-away prepaid cell phone purchased just for that trip.
- ***During your journey***: do not use hotel or other public networks, or untrusted computers for business needs; do not send sensitive information; assume the sites you visit (even hotel rooms) may be subject to video, audio, or other monitoring.
- ***After you return***: erase all personal information from temporary used accounts and devices; change passwords - that will render the stolen ones useless; reset the temporary devices to the factory-default state to remove any installed malware.

Read more at:
http://securelist.com/blog/research/66779/the-darkhotel-apt/

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

iOS User Security Guide. Part 1

This guide is designed for end users who own an iOS 7.x or iOS 8.x device and want to make beneficial security changes to their device to improve the overall mobile experience in regards to security, safety and privacy.

Security Improvement Instructions. Included are steps to follow to beneficially improve the security posture of your iOS device.

- ***Run the Latest Software Version***. Bugs and security vulnerabilities are inevitable, so it is important to utilize the latest software version available for your device. Many devices will inform you when an update is available, but you can manually instigate an update check to see if your device has a newer update available. In order to check if your device is running the latest software version navigate to “Settings” -> “General” -> “Software Update”; Note: preferably use a Wi-Fi network to download the system update, to reduce cellular data usage
- ***Enable device passcode***. This prevents someone from picking up your device and accessing your data. In order to setup a password navigate to “Settings” -> “Passcode” (or “Touch ID & Passcode”);
- ***Enable SIM card lock***. Enabling SIM card lock prevents a thief from abusing your cellular service and costing you money. In order to setup a SIM card lock navigate to “Settings” -> “Phone” -> “SIM PIN” (you will have to introduce default password for SIM, which is usually "1111"). After the SIM lock feature is activated choose “Change PIN” to ensure that no one can bypass this security measure. Be sure to remember your new PIN.
- ***Enable device auto-lock***. Auto-lock will automatically lock your device after it goes unused for a certain period of time. This potentially prevents someone from picking up your device and accessing your data. In order to activate auto-lock feature navigate to “Settings” -> “General” -> “Auto-Lock”;
- ***Enable restrictions***. This feature allows you to prevent some of your device capabilities, like in-app purchases, to be used without entering a password. This can be useful for parental control or in case, you do not want your relatives, who can access the device, to see or to do more than they should. In order to enable restrictions navigate to “Settings” -> “General” -> “Restrictions”;
- ***Safari fraudulent website warning***. Safari has the ability to warn you if a web site is suspected to be a phishing or fraudulent website designed to trick you into divulging personal information. In order to ensure that “Fraudulent Website Warning” setting is set to “on” navigate to “Settings” -> “Safari”.

Read more at:
https://bluebox.com/ios-user-security-guide/

Disclaimer: