CyberSecurity MALAYSIA
An agency under MOSTI

www.cybersecurity.my

eSecurity

The First Line of Digital Defense Begins with Knowledge

Vol 31 - (Q2/2012)

Rogue Antivirus
Has the 'Flame' Malware been Doused Completely?
Kriptografi di Sekeliling Kita

"Security in IT is like locking your house or car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target."

Paul Herbka

KDN License number PP 15526/10/2012(031392)

ISSN 1985-1995

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Your **cyber safety** is our **concern**

Securing Our Cyberspace

CyberSecurity Malaysia, an agency under Malaysia's Ministry of Science, Technology and Innovation was set up to be the national cyber security specialist centre. Its role is to achieve a safe and secure cyberspace environment by reducing the vulnerability of ICT systems and networks while nurturing a culture of cyber security. Feel secure in cyberspace with **CyberSecurity Malaysia.**

www.cybersecurity.my

- Cyber999 / Computer Emergency Response (MyCERT)
- Digital Forensics
- Security Assurance
- Malaysia Common Criteria Certification Body (MyCB)
- Security Management and Best Practices
- Training and Outreach
- Cyber Security Policy Research

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my

CEO MESSAGE

Considerable work has been done in the first half of this year in various forms to come to understandings amongst a cyber security community of how the community can work together to enhance cyber security. We have come to believe the e-Security Bulletin is a particularly appropriate for sharing new knowledge and identifying new challenges, so that we can expand the discussion on relevant issues at suitable forums later on.

Beginning in this year, we saw a number of resolutions derived at local and global forums in combating the cyber threats. However, they seem to be far from effective in addressing the rapidly-changing world of cyber security threats. It is alarming to see today how cyber threats are growing in sophistication, and how the malicious software are emerging in frequency and gravity. I have no better examples than to quote the Stuxnet, Duqu and Flame malware, as well as the creation of new phenomenon towards "digital hacktivism" that have threatened and will continue to threaten us all.

For so long, we have observed that Internet users have not given adequate attention to the risks posed by cyber threats. The rise of cyber incidents in the first half of this year, as reported to MyCERT (www.mycert.org.my), shows that we have to do more to protect the nation's cyberspace. It is even more alarming that cyber threats are encroaching into every sphere of our lives in multi-dimensional forms.
Perhaps, we should adopt a fundamental shift in approach towards solving the problems; amongst others is to combine our efforts and ideas, and to act fast against cyber threats which are growing exponentially. Equally important, we should also take up the issue of the human aspect of cyber security more seriously. This is to avoid them from falling victim to the weakest link – the human factor. Implementing the latest most advanced technology and security safeguards are to no avail if the users are not properly trained to be part of the cyber security plan. History also shows reliance on an advanced technology is doomed if the people operating and using the technology are not fully trained and given an adequate education.

It is the goal of e-Security bulletin here is to stimulate discussion on relevant common issues. I believe that all of us are intrinsically linked to cyber security in many ways and this bulletin provides a comprehensive concept of security and a mature platform for raising our views that can subsequently benefit us all. Thanks to those who have contributed their articles for this publication; and to others - enjoy your reading.

Thank you and warmest regards,
Zahri bin Yunos
Acting CEO, CyberSecurity Malaysia

EDITOR'S DESK

Another quarter has gone by and now we brought you the second edition of eSecurity Bulletin for 2012. For the first half of the year, news are reporting of a new cyber threat, known as 'Flame', that appears to be targeting systems in several countries in Middle East. This newly malware provides an attacker with remote access to a hijacked computer. This malware can "listen" to your conversations; even "look" through your webcam. To know more about this Flame malware, please read through our published article entitled "Has the 'Flame' malware been doused completely? "

If Flame malware does not scare you, we have to be aware of computer malicious software that deceives you into paying for fake antivirus. Equip your knowledge and not be a victim by reading our article entitled "Do not be deceived with fake antivirus". And if you think encryption is a complex subject, be amazed that encryption has been used extensively in our life. Read "Kriptografi di sekeliling kita" for further information.

Finally not to forget our contributors, thank you so much. Your commitment and time in making this bulletin informative is very much appreciated.

Best Regards,
Sabariah Ahmad, Editor

TABLE OF CONTENTS

READER ENQUIRY
Security Managment and Best Practices, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation (MOSTI) • E-mail: smbp@cybersecurity.my

PUBLISHED AND DESIGN BY
CyberSecurity Malaysia (726630-U)
Block A, Level 8, Mines Waterfront Business Park, No 3,
Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan.

MyCERT 2nd Quarter 2012 Summary Report

Introduction

The MyCERT Quarterly Summary Report provides an overview of activities carried out by the Malaysian Computer Emergency Response Team (hereinafter referred to as MyCERT), a department within CyberSecurity Malaysia. These activities are related to computer security incidents and trends based on security incidents handled by MyCERT. The summary highlights statistics of incidents according to categories handled by MyCERT in Q2 2012, security advisories and other activities carried out by MyCERT personnel. The statistics presented in this report reflect only the total number of incidents handled by MyCERT and not elements such as monetary value or repercussions of the reported incidents. Computer security incidents handled by MyCERT are those that occur or originate within the Malaysian constituency. MyCERT works closely with other local and global entities to resolve computer security incidents.

Incidents Trends Q2 2012

Incidents were reported to MyCERT by various parties within the constituency as well as from foreign-based sources, which included home users, private sector entities, government agencies, security teams, foreign CERTs, Special Interest Groups including MyCERT's proactive monitoring on several cyber incidents.

From April to June 2012, MyCERT, via its Cyber999 service, handled a total of 2,441 incidents representing a 22.33 percent decrease compared to Q1 2012. In Q2 2012, incidents such as Cyber Harassment, Denial of Service and Vulnerabilities Report had increased while other incidents had decreased tremendously.

Figure 1 illustrates incidents received in Q2 2012 classified according to the type of incidents handled by MyCERT.

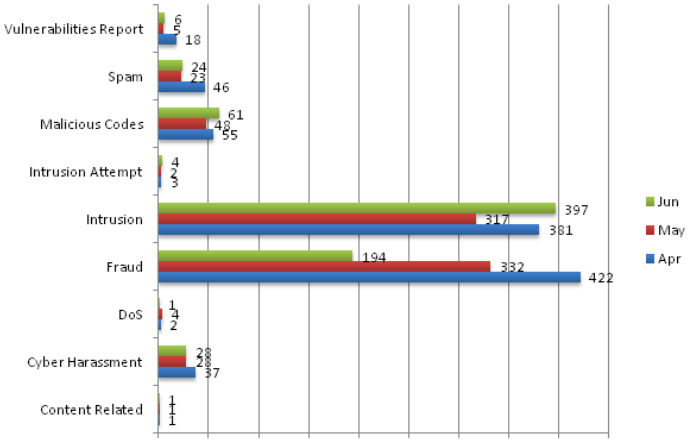


Figure 1: *Breakdown of Incidents by Classification in Q2 2012*

Figure 2 illustrates incidents received in Q2 2012 classified according to the type of incidents handled by MyCERT and its comparison with the number of incidents received in the previous quarter.

Categories of Incidents	Quarter		Percentage
	Q4 2011	Q1 2012	
Intrusion Attempt	46	9	-80.43
Denial of Service	5	7	40
Spam	201	93	-53.73
Fraud	1491	948	-36.42
Vulnerability Report	16	29	81.25
Cyber Harassment	80	93	16.25
Content Related	7	3	-57.14
Malicious Codes	189	164	-13.23
Intrusion	1108	1095	-1.17

Figure 2: *Comparison of Incidents between Q1 2012 and Q2 2012*

Figure 3 shows the percentage of incidents handled according to categories in Q2 2012.

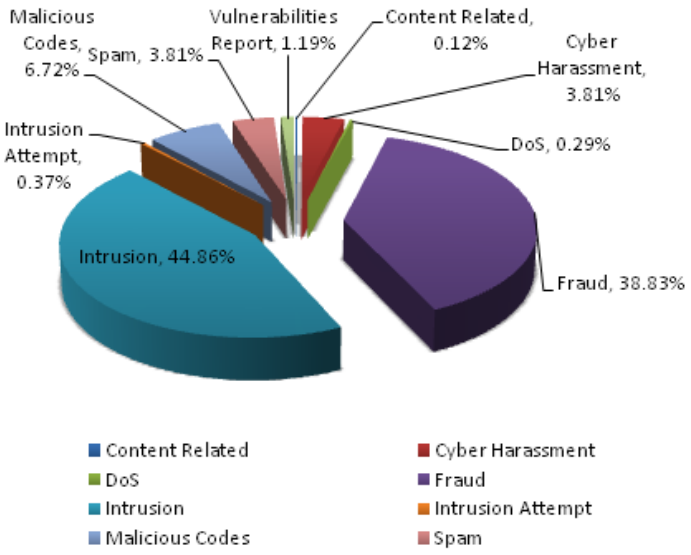


Figure 3: *Percentage of Incidents in Q2 2012*

In Q2 2012, a total of 1,095 incidents were received on Intrusion representing a 1.17 percent decrease compared to the previous quarter. The Intrusion incidents reported to us are mostly web defacements or known as web vandalisms followed by account compromise. Based on our findings, the majority of web defacements were due to vulnerable web applications or unpatched servers involving web servers running on IIS and Apache.

In this quarter, we received a total of 844 .MY domains defaced belonging to various private and government agencies compared to 689 .MY defaced domains in Q1 2012. The increase in web defacements in this quarter may be due to a recent issue presented in the local media that caught the attention of many Internet users. MyCERT had responded to web defacement incidents by notifying respective Web Administrators to rectify the defaced websites by following our recommendations.

Figure 4 shows the breakdown of domains defaced in Q2 2012.

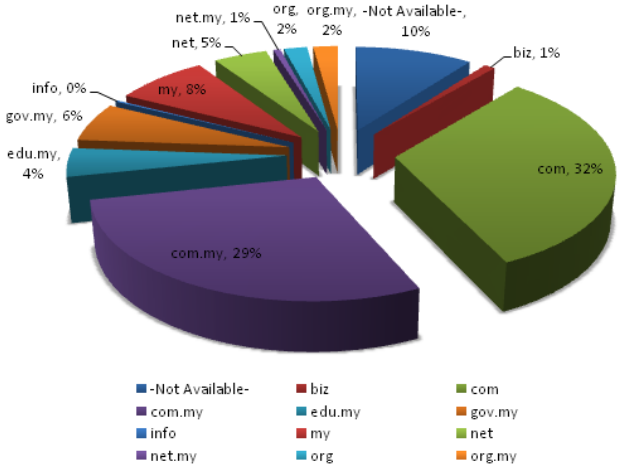


Figure 4: *Percentage of Web Defacement by Domain in Q2 2012*

Account compromise incidents still prevails in this quarter as was in the previous quarter. However the numbers had decreased to 44 incidents compared to 68 incidents in Q1 2012. The decrease may indicate a positive sign that Internet users are aware of the threats facing them and are taking preventive measures to safeguard their accounts. The trend that we observed in Q1 2012 still prevails in Q2 2012 in which unscrupulous individuals are taking advantage of various techniques to compromise legitimate accounts belonging to other Internet users. The majority of account compromise incidents involved email and social networking accounts. Account compromise incidents could be prevented if users practice good password management such as using strong passwords and safeguarding their passwords.

Users may refer to the URLs below on good password management practices:
http://www.auscert.org.au/render.html?it=2260
http://www.us-cert.gov/cas/tips/ST04-002.html

Incidents involving fraud had decreased to about 36.42 percent in this quarter compared to the previous quarter but continue to be a trend in this quarter and is one of the most frequently reported incidents to Cyber999.

A total of 948 fraud incidents were received in this quarter, from organisations and home users. Phishing incidents involving foreign and local brands continue in this quarter along with other types of frauds. Incidents on job scams had also increased targeting other industries such as hospitals and specialist centres.

Cyber harassment incidents had increased in this quarter with a total of 93 incidents representing 16.25 percent increase. Harassment incidents generally involved cyberstalking, cyberbullying and threats done via emails and social networking sites. We advised users to be very cautious with whom they communicate on the net particularly with unknown individuals and be ethical on the net.

In Q2 2012, MyCERT handled 164 incidents on malicious codes, which represents a 13.23 percent decrease compared to the previous quarter. Some of the malicious code incidents we handled are active botnet controllers, hosting of malware or malware configuration files on compromised machines and malware infections to computers. In this quarter, we had issued an advisory on the DNSChanger malware affecting computers worldwide, which started propagation since November 2011. DNSChanger is a type of malware that infect computers with the purpose of diverting traffic to potentially illegal and malicious websites. The malware modifies the infected computer's DNS server settings replacing it with DNS server belonging to an attacker.

MyCERT had come up with a tool that can detect computers infected with DNS changer malware and clean up the infected computer. More information on the DNSChanger malware is available at: http://www.mycert.org.my/en/services/advisories/mycert/2012/main/detail/855/index.html.

Advisories and Alerts

In Q2 2012, MyCERT had issued a total of 16 advisories and alerts for its constituency which involved popular end-user applications such as Adobe PDF Reader and Multiple Microsoft Vulnerabilities. Attackers often compromise end-users' computers by exploiting vulnerabilities in the users' applications. Generally, the attacker tricks the user in opening a specially crafted file (i.e. a PDF document) or web page.

Readers can visit the following URL on advisories and alerts released by MyCERT: http://www.mycert.org.my/en/services/advisories/mycert/2011/main/index.html.

Conclusion

In conclusion, the number of computer security incidents reported to us in this quarter had decreased slightly compared to the previous quarter. However, some categories of incidents reported to us continue to increase. The slight decrease could be a positive indication that more Internet users are aware of current threats and are taking proper measures against them. No severe incidents were reported to us in this quarter and we did not observe any crisis or outbreak in our constituencies. Nevertheless, users and organisations must be constantly vigilant of the latest computer security threats and are advised to always take measures to protect their systems and networks from these threats.

Internet users and organisations may contact MyCERT for assistance at the below contact:

E-mail: mycert@mycert.org.my
Cyber999 Hotline: 1 300 88 2999
Phone: (603) 8992 6969
Fax: (603) 8945 3442
24x7 Mobile: 019-266 5850
SMS: Type CYBER999 report <email> <report> & SMS to 15888
http://www.mycert.org.my/

Please refer to MyCERT's website for latest updates of this Quarterly Summary. ■

CyberCSI – Half Year 2012, Summary Report

Introduction

For the first half of 2012, CyberCSI summary provides an overview of activities undertaken by the Digital Forensics Department (hereinafter referred to as DFD) of CyberSecurity Malaysia for the month of January to June 2012. These activities were focussed on case analysis received from Law Enforcement Agencies (hereinafter referred to as LEAs) and Regulatory Bodies (hereinafter referred to as RBs) such as the Royal Malaysian Police (RMP), the Malaysian Anti-Corruption Commission (MACC), the Malaysian Communications and Multimedia Commission (MCMC) and the Securities Commission Malaysia (SC), This summary will also highlight the training sessions and talks given to LEAs, RBs and the public based on Digital Forensics own module and also reviews on DFD Research and Development activities. Forensic cases include cases on Computer Forensics, Mobile Forensics, Audio Forensics and Video Forensics. All cases were handled by Digital Forensic Analysts who are specialised in their respective fields.

The summary of this report includes statistics for forensic cases, trainings and lectures to LEAs and RBs. For statistics on forensic cases, it describes the number of cases and type handled by the DFD in the first six (6) months of 2012. For trainings and lectures, these involved the participant from authorities and the universities. The objective of these trainings and lectures is to share knowledge between our experts and participants so that both parties can get the benefits, where latest issues, challenges and technologies are discussed and shared. The report briefly discussed DFD Quality Management System services. DFD was offered to LEAs and RBs in Malaysia to develop Digital Forensics Laboratory Quality Management Systems in accordance with ASCLD/LAB-International and ISO/IEC 17025:2005 requirements. At the end of the report, it also highlighted the training sessions and talks given to LEAs, RBs and public based organisations on digital forensic modules.

ASCLD/LAB-International Quality Management System (QMS)

CyberSecurity Malaysia's Digital Forensic Laboratories has been recognised as a pioneer organisation in Asia that obtained accreditation from ASCLD / LAB. It is a great achievement for CyberSecurity Malaysia. CyberSecurity Malaysia started this initiative since 2008. With this recognition, DFD can assist other digital forensic laboratories to go for this standard. There are a few digital forensic laboratories in Malaysia which has yet to obtain this certification of accreditation. This accreditation is recognised internationally.

Based on the situation, DFD take opportunities to offer its services to develop a Quality Management System (QMS) based on ASCLD/LAB International and ISO/IEC 17025:2005 requirements for Digital Forensic Laboratories to LEAs and RBs who are interested to obtain such accreditation. DFD will also provide the consultancy for the development of laboratories.

Our services will cover:

- A forensics and security policy to ensure adherence to strict regulations when handling and processing evidence through Quality Manual, Training and Gap Analysis which satisfies all the criterias set by ASCLD / LAB in obtaining certification.

- To develop a forensics flow and Standard Operating Procedures (SOPs) in ensuring the activities and operations are guided through a recognised forensics standard. This will ensure evidence is admissible in a Court of Law.

- To give consultancy on physical security and operational procedures in handling and processing digital evidence.

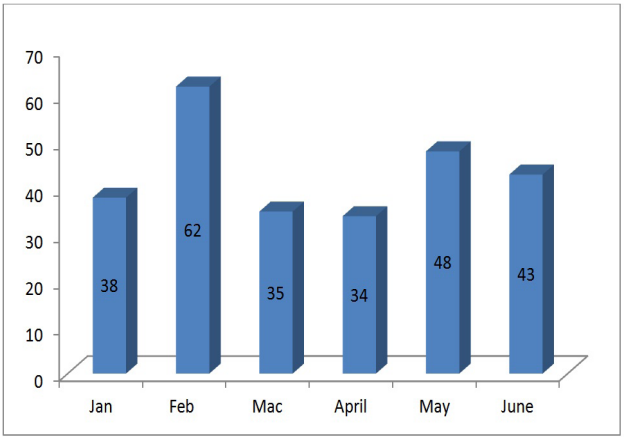
- To provide SOPs and safety requirements to acquire, replicate, handle, analyse, store and process any digital evidence like Biometric, CCTV, Fire Suppression Systems, HVAC Systems, Humidity and Temperature Controller Systems.

Hopefully in the future, many more LEAs and RBs show interest in seeking advice from us for ASLCD / LAB -International certifications.

Digital Forensics and Data Recovery Statistics

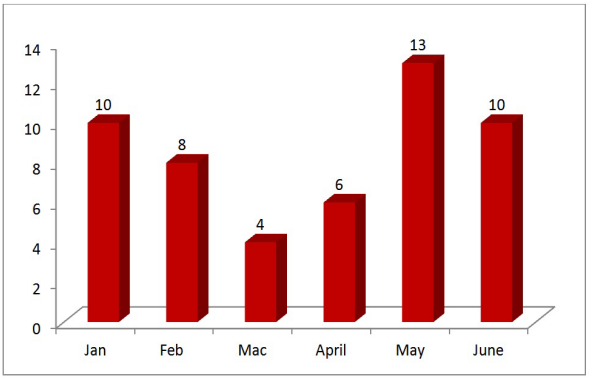
- Digital Forensics Case Statistics

As of 30th June, the statistics for cases on Digital Forensics that DFD received was at 260 cases. These cases, received on a monthly basis, are summarised in the graph below:



- Data Recovery Case Statistics

The number of data recovery cases received from 1st January until 30th June was at 51 cases. The summary cases received by month are as below:



Talk and Training

- Training

During this period, DFD conducted several training sessions, which involved participants from LEAs, RBs and Universities. The training that they requested focussed on Digital Forensics for First Responders and Digital Forensics Investigation & Analysis. The objectives of the training programmes were to share knowledge between DFD experts and participants so that both parties can benefit and discuss latest issues and technologies. These training sessions were beneficial for them particularly in understand the role of First Responders and being able to produce a high quality analysis result.

- Talk

For these six months, DFD has conducted several talks as requested by LEAs and RBs. Favourite topics requested by them are mostly related to digital forensics and information security in Malaysia. The sessions were designed to create awareness on the importance of digital forensics to employees at these agencies and the need to practice it on a daily basis. In addition to training professionals at LEAs, stakeholders and other government agencies, these sessions also help to ensure sustainability and effective dissemination of information and resources.

Conclusion

Trainings and talks are important elements that need to be balanced with fast growing complexities of information technology and cyber crimes. Therefore, DFD will continue to focus on those identified fields in order to contribute expertise to countries in the field of digital forensics. ■

Rogue Antivirus

BY | Farah Binti Ramlee

"Solid and trusted antivirus protection is an educated move in the right direction. Ignorance is not an option no matter how blissful it may be."

Introduction

There's a saying when there is good, there will always be bad. The dominant concepts of Ying and Yang are never far apart from the daily routines of our lives including in the vast developing IT infrastructure arena. Ever since the world was slammed by Kevin Mitnick's computer and communications-related crimes, bad viruses and malicious software are aggressively spreading and evolving to be much smarter and more dangerous.

Throughout the years, it is handful job for the legitimate antivirus developers and companies as they too need to evolve in order to be a few steps ahead of the more matured and sophisticated viruses or malicious attacks. There are many ways malicious attacks are being performed and one of them is by using social engineering methods. By using good social engineering techniques, something good may very well turn to bad.

This phenomenal occurrence whereby rogue antivirus software relies on social engineering is often designed to defeat the security built into modern operating systems and browser software that causes an unsuspecting user to unwittingly install malicious codes supplied by an attacker on their computers. This essentially provides a loophole without realisation. Instead of removing the viruses and malicious wares, it installs them. It makes things easier and merry for an attacker as they are getting smarter every day.

Learn the behavioural of the rogue antivirus

A. Modus operandi

Perpetrators of rogue security software scams use a wide variety of methods to fool potential victims. One very common method is to pop up a flashing or a seemingly scary message when visiting a website that says, "Your PC is infected with a virus. Click here to fix" [1]. If the advertisement is clicked on, this action may be authorising it to download the malicious software to the computer and, once installed, messages will be popping out about viruses, spyware, etc, on the computer. This can only be fixed by buying the "premium" version of the product.

Some rogue security software, however, propagate onto computers of end-users as drive-by downloads which exploit security vulnerabilities in web browsers, PDF viewers, or e-mail clients to install themselves without any manual interaction [2].

More recently, malware distributors have been utilising SEO poisoning techniques by pushing infected URLs to the top of

search engine results about recent news or events. People looking for articles on such subject matters on a search engine may encounter results that, upon being clicked, redirect them through a series of sites before arriving at a landing page that says their machines are infected and pushes a download to a "trial " of a rogue programme. A 2010 study by Google found 11,000 domains hosting rogue antivirus software, accounting for 50 percent of all malware delivered via Internet advertising [2].

B. Characteristics

A few of the characteristics that would identify the programme as a rogue antivirus are listed below [3]:

- Rogue antivirus programmes often generate more "alerts" than software made by reputable companies
- Users may be bombarded with pop-ups, even when not online
- High-pressure sales copy will try their very best to convince users to buy the programme immediately
- If a user's machine has been infected, the computer may dramatically slow down
- Other signs of infections include: new desktop icons; new wallpapers, or having your default homepage redirected to another site

C. Installation Process

In most cases, rogue antivirus comes in the form of package installers rather than a single malicious executable file. In this article, AntiSpyware is chosen as a rogue antivirus example. By clicking the AntiSpyware's rogue antivirus package installer, an installation wizard will appear as what will normally appear during a legitimate antivirus installation. AntiSpyware installer is being run as shown in Figure 1. Usually, this is the point where the malware starts to reside in a victim's computer, which the victim personally had chosen to install it into his/her machine earlier. This really shows that the social engineering techniques by mimicking legitimate antivirus solutions actually works. Some rogue antivirus even issues end-user license agreements (EULA), and users or victims, as expected, will blindly accept it and install the malware into their machines.

Figure 1: *Rogue Anti-Spyware installer*

An End-User License Agreement as shown in Figure 1.1 will pop up during installation. Naturally, end-users would just continue the installation without reading the agreement at hand. This in turn, allow malware or spyware to be installed together without notice.

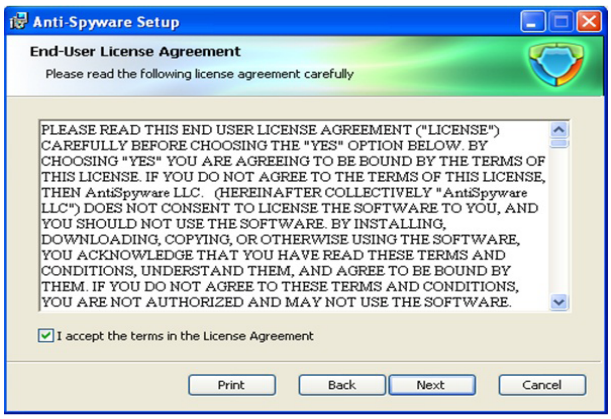


Figure 1.1 *End-User License Agreement*

Once the installation is complete, the rogue antivirus will also feature a small icon enabling them to seemingly act as the real antivirus programme as shown in Figure 1.2.

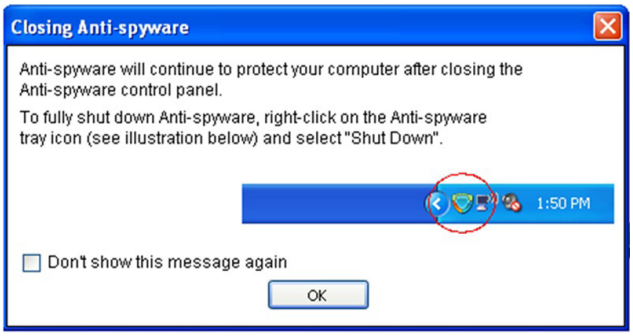


Figure 1.2 *Small icon at taskbar*

D. Rogue Antivirus Symptomps

After completing the installation, a victim will allow the AntiSpyware software to start scanning his/her system. The rogue antivirus will then identify the viruses that reputedly infected the victim's computer.

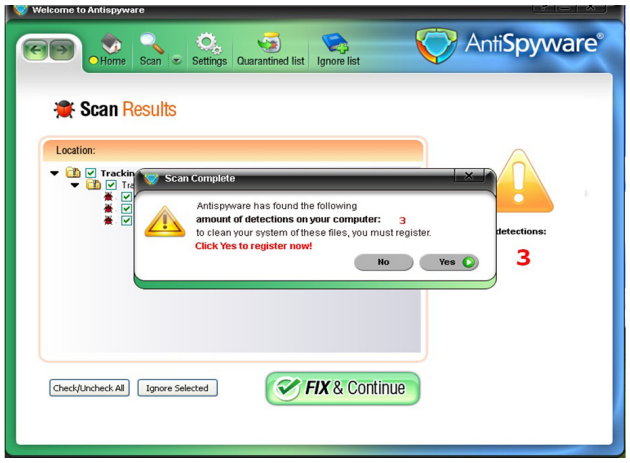


Figure 1.3 *AntiSpyware scanning*

After completion of scanning, the rogue antivirus will prompt a message that indicates multiple viruses were detected and the software will pop out a removing action as shown in Figure 1.3. Before a user can utilise the "full version" of the AntiSpyware and remove the detected viruses as shown after the scanning process, they will be forced to register for activation as depicted in Figure 1.4.

In an AntiSpyware scenario, a victim will automatically be directed to an innocent looking fraudulent website insisting for payment as shown in Figure 1.5

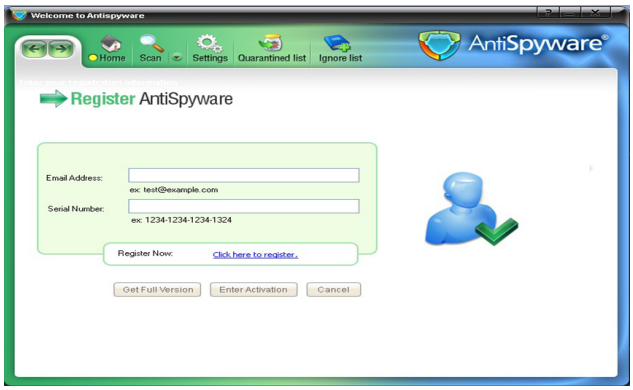


Figure 1.4 *Registering AntiSpyware*

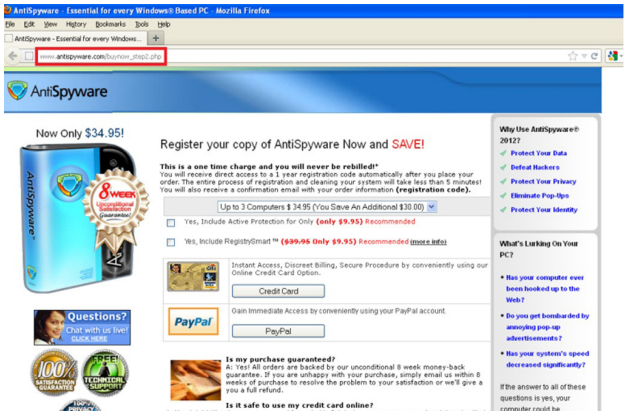


Figure 1.5 *Fraudulent Website*

Figure 1.6 displays the credit card payment gateway that is assigned after a user has chosen credit card as his/her method of payment, hence, falling for the fake.

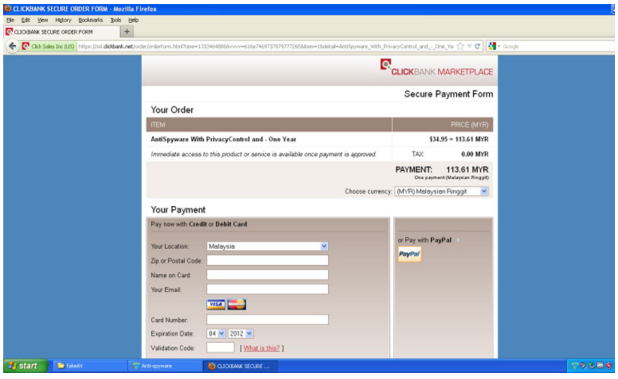


Figure 1.6 *Credit card payment gateway*

Other symptoms that would be portrayed by the rogue antivirus, both supported by

Symantec Corporation and Trend Micro Incorporated, are recurring annoying pop-up notifications even when offline and conjuring the infamous "Blue Screen of Death". This later generates a fake start-up image trying to convince victims to purchase the rogue antivirus to stop the supposed attacks [4][5].

More symptoms were reported by Trend Micro and are listed below [4]:

It could slow down computer performance

- Redirects a victim's homepage to another site
- Create new desktop shortcuts and change the desktop's wallpaper
- Automatically downloads other software after computer reboots
- Flooding the system with adult/porn site URLs
- Some computers will experience memory issues such as the corruption of secondary memory and boot sectors

How to remove and uninstall a rogue antivirus?

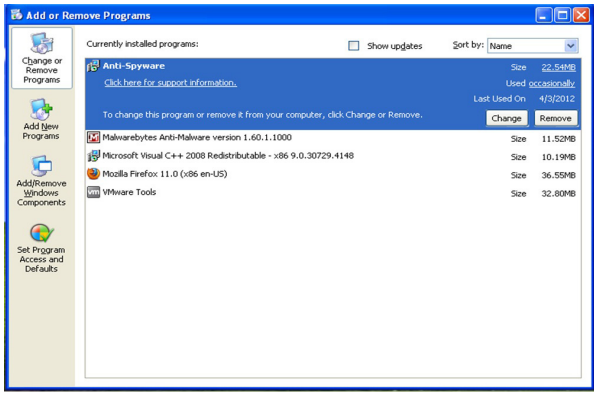


Figure 2 *Add or Remove Programmes*

A. Uninstalling and removing a rogue antivirus

Victims who started to notice the maliciousness of the software will usually start to panic and try their best to remove it. Common practice dictates, add/remove programmes will be used to uninstall the unwanted installed applications as shown in Figure 2.

For this example, even after the completion of programme removal, the small icon is still visible at the taskbar proving that the rogue antivirus installed earlier was not completely removed or wiped out.

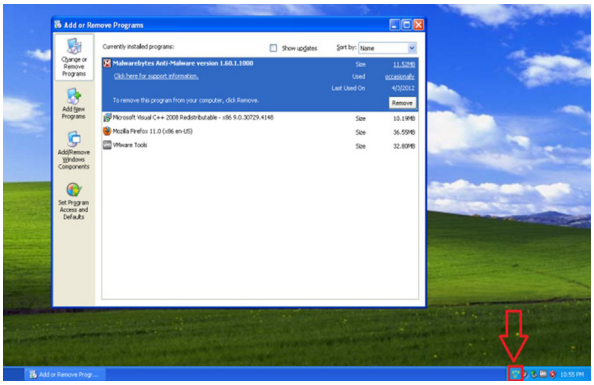


Figure 2.1 *After programme removal, small icon is still visible at taskbar*

In most cases, victims are able to fully clean and wipe out these malicious programmes by using up-to-date antivirus or antimalware software. There are several free products out there and most of them are capable in detecting and removing them. As a quick example, in this article, Malwarebytes Anti-malware (personal edition) software was used as the removal tool. Malwarebytes was used to scan the infected computer and in just a few minutes, eight malware objects were detected. The malware objects were detected as Rogue Antispyware, according to Malwarebytes' virus signature. Since Malwarebytes, with the latest updated signature, was able to recognise the rogue antivirus, the removal process will cause no issue to the victims.

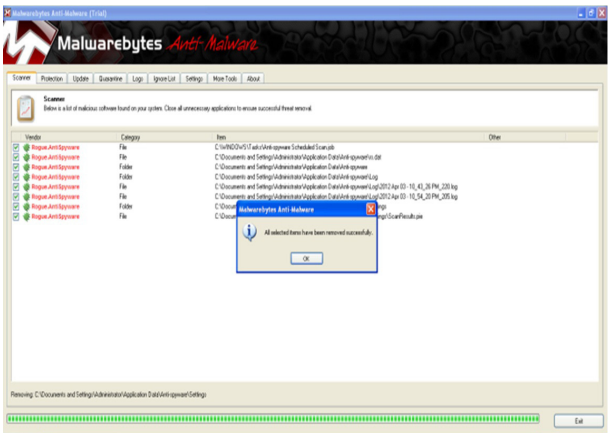


Figure 2.2 *Malwarebytes detection and complete removal*

B. Malware detection

Usually, rouge antivirus can be detected and removed using the most up-to-date version of antimalware or antivirus. To strengthening this statement, the setupxv.exe of the AntiSpyware installer file was uploaded to VirusTotal, www.virustotal.com, a free online virus, malware and URL Scanner. (Note:This is not an article to promote any type of product but just want to highlight that there are solutions available out there to assist in detecting the rogue antivirus.) 31 out of 42 antivirus listed were able to detect that the provided setupxv.exe file is a malicious malware. As shown in Figure 2.4, we are able to conclude that most antivirus or antispyware solutions from trusted companies successfully detected the malicious content and kept their database updated with the latest threats caused by rogue antivirus.

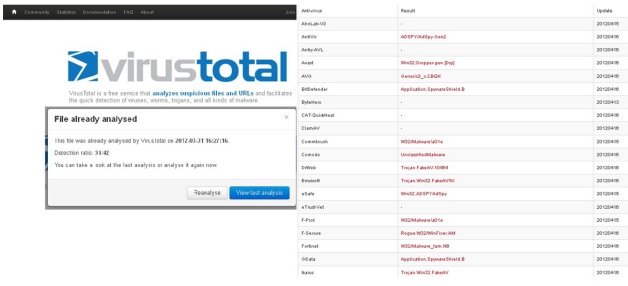


Figure 2.3 *VirusTotal analysis results*

Conclusion

It is highly recommended to install antivirus or antispyware products from trusted companies. The lists of several legitimate antivirus solutions that can be used for reference are listed at www.virustotal.com and www.virusbtn.com. Be sure to use the latest versions of this solution, and make sure the signatures are also updated. If the antivirus scan result detects any suspicious programmes or applications, remove them immediately.

Many of these rogue programmes have legitimate sounding names to fool potential victims, and may even use pop-up windows that look nearly identical to those found in real antivirus programmes or in Microsoft Windows. Do not be fooled and do not assume that a respectable website has truthful and legitimate content. A good rule of thumb is to always assume that these ads are bogus and never click on them. This includes the ads received through email or links to a "great, free antivirus programme!" that you come across in website forums [1]. ■

References

1. *Josh Kirschner. (2009, October). Protect Yourself from Fake Security Software. Available: http://www.techlicious.com/how-to/protect-yourself-from-fake-security-software/*
2. *Wikipedia. Rogue security software. Available: http://en.wikipedia.org/wiki/Rogue_security_software*
3. *Jim and Audri Lanford. 10 Tips to help you avoid fake anti-virus software scams: Internet ScamBusters #232. Available: http://www.scambusters.org/fakeantivirus.html*
4. *Trend Micro Incorporated. (2010, July). FakeAV The Growing Problem. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_fakeav-growing-problem.pdf*
5. *Symantec Corporation. Symantec Power Eraser User Guide. Available: http://www.symantec.com/theme.jsp?themeid=spe-user-guide*

Has the 'Flame' Malware been Doused Completely?

BY | Fortinet

"Security researchers analysing the sophisticated 'Flame' malware were amazed at its extraordinary spying capabilities. Even though its creators had initiated the self-destruct command for the malware, the psychological impact it has left industrial giants and even governments are long-lasting"

Introduction

The harsh reality of cyber espionage surfaced again when the 'Flame' malware was discovered recently by security researchers. The advanced persistent threat (APT), which targeted computers in Middle East countries, was described by security experts as a highly sophisticated cyber-weapon. Flame, unlike most other malware, was neither designed to disrupt nor damage computers and network infrastructure, nor was it meant to phish out banking details. The sole purpose of the malware was to stealthily siphon out industrial design files (AutoCAD documents), PDF documents, and emails from affected computers. Furthermore, Flame's creators had designed the multi-module malware to be capable of sniffing networks, taking screenshots, logging keystrokes and recording conversations. In addition, the malware could use the infected computer's Bluetooth capabilities to connect to other discoverable Bluetooth devices like mobile phones to steal contact information. This gamut of intelligence seeking functions convinced security researchers analysing the malware to believe that Flame is the complete attack toolkit designed for cyber espionage.

Now that the malware has been discovered, however, Flame's creators have issued a self-destruct command to remove all its traces from affected computers. The self-destruct mechanism removes all modules of the malware and overwrites the disk with random characters to prevent researchers from studying the malware files. Even antivirus and security companies have updated their solutions to detect the Flame malware now. The plug is being pulled on Flame, however, it does not imply that businesses and even governments should not take any note of this. There could be similar undetected small programmes lying in their networks that are quietly transmitting data and information to their rivals.

Protecting against Flame and other APT Attacks

Now that antivirus solutions can detect and remove traces of Flame, it is no longer a serious threat for companies with updated security solutions. The real danger stems from hackers and cybercriminals who can learn from this cyber-espionage episode and develop stealthy malware that could take corporate spying to a whole new level. Businesses can safeguard themselves from APT attacks by practicing the so-called holy trinity of security:

1. **Educate Users and Keep Security Policies Relevant**
   Users are generally considered the

weakest link of the chain by attackers, and are often the target of initial infections. Companies need to educate them on APT infection vectors and social engineering techniques. And, as that won't guarantee that employees will never open an infected document, IT managers should make sure each user only has the access rights that he/she needs and no more.

2. **Maintain Up-to-Date Systems**
   The latest security patches must be applied. IT-wide signature maintenance, typically obtained through a security services provider, includes making the zero-day window as short as possible to reduce vulnerabilities and operational risks.

3. **Adopt "Intelligently Redundant" Security Strategy**
   Enterprises need to take a multi-disciplinary and consolidated approach to secure all IT assets. Antivirus and intrusion prevention capabilities are essential but firms should consider data loss prevention (DLP) technologies too, and look at the big picture when it comes to the threat landscape. True mitigation results in a blend of policies and protection against the full threat spectrum. Antispam, Web filtering and application control all carry out their part to block APTs during different stages of attacks. The rule of thumb is that no single security layer is fool proof, and integrating them intelligently helps ward off multi-vector threats.

Here are the layers that enterprises must have:

- **Effective protection against multiple attack vectors**
  This involves having security infrastructure that provides protection at a number of levels and vectors, and should include emails, instant messaging systems, Web exploits, applications, malware and botnets.
- **Robust in-depth asset hardening**
  This should cover networks, Web applications, data/databases, laptops and servers. The impact of zero-day attacks are best minimised by a combination of keeping patching windows as short as possible, hardening all such assets through robust configuration management based on best practices (e.g. 'least privileges'), and judicious deployment of two-factor authentication to critical services.
- **Application control**
  This enables enterprises to exercise risk/threat-based application channels, peer-to-peer and botnet controls. Employees will be able to safely access social networking platforms like Facebook, LinkedIn and Twitter. Botnet control is particularly important since most modern threats rely on an egress communication channel – blocking communication effectively mitigates many of these threats.
- **Monitoring**
  This includes infrastructure-wide monitoring to rapidly respond to any real or potential attacks, as well as up-to-the-minute threat signatures on applications, networks, data and DLP. There are far too many documented cases of threats laying resident on systems and eventually creating millions of dollars in damages simply because they were allowed to live for months and, in some cases, year.

APTs are continuing to surface. Flame is just the latest incident following Ghostnet, Operation Aurora and Stuxnet. It is high time for CIOs to assess their exposure to APTs and start taking preventive and remedial measures to stop espionage attacks that may be catastrophic to their businesses. ■

Fortinet is a leading provider of network security appliances and the worldwide leader in Unified Threat Management or UTM. Fortinet integrates multiple levels of security protection (such as firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam) to help customers protect against network and content level threats.

Kriptografi di Sekeliling Kita

BY | Abdul Alif Bin Zakaria dan Liyana Chew Binti Nizam Chew

Introduction

Kriptografi kini bukanlah hanya digunakan oleh perisik sahaja. Malah ia digunakan di mana-mana sahaja di sekeliling kita tanpa disedari. Ia adalah mekanisme yang digunakan untuk menyembunyikan maklumat rahsia, memberi pengesahan kepada pengguna yang sah bagi mengelakkan pindaan maklumat yang tidak dapat dikesan dan mencegah penggunaan rangkaian tanpa kebenaran oleh penceroboh. Boleh dikatakan hampir setiap individu di Malaysia adalah pengguna peranti yang menggunakan kriptografi. Lebih maju teknologi berkembang, lebih banyaklah peranti yang akan dihasilkan menggunakan kriptografi sebagai agen keselamatan maklumat. Artikel ini akan menerangkan sedikit sebanyak konsep kriptografi yang digunakan di dalam peranti yang kita gunakan hampir setiap hari tanpa disedari. Diharapkan informasi yang terdapat di dalam artikel ini dapat membantu pengguna agar lebih berwaspada dalam menggunakan peranti tersebut dan menjaganya sebaik mungkin supaya musuh tidak akan berpeluang untuk menceroboh maklumat peribadi kita.

MyKAD

MyKad yang juga bertindak sebagai kad pengenalan warganegara Malaysia, menggunakan teknologi cip yang mempunyai ciri-ciri keselamatan yang tinggi. Cip yang digunakan telah diuji kualiti ketahanannya di Institut Penyelidikan Industri dan Standard Malaysia (SIRIM). Kegunaan cip tersebut adalah untuk menyimpan data pemegang MyKad yang sah. Pada tahun 2012, kapasiti MyKad telah ditingkatkan daripada 64kb kepada 80kb membolehkan lebih banyak data dapat disimpan. Teknologi cip pada MyKad menggunakan pengesahan menggunakan kekunci simetri kriptografi dan melalui proses penyulitan (encryption) untuk melindungi data sistem operasi pelbagai lapisan dengan firewall serta landasan cip yang selamat. MyKad menggunakan dua jenis teknologi biometric bagi tujuan pengenalan diri iaitu gambar berwarna pemegang kad dan Sijil Digital (Digital Certificate) untuk pengesahan diri. MyKad ini juga mempunyai ghost image yang menggunakan teknologi turisan laser pada permukaan kad bagi mengelakkan pemalsuan.

Aplikasi Prasarana Kekunci Awam (Public Key Infrastructure) memuatkan Sijil Digital dan Kekunci Persendirian (Private Key) di dalam MyKad. Sijil Digital ini membolehkan empat transaksi berikut dilakukan secara elektronik. Pengesahan; orang lain tidak boleh menyamar sebagai anda. Pembuktian; tandatangan digital sebagai bukti sah transaksi. Sulit; maklumat sulit boleh dienkrip sebagai sulit. Integriti; tiada pihak ketiga boleh mengubah sebarang maklumat.

Setiap rakyat Malaysia yang sah kerakyatannya mestilah mempunyai sekeping MyKad yang unik dimana ia tidak mungkin sama dengan mana-mana MyKad yang dimiliki oleh individu lain. Dengan adanya ciri-ciri keselamatan pada MyKad ini, sepatutnya tidak wujud masalah penduaan MyKad di Malaysia.

Figure 1 *MyKAD*

Kad ATM (Automated Teller Machine)

Kad ATM bank dicipta untuk menjalankan urusniaga perbankan seperti pengeluaran wang, pertanyaan baki, pemindahan wang, penukaran nombor PIN, dan lain-lain urusniaga. Penggunaan cip pada kad ATM menjadikannya satu sistem yang lebih terjamin berbanding sistem jalur magnetik yang digunakan sebelum ini dimana ia boleh menyimpan lebih banyak data.

Setiap kali menggunakan mesin ATM atau membeli produk dan servis atas talian (online), kita menghantar data dengan harapan data tersebut sampai dengan selamat tanpa dipintas oleh pihak ketiga. Jika perkara ini berlaku, sistem kewangan berisiko untuk digodam dan kerugian wang ringgit akan dialami.

Kad ATM bercip mempunyai sistem operasi tersendiri, memori, antara muka (interface) komunikasi dan ciri-ciri keselamatan. Kebolehannya untuk menyulitkan (encrypt) dan menyahsulitkan (decrypt) data pelanggan ketika urusniaga dijalankan menggunakan kriptografi merupakan aspek penting yang terdapat pada kad ATM. Manfaat penting kad ATM bercip adalah keupayaannya menyimpan data dalam cip pada kad dengan selamat dan keupayaan untuk menghantar dan menerima data kewangan yang sensitif dalam cara yang selamat.

Figure 2 *Kad ATM*

Siaran ASTRO

Lebih tiga juta penduduk di Malaysia adalah merupakan pengguna rangkaian Astro. Tahukah anda bahawa setiap pelanggan Astro adalah penguna kriptografi? Penggunaan kriptografi adalah terletak pada kad pintar Astro yang dimasukkan kedalam slot yang terdapat pada dekoder Astro tersebut bagi menikmati siaran Astro yang dilanggan.

Untuk pengetahuan anda, setiap kad pintar Astro mempunyai master key dimana hanya pelanggan Astro yang sah dan pelanggan yang membayar yuran langganan sahaja yang dapat melayari Astro. Fungsi master key ini adalah untuk menjana sub key yang menyahsulitkan setiap paket yang dipancarkan melalui satelit setiap kurang dari sepuluh saat ke piring Astro pelanggan.

Jika master key tersebut adalah sah, maka setiap paket yang diterima akan dapat dinyahsulitkan dengan betul. Dengan itu, para pelanggan dapat menoton siaran yang diingini. Pihak Astro akan memperbaharui dari masa ke semasa master key semua pelanggan dan hanya pelanggan yang telah membuat pembayaran yuran langganan sahaja dapat terus menikmati pakej-pakej Astro yang dilanggani.

Figure 3 *Kad ASTRO*

Pasport Antarabangsa Malaysia

Sesiapa sahaja yang melintasi sempadan Malaysia memerlukan dokumen perjalanan yang sah. Maka kegunaan passport yang sah amatlah penting bagi merekodkan semua lintasan yang berlaku di sempadan negara. Pihak imigresen terpaksa mengetatkan prosedur untuk warga asing kerana unsur-unsur yang tidak diingini boleh memasuki negara kita dengan sewenang-wenangnya tanpa direkod.

Oleh itu satu sistem keselamatan telah diperkenalkan iaitu penggunaan RFID (Radio Frequency Identification Device) di dalam pasport antarabangsa Malaysia. RFID ialah penggunaan sistem tanpa wayar yang menggunakan medan elektromagnet frekuensi radio untuk memindahkan data dari tag yang dilampirkan kepada sesuatu objek. Ini bermakna tag berkenaan tidak perlu menggunakan kuasa bateri untuk beroperasi.

Kebiasaannya RFID digunakan untuk tujuan pengenalan automatik dan pengesanan. Penggunaan RFID bukan sahaja dapat meningkatkan tahap keselamatan dokumen perjalanan, tetapi ia juga boleh memudahkan dan mempercepatkan proses pemeriksaan imigresen. Dengan adanya RFID, Pegawai Imigresen bukan sahaja boleh mendapatkan semua data yang dikehendaki malah mereka akan dapat mengesan jika pemegang pasport mempunyai pasport yang tidak sah ataupun palsu.

Bagi membolehkan data diperoleh daripada pasport (tag), pembaca (reader) diperlukan untuk berinteraksi dengan tag. Dalam protokol ini, data rahsia tag tidak akan dihantar melalui saluran komunikasi yang tidak selamat antara tag dan reader. Reader akan memberi challenge kepada tag yang kemudian akan memberi tindak balas yang dikira menggunakan kunci kriptografi dan nilai rahsia. Jika tindak balas yang diberikan adalah betul, maka data akan dapat dibaca oleh reader. Protokol ini menggunakan kaedah kekunci simetri kriptografi ataupun public key cryptography. Tag yang menggunakan kriptografi biasanya melibatkan kos yang lebih tinggi berbanding tag yang tidak menggunakan kriptografi menyebabkan ia tidak digunakan secara meluas dan terhad. Tag yang menggunakan kriptografi juga dapat mencegah pengklonan tag.

Figure 4 *Pasport Antarabangsa Malaysia*

Cakera Padat

Cakera padat merupakan peranti yang sangat popular masa kini kerana ia digunakan secara meluas di seluruh dunia. Fungsinya yang pelbagai dan bentuknya yang praktikal menjadi pilihan pencipta perisian komputer, permainan video, penerbit filem dan muzik. Namun, dengan penggunaan cakera padat yang meluas, kegiatan cetak rompak dilakukan secara berleluasa. Justeru itu, satu penyelesaian telah diperkenalkan iaitu dengan menggunakan kunci product (product key) sebagai pembanteras gejala cetak rompak.

Kunci produk yang juga dikenali sebagai kunci perisian, adalah perisian berasaskan kunci untuk program komputer. Ia memperakui bahawa salinan program tersebut adalah asli. Pengaktifan kadangkala dilakukan di luar talian (offline) iaitu dengan memasukkan

kunci. Ada juga pengaktifan yang dilakukan di dalam talian (online) Proses pengaktifan ini diperlukan untuk mencegah pengguna lain menggunakan kunci yang sama. Tidak semua perisian mempunyai kunci produk. Ini adalah kerana pencipta perisian boleh memilih untuk menggunakan kaedah yang berbeza untuk melindungi hak cipta mereka. Dalam beberapa kes, seperti perisian sumber terbuka (open source software), perlindungan hak cipta tidak digunakan.

Figure 5 *Cakera Padat Permainan Video*

Permainan video menggunakan kunci produk untuk mengesahkan bahawa ia tidak disalin semula. Sebagai contoh, seseorang pengguna tidak dapat bermain permainan video seperti Fifa di dalam talian tanpa kunci produk yang asli dan unik.

Pengguna juga tidak dibenarkan untuk bermain dalam talian dengan dua kunci produk yang serupa pada masa yang sama. Kunci produk terdiri daripada satu siri nombor dan huruf. Ia biasanya dimasukkan oleh pengguna semasa pertama kali menggunakan perisian komputer tersebut. Kunci produk dimanipulasikan menggunakan algoritma matematik secara kriptografi dan cuba untuk memadankan keputusan untuk satu nilai yang sah. Jika kunci produk yang dimasukkan itu betul, pengesahan akan diberikan dan pengguna dapat menggunakan perisian tersebut.

KOD BAR

Kod bar adalah kod optik yang boleh dibaca menggunakan peralatan khas. Ianya mewakili data yang berkaitan dengan objek yang dipasangkan dengan kod bar tersebut. Pada asalnya, kod bar mewakili data dengan mempelbagaikan lebar dan jarak garisan selari, dimana ia dirujuk sebagai linear atau satu dimensi (1D).

Kemudian penghasilan kod bar berkembang menjadi segi empat tepat, titik, heksagon dan lain-lain corak geometri dalam dua dimensi (2D). Walaupun kini sistem 2D menggunakan kod bar pelbagai simbol, secara amnya ianya masih dirujuk sebagai kod bar

Figure 6 *Kod Bar 1D dan 2D*

Kebiasaannya kod bar digunakan pada produk barangan yang dijual di pasaraya. Ini adalah untuk memudahkan juruwang menjalankan tugas ketika proses pembayaran oleh pelanggan. Dengan hanya satu klik pada pengimbas kod bar, harga dan nama produk dipaparkan pada skrin juruwang. Selain daripada memudahkah juruwang di sesebuah pasaraya, penggunaan kod bar ini dapat membantu pihak pengurusan memantau

jumlah produk yang telah dijual.

Dengan memantau penjualan produk tersebut, pihak pengurusan dapat membuat keputusan-keputusan lain seperti menambah tempahan ataupun memberhentikan penjualan sesuatu produk.

Pengimbas kod bar (scanner) digunakan untuk mengimbas kod bar tersebut. Data dihantar oleh rangkaian tanpa wayar (wireless) ataupun berwayar (wired) kepada pelayan web yang selamat (secure web server). Melalui kaedah kriptografi, pengesahan akan diberikan dan data akan dikembalikan kepada pengimbas oleh rangkaian tanpa wayar ataupun berwayar.

Untuk pengetahuan anda, data yang terdapat pada sesuatu kod bar sebenarnya dilindungi dengan penggunaan kriptografi. Ini adalah bertujuan untuk mengelakkan data tersebut diolah oleh pihak yang tidak bertanggungjawab. Sebagai contoh, sekiranya data ataupun harga sesuatu barang diubah sehingga menjadikan harganya terlalu muarah di sebuah pasaraya, ia mungkin akan menyebabkan kerugian besar kepada pasaraya berkenaan.

Kesimpulan

Sejak zaman dahulu lagi pemimpin-pemimpin dunia telah menggunakan sistem komunikasi secara “tersembunyi”. Apa yang dimaksudkan dengan “tersembunyi” dalam komunikasi secara selamat ialah dengan menggunakan kriptografi sebagai medium perantaraan. Dengan adanya kritografi, jika sesuatu maklumat dapat dipintas oleh musuh, mereka tidak mungkin dapat mengetahui atau membaca isi kandungan maklumat tersebut. Ini adalah kerana maklumat tersebut telah diubah atau diolah kedalam bentuk yang tidak boleh dibaca dengan mata kasar. Hanya penghantar maklumat dan penerima yang sepatutnya sahaja yang dapat mengetahui isi kandungan maklumat yang dihantar.

Walaubagaimanapun, setiap kod rahsia tetap dapat dibongkar dengan adanya kuasa komputer yang bertambah maju setiap hari seiring dengan kemajuan teknologi moden kini. Namun dengan adanya kriptografi, sekurang-kurang kita dapat mempertahankan sistem komunikasi daripada digodam oleh musuh. Justeru itu kita haruslah sentiasa mempertingkatkan tahap kesedaran kita tentang keselamatan informasi yang kini telah menjadi bahan bualan dunia agar kita bersedian menghadapi segala kemungkinan yang bakal berlaku. ■

Rujukan

1. *Kemantapan Keselamatan Perlindungan: Cabaran, Haluan Dan Isu*
2. *http://www.cgso.gov.my/~cgso/portal/index.php/ms/artikel/87-artikel-kemantapan-keselamatan-perlindungan.html*
3. *Security Code To Crackdown On Counterfeiting*
4. *http://www.wlp.com/security-brochure.pdf*
5. *MyKad - Kelebihan di Tangan Anda*
6. *http://www.jpn.gov.my/MyKad_Website/index.html*

Training Programs

CyberSecurity MALAYSIA

Professional Development Schedules in CyberSecurity Malaysia Calendar 2012

No.		Program Duration	Standard Fees (RM)	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Fundamental/Introduction															
1	Essentials Digital Forensics for Non-IT Background (for advocaters, majistrates, prosecutors, judges and any others)	2 days	1500		9-10										
2	Digital Forensics for First Responder	4 days	3200				3-6								
3	Malaysia Common Criteria (MyCC 1.0) - Understanding Security Target, Protection Profile & Supporting	1 day	790		20					23					
4	Introduction to ISO 27001 & ISO 27002:2005 Information Security Management System	1 day	650	9	10	5	6		11	9	6	3	8	5	10
5	Business Continuity Management for Essentials	1 day	1000		20		23		25			24			
6	Data Encryption for Beginners	1 day	790						4					19	
7	Cryptography for Beginners	1 day	890					21				10			
8	CSM Security Essential Training	2 days	1590		27-28			7-8						5-6	
9	Google-Fu Power Search Technique	2 days	1400			5-6				9-10					
10	Wireless Security	2 days	1350					9-10						7-8	
11	Forensics on Internet Application	1 day	900											20	
12	Customize Training Package for groups and companies (Fundamental Courses Item 1-12)	1-5 days	Negotiable												
Intermediate															
1	Malaysia Common Criteria (MyCC 2.0) - Foundation Evaluator Training	3 days	3290		21-23					24-26					
2	Incident Response & Handling for Computer Security & Incident Response Team (CSIRTS)	3 days	3590					14-16					31(Oct)-2(Nov)		
3	Cryptography for Information Security Professional	3 days	3590					22-24				11-13			
4	ISO 27001 Implementation	3 days	3200	10-12	13-15	6-8	23-25	8-10	12-14	10-12	7-9	4-6	9-10	6-8	11-13
5	Google-Fu Googling to the Max	2 days	1600			7-8				11-12					
6	Incident Handling and Network Security Training Workshop (IHNS)	3 days	3590			26-28						3-5			
7	Digital Forensics on Data Recovery	2 days	1800									24-25			
8	Network Security Assessment Training NEW!	2 days	1300											27-28	
9	Server and Desktop Security Assessment Training NEW!	2 days	1300							17-18	14-15	11-12	16-17	13-14	11-12
10	Web Application Security Assessment Training NEW!	1 day	750									11		13	
11	Customize Training Package for groups and companies (Intermdiate Courses Item 1-8)	1-5 days	Negotiable												
Specialization/Specific Domains															
1	Risk Management NEW!	2 days	1800									19-20			
2	Business Impact Analysis NEW!	2 days	1800									24-25			
3	ISMS Internal Auditor Course (ISO 27001) NEW!	3 days	2850		20-22	12-14	3-5	21-23	19-21	17-19	14-16	18-20	16-18	20-22	18-20
Professional Certification															
1	Certified Information System Security Professional (CISSP) CBK Review Seminar	5 days	4705				16-20						1-5		
2	System Security Certified Practitioner (SSCP) CBK Review Seminar	5 days	4372				23-27						8-12		
3	Certified Secure System Lifecycle Professional (CSSLP)	5 days	4180				7-11						15-19		
4	SEC504: Hacker Techniques, Exploits & Incident Handling	6 days	USD4400						18-23						
5	Digital Forensics Investigation & Analysis	4 days	3850							16-20					
6	Business Continuity Management Professional Certification (BCLE2000)	5 days	8900			5-9		7-11		9-13			1-5		3-7
7	Professional in Critical Information Infrastructure Protection	3 Weeks	USD6000											19(Nov)-7(Dec)	
8	Cyber Warrior	5 days	4850			19-23			18-22						17-21
9	Cyber Defender	5 days	4890			12-16			11-15						3-7
10	ISO 27001 Lead Auditor (External Auditors)	5 days	5000						25-29	16-20			15-19	26-30	17-21
Examination															
1	CISSP Examination	6 hrs	USD599		25			12							
2	SSCP Examination	6 hrs	USD300		25			12							
3	Certified Forensics Investigation Analyst (CFIA)		580												
4	Kryterion Test Center			19		29	13	17		13		26		27	
5	Cyber Warrior - Operation D-Day (fully hands on examination)	1 day	1200			26			25						28

*Subject to change

Venue

CyberSecurity Malaysia, Training Centre, Level 4, Block C, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia. | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0844 (ISPD)

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

MS ISO/IEC 17025 TESTING SAMM NO. 456 (MySEF LABORATORY)

MSC MALAYSIA Status Company

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

As interesting as this video claims to be,
you are actually being tricked into downloading a malware.

Be smart. Be safe

www.CyberSAFE.my

Corporate Office:
CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan | Tel: +603 - 8946 0999 | Fax: +603 - 8946 0888
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my