Попередження споживачам: піратське програмне забезпечення може містити віруси
Pirated software may contain malware

Козак А.С., курсант начально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції НАВС
Науковий керівник: старший викладач кафедри *Марченко І.В.*

You decide to order some software from an unknown online seller. The price is so low you just can’t pass it up. What could go wrong?

Whether you’re downloading it or buying a physical disc, the odds are good that the product is pirated and laced with malicious software, or malware. Is Your Software Pirated?

Possible signs of what to look for:

- No packaging, invoice, or other documentation...just a disc in an envelop;
- Poor quality labeling on the disc, which looks noticeably different than the labeling on legitimate software;
- Software is labeled as the full retail version but only contains a limited version;
- Visible variations (like lines or differently shaded regions) on the underside of a disc;
- Product is not wrapped correctly and is missing features like security tape around the edges of the plastic case;
- Typos in software manuals or pages printed upside down;
- User is required to go a website for a software activation key (often a ploy to disseminate additional malware). [5]

Today, the National Intellectual Property Rights Coordination (IPR) Center–of which the FBI is a key partner–is warning the American people about the real possibility that illegally copied software, including counterfeit products made to look authentic, could contain malware. An increasing amount of software installed on computers around the world–including in the U.S.–is pirated and that this software often contains malware. Pirated software can be obtained from unknown sellers and even from peer-to-peer networks. The physical discs can be purchased from online auction sites, less-than-reputable websites, and sometimes from street vendors and kiosks. Pirated software can also be found pre-installed on computers overseas, which are ordered by consumers online and then shipped into the United States. Cyber criminals are not stopping at infecting just a few computers - the threat is much bigger. [2]

Who's behind this crime? Criminals, hackers and hacker groups, and even organized crime rings. And the risks to unsuspecting consumers? For starters, the inferior and infected software may not work properly. Your operating system may slow down and fail to receive critical security updates. But the greater danger comes from potential exposure to criminal activity–like identity theft and financial fraud–after malware takes hold of your system. [5]

Hackers mount cyber-attacks - mainly by sending viruses into computer systems - countless times every day. Cyberspace has no borders and is presenting lucrative opportunities for organised criminals, who steal data and electronic cash. There's an even bigger security issue though. If ever there is a third world war, circuits and servers could be the battlegrounds. These are the issues under discussion at Queen's University's second annual World Cyber Security Summit in Belfast. The keynote speaker is Eugene Kaspersky, a Russian expert who founded Europe's largest anti-virus company. He said cyber-crime is unfortunately a very successful enterprise. [3]

Software Buying Tips for Consumers

When buying a computer, always ask for a genuine, pre-installed operating system, and then check out the software package to make sure it looks authentic.

Purchase all software from an authorized retailer. If you're not sure which retailers are authorized, visit the company website of the product you're interested in. Check out the company's website to become familiar with the packaging of the software you want to buy.

Be especially careful when downloading software from the Internet, an increasingly popular source of pirated software. Purchase from reputable websites.

Before buying software off the beaten path, do your homework and research the average price of the product. If a price seems too good to be true, it's probably pirated. If you're not the paying customer, you're very likely to be the product. [1]

Some very real dangers:

Once installed on a computer, malware can record your keystrokes (capturing sensitive usernames and passwords) and steal your personally identifiable information (including Social Security numbers and birthdates), sending it straight back to criminals and hackers. It can also corrupt the data on your computer and even turn on your webcam and/or microphone.

Malware can spread to other computers through removable media like thumb drives and through e-mails you send to your family, friends, and professional contacts. It can be spread through shared connections to a home, business, or even government network. Criminals can also use infected computers to launch attacks against other computers or against websites via denial of service attacks.

And know this: Pirated software is just one of the many threats that the IPR Center and the FBI are combating every year. The theft of U.S.

intellectual property–the creative genius of the American people as expressed through everything from proprietary products and trade secrets to movies and music–takes a terrible toll on the nation. It poses significant (and sometimes life-threatening) risks to ordinary consumers, robs businesses of billions of dollars, and takes away jobs and tax revenue. An example of a malware is Cryptolocker Ransomware. It encrypts user's files. The FBI is aware of a file-encrypting Ransomware known as CryptoLocker. Businesses are receiving emails with alleged customer complaints containing attachments that when opened, appear as a window that is in fact a malware downloader. This downloader installs the actual CryptoLocker malware.

The verbiage in the window states that important files have been encrypted using a unique public key generated for the computer. To decrypt the files you must obtain the private key. A copy of the private key is located on a remote server that will destroy the key after the specified time shown in the window. The attackers demand payment of a ransom ranging from $100 to $300 to decrypt the files.

Unfortunately, once the encryption of the files is complete, decryption is not feasible. To obtain the file specific Advanced Encryption Standard (AES) key to decrypt a file, you need the private RSA key (an algorithm for public key cryptography) corresponding to the RSA public key generated for the victim's system by the command and control server. However, this key never leaves the command and control server, putting it out of reach of everyone except the attacker. The recommended solution is to scrub your hard drive and restore encrypted files from a backup.

As with any virus or malware, the way to avoid it is with safe browsing and email habits. Specifically, in this case, be wary of email from senders you don't know, and never open or download an attachment unless you're sure you know what it is and that it's safe. Be especially wary of unexpected email from postal/package services and dispute notifications. [4]

Cyber-security is not a national problem, it's international. [3]

Ця стаття присвячена злочинАМ сучасності, які поширені на весь світ, це – кіберзлочинність. У науковій роботі висвітлена тема «Піратського програмного забезпечення, що може містити віруси». У своїй праці я спробував якомога ширше розкрити проблеми, пов'язані із фальшивим програмним забезпеченням та негативними наслідками, що, зазвичай, можуть виникнути в результаті його використання, а також навів приклади, описав характерні ознаки та шляхи уникнення таких програм. Ця тема є дуже актуальною, адже на сьогоднішній день все більше і більше злочинів здійснюється за допомогою використання комп'ютерних мереж та програмних продуктів. Правоохоронні органи повинні докладати великі зусилля на подолання злочинів цього типу, які стрімко наближаються до глобальних масштабів.

Сподіваюсь, що інформація, котру я використав у своїй статті, допоможе Вам, шановні читачі та колеги, не користуватися піратськими програмними породуктами і не стати жертвою кіберзлочину.

Список використаних джерел:

1. Вудворд Алан, професор, комп'ютерний факультет Університету Суррея: Точка зору: як хакери експлуатують 'сім смертних гріхів» – Грудень 2012
2. Москвич К., техн. репортер, Новини Бі-бі-сі: П'ять найбільших світових загроз – Квітень 2012
3. Пейдж Кріс, репортер новин Бі-бі-сі: Борці з кіберзлочинністю – Березень 2012;
4. Центр інтернет злочинності: Оголошення Служби Громадської інформації «Криптолокер здирників шифрує файли користувачів» – Жовтень 2013 / http://www.ic3.gov
5. Центр інтернет злочинності: Оголошення Служби Громадської інформації «Для споживачів: віруси у піратському ПЗ» – Червень 2013 / http://www.ic3.gov

Forensic Science

Labunskiy R.D., cadet of the faculty training for special units NAIAU

Forensic science (often shortened to **forensics**) is the application of a broad spectrum of sciences and technologies to investigate and establish facts of interest in relation to criminal or civil law. The word forensic comes from the Latin forēnsis, meaning «of or before the forum.» In Roman times, a criminal charge meant presenting the case before a group of public individuals in the forum. Both the person accused of the crime and the accuser would give speeches based on their sides of the story.

There are many definitions of «Forensic Science»:

Definition of Forensic-Science №1

Forensic science is the application of natural sciences to matters of the law. In practice, forensic science draws upon physics, chemistry, biology, and other scientific principles and methods. Forensic science is concerned with the recognition, identification, individualization, and evaluation of physical evidence. Forensic scientists present their findings as expert witnesses in the court of law.

(Midwest Forensics Resource Center at the U.S. Dept. of Energy)

Definition of Forensic-Science №2

The word «**forensic**» means «pertaining to the law»; forensic science resolves legal issues by applying scientific principles to them.

(Hall Dillon, Bureau of Labor Statistics)

Definition of Forensic-Science №3

Forensic Science is the application of the methods and techniques of the basic sciences to legal issues. As you can imagine Forensic Science is a very broad field of study. Crime Laboratory Scientists, sometimes called Forensic Scientists or, more properly, Criminalists, work with physical evidence collected at scenes of crimes.

(California Criminalistics Institute)