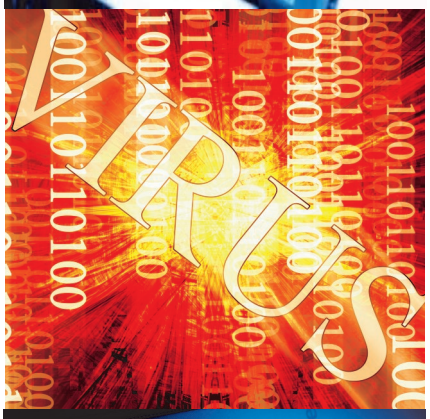
CERT-MU eSecurity Newsletter

2014 Top Security Breaches & Emerging Threats of 2015

Volume 4| Issue 4 | March 2015

NCB

CERT-MU



CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

Your Partner in Cyber Security

www.cert-mu.org.mu

CERT-MU SERVICES

Reactive Services:

* Incident Handling
* Vulnerability Scanning and Penetration Testing

Proactive Services:

* Dissemination of Information Security News, including virus alerts, advisories, vulnerability notes and warnings on latest cyber-attacks
* Awareness campaigns on different Information Security themes for corporates, youngsters and the public in general
* Organisation of international events such as Safer Internet Day and Computer Security Day
* Organization of professional trainings on Information Security areas
* Provision of educational materials through publications (includes guidelines, e-security newsletters, brochures, booklets, flyers) and a dedicated cyber security portal

Security Quality Management Services:

* Assistance to organisations for the implementation of Information Security Management System (ISMS) based on ISO 27001
* To conduct third party information security audits
* To carry out technical security assessment of ICT infrastructure of organisations

Cyber Security Portal

The Cyber Security Portal is an initiative of CERT-MU to sensitise and raise awareness of the general public on the technological and social issues facing Internet users (Organisations, Parents, Home-Users and Kids).

The Portal consists of Internet best practices for:

* Organisations
* Parents
* Kids
* Home users

More information is available on:
www.cybersecurity.ncb.mu

INSIDE THIS ISSUE:-

Dear Readers,

Greetings from CERT-MU

The year 2014 has seen significant developments in the cybersecurity and IT industry. At the same time, a full spectrum of cyber threats hit local and global headlines – from application vulnerabilities such as the Heartbleed, Shellshock/Bash, data breaches, phishing scams, malicious software, mobile threats, government sponsored attacks, incidents involving social networking and to worldwide cyberattacks by hacktivists. All indications are that the year 2015 will bring more of the same, with the struggle between those wishing to create new threats and exploit vulnerabilities and those looking to protect against them likely to intensify. Advancements in the Internet of Things also means consumers will have increased connectivity across their devices, gadgets and machines and with this connectivity comes the potential for a whole new range of security risks.

In this eSecurity Newsletter, the top security breaches of 2014 have been highlighted. As 2015 is expected to be an exciting year for the Information Security community, the emerging threats for 2015 are also discussed.

We trust that you will find the articles interesting and enjoy reading.

2014 Top Security Breaches

Over the last year, information and technology have become more tightly intertwined in our lives. The ubiquity of mobile devices has increased citizens' reliance on cloud services to store personal and business data, making them more productive but at the same time, more vulnerable. While phones and tablets have become the most common devices to connect to the Internet, interconnected devices, the so-called Internet of Things promise to deliver greater control and understanding over our lives, but at the same time raise privacy concerns. As technology keeps changing at an outstanding rate, threats are also evolving fast, with cyber criminals finding new and creative ways to exploit users and technology all the time. In 2014, it seemed that no industry went unscathed as the data breaches were broad and deep. The world witnessed a series of high-profile security breaches such as the Target and Home Depot fiascos, and then there was the massive breach at JP Morgan Chase, which compromised personal information of more than 83 million households and businesses, and finally over 100 terabytes of internal files and films recently stolen from Sony. In addition to large retailers, media companies and financial institutions, technology companies like eBay and Snapchat were hacked, too, and so were government organizations and healthcare institutions. This year, massive Internet infrastructure vulnerabilities were discovered, including Shellshock, Heartbleed and POODLE. These publicized events are only a fraction of the overall exposure to losses emanating from cyber incidents, which in 2014 is estimated to be hundreds of billions of dollars. Hence by knowing how threats have worked in 2014, organisations will be in a better position to strengthen their IT infrastructure and develop specific action plans to tighten their defenses. The top security breaches of 2014 are discussed below and a prediction for 2015 are also given.

DATA BREACHES:

JPMorgan Chase breach affected 83 million customers

In October 2014, JPMorgan Chase, the largest bank in the United States became victim to a cyberattack. Names, addresses, phone numbers and email addresses were compromised. 76 million households and 7 million small businesses were affected as stated by the bank. In addition to customer information, the attack also compromised internal Chase data used in connection with providing or offering services, such as the Chase line of business the user is affiliated with. The bank did not provide many other details about the attack, but said its customers who used its online or mobile services on Chase.com, JPMorgan Online, Chase Mobile or JPMorgan Mobile were affected.

Home Depot Data Breach

Home Depot, an American Retailer suffered from a data breach in which 56 million customer debit and credit cards were put at risk after hackers broke into the company's payment systems. The investigations revealed that hackers escaped detection by using custom-made malware that had never been seen before. The malware used was not detected by anti-virus software. Home Depot said the malware that stole the credit card data resided on its computer systems from April until September 2014. Attackers stole 56 million payment card details and collected 53 million email addresses of people who shopped at Home Depot's stores between April and September in the U.S. and Canada. They gained access to American retailer's network by using the login credentials of one of the retailer's vendors.

EBay Hacked

In May 2014, eBay faced a data breach whereby the customers were exposed to malware due to a flaw on eBay's website. Clicking some listing on eBay immediately redirected to a malicious sites. EBay removed some listings but described the vulnerability

as "an isolated incident. Multiple vulnerabilities existed on the website of Ebay and it has been criticized by security experts for not responding to these vulnerabilities quickly enough as the underlying vulnerability remains, even though individual links have been removed. Hackers accessed the website using cross-site scripting though Javascript.

Community Health Systems breach impacted more than 4 million patients

The major Community Health Systems (CHS) breach impacted

more than 4 million patients started with the exploit of a VPN device, which was vulnerable to the notorious Heartbleed bug. According to the Security Consultant of the organisation, attackers targeted a VPN concentrator device manufactured by Juniper Networks. After leveraging the Heartbleed flaw, attackers were able to obtain VPN credentials stored in memory on the CHS Juniper device. The attack happened soon after word spread of the pervasive Heartbleed bug in early April 2014 – which essentially allows attackers to read protected pieces of memory that could contain sensitive information. In this case, the obtained information led the hackers to database containing names, addresses, birth dates, phone numbers and social security numbers.

Credit Card Details of 20 Million South Koreans Stolen

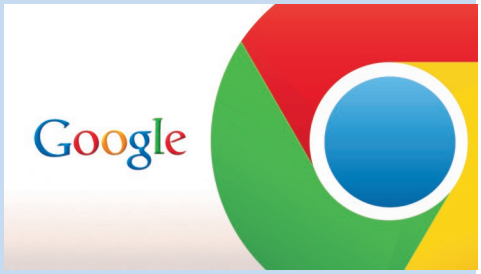
In January 2014, the credit card details from almost half of all South Koreans have been stolen and sold to marketing firms as per BBC World News. The data was stolen by a computer contractor working for a company called the Korea Credit Bureau that produces credit scores. The names, social security numbers and credit card details of 20 million South Koreans were copied by the IT worker. The scale of the theft became apparent after the contractor at the centre of the breach was arrested. Managers at the marketing firms which allegedly bought the data were also arrested. Early reports suggest that the contractor got hold of the giant trove of data thanks to the access Korea Credit Bureau enjoys to databases run by three big South Korean credit card firms. The contractor stole the data by copying it to a USB stick.

Data breach affects 16 Million Users in Germany

A data breach affecting 16 million German internet users was discovered in January 2014 by the country's Federal Office for Information Security (BSI). The agency was informed of the millions of compromised online accounts by law enforcement and research institutions that were analyzing botnets. In addition to infecting users' computers with malware, hackers stole passwords and usernames tied to email addresses and social media accounts, as well as on some online shopping portals. According to a report by Associated Press, a spokesman for BSI stated that the majority of users appear to be in Germany because half of the accounts have ***".de"*** domain-name endings. The agency set up a web page where individuals can check to see if they have been impacted by the breach.

5 million 'compromised' Google accounts leaked

In September 2014, a database of some 5 million login and password pairs for Google accounts were leaked to a Russian cyber security Internet forum. The text file containing the alleged compromised accounts data was published on the Bitcoin Security board. It listed 4.93 million entries, although the forum administration has since purged passwords from it, leaving only the logins. The accounts were mostly those of Google users and gave access to Gmail mail service, G+ social network and other products of the US-based Internet giant. The forum user "tvskit", who published the file, claimed that 60 percent of the passwords were valid, with some users confirming that they found their data in the base as per the reports of CNews, a popular Russian IT news website.



Apple iCloud Accounts of Celebrities Hacked

In September 2014, hackers accessed celebrities' iCloud accounts through targeted attacks on usernames, passwords, and security questions. This resulted in the leak of celebrity's intimate pictures. The images seemed to have been acquired from Apple's iCloud. This leak has raised questions to the security of iCloud. Apple has issued a statement that certain celebrity iCloud accounts were compromised. However, upon investigation of the breaches, Apple stated that no compromise was found in any Apple's systems including iCloud or Find my iPhone. Several theories were put forward. For example, the celebrities may have been hacked while connecting to an open public Wi-Fi network. If the celebrities accessed their personal accounts, attackers connected to that network might have been able to intercept and capture the username and password credentials.

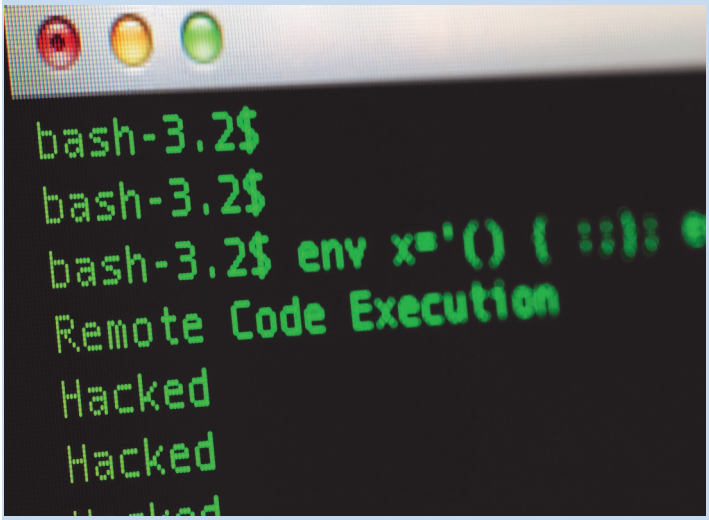
APPLICATIONS AND WEB SECURITY:

Heartbleed Bug

In April 2014, security researchers discovered a major security flaw that has been exposing users' personal information and passwords to hackers for the past two years. According to experts, it was one of the biggest security issues to have faced the Internet to date. This critical vulnerability was present in a piece of open source software called OpenSSL, which is designed to encrypt communications between a user's computer and a web server. The bug existed in a piece of open source software called OpenSSL, one of the most widely used encryption tool and is designed to encrypt communications between a user's computer and a web server, a sort of secret handshake at the beginning of a secure conversation. The bug dubbed as "Heartbleed" was regarded as one of the most critical vulnerability in the OpenSSL cryptographic software library. This OpenSSL cryptographic library affected around 17% of SSL web servers which use certificates issued by trusted certificate authorities. The exploitation of the Heartbleed bug led to several data breaches. For example, Canada's tax authority and a popular British parenting website reportedly suffered from user data loss whereby the social insurance numbers of approximately 900 taxpayers were removed from the system.

Shellshock / Bash Vulnerability

In September 2014, a critical vulnerability known as the "Shellshock bug" was identified in GNU's bash shell, which allowed remote attackers to run remote commands on vulnerable systems. The Shellshock flaw affected the Bash shell used across



many UNIX-based systems including Mac OS X and variants of Linux. Successful exploitation of the Shellshock vulnerability allowed attackers to insert malicious pieces of code from a remote location and get full system control of the vulnerable system. Because of Bash's ubiquitous status amongst Linux, BSD, and Mac OS X distributions, many computers were vulnerable to Shellshock - all unpatched Bash versions between 1.14 through 4.3 were at risk. This vulnerability was regarded as critical, since Bash is widely used in Linux and UNIX operating systems running on Internet-connected computers, such as Web servers. BASH is the default command-line shell processor that is often run in a text window on Linux and UNIX systems. It also allowed users to type commands that cause actions and has the ability to read commands from a scripted file.

Poodle Vulnerability

After the Heartbleed bug and the Shellshock vulnerabilities, another critical vulnerability made its apparition in October 2014. The vulnerability known as "POODLE" (Padding Oracle On Downgraded Legacy Encryption) was exploited to steal data and is similar to the BEAST attack. The vulnerability affected SSL version 3.0. While this is an obsolete and insecure protocol and was replaced by its successors, many TLS implementations remained backwards-compatible with SSL 3.0 to interoperate with legacy systems for a smooth user experience. The vulnerability allowed a network attacker to extract the plaintext of targeted parts of an SSL connection, usually cookie data. Unlike the BEAST attack, this vulnerability does not require such extensive control of the format of the plaintext.

MALWARE AND SCAMS:

Yahoo Malvertising Attack Linked to Larger Malware Scheme

European users were served with malicious advertisements between December 31, 2013 and 03rd January 2014. The malvertising attack infected Yahoo users and directed them to other websites that tried to install malicious software on their computers. According to Yahoo, this ad-related malware have affected more than 2 million PCs and compromised Yahoo users' personal data. The company further stated that some people outside Europe have also been hit. IT firm Cisco discovered that victims landed on websites that have been used in other on-going cyber-attacks. The analysis of the attack indicated that the domains that victims were redirected to, matched a pattern.

Poisoned YouTube ads serve Caphaw banking Trojan

In February 2014, malicious advertisements were discovered on YouTube. According to security researchers, YouTube's ad network was compromised to host the Styx exploit kit. Styx is an attack toolkit that allows the remote attacker to perform various malicious actions on the compromised computer. The Styx exploit kit is attached with the Caphaw banking Trojan and spreads the malware by taking advantage of a Java vulnerability. The Caphaw malware that infected YouTube visitors is a variant of banking Trojan Shylock, and was previously used in a campaign which targeted customers of 24 banks around the world. In that campaign, Caphaw was also believed to have been delivered as part of a crimeware kit that exploited vulnerable versions of Java. In this scenario, the malware tried to detect the version of Java installed and based on the version, it sent out different URLs to ensure that the exploit is compatible with Java versions. Google has confirmed that a rogue advertiser was behind this malvertisment.

"Windigo" Operation infected 25,000 servers to bolster spam, malware campaign

In March 2014, cyber criminals compromised thousands of UNIX and Linux servers by using a backdoor Trojan and sustain a far reaching spam and malware campaign. Dubbed as "Operation Windigo", more than 25,000 servers around in the world have been infected during the last two years. In collaboration with Germany's CERT-Bund, the Swedish National Infrastructure for Computing, the European Organization for Nuclear Research (CERN), and other organizations that formed an international working group, ESET figured out Windigo's complex attack cycle. According to security experts, an OpenSSH backdoor, dubbed Linux/Ebury stole administrators' credentials ultimately gives Windigo attackers the ability to redirect end users to malicious content or spam their actions with messages. Among the servers in 110 countries that have been impacted by Operation Windigo, the majority are in the United States, Germany, France, Italy and the U.K. It was also estimated that currently more than 10,000 servers were infected worldwide and Windigo is responsible for sending around 35 million spam messages a day to end users.

24,000 computers worldwide infected by Middle Eastern malware

Security experts discovered a remote access tool (RAT) that infected 24,000 computers worldwide in March 2014. Dubbed as "njRAT", the malware shared similar functions as other RATs, but its most unique attribute stems from its regional usage. The RAT was developed by Arabic speakers and was capable of downloading additional malware, log keystrokes, compromise webcams, and can control botnets. The malware was primarily used by attackers in the Middle East and spreads via "infected USB keys or networked drives. 80 percent of the command and control servers tied to the malware are located in Middle East regions. While a majority of the usage is geared toward typical cyber-criminal motives, experts at Symantec observed the malware infected the networks of governments and political activists.

"Nemanja" POS malware compromises 1,500 devices and half a million payment cards, worldwide

In May 2014, about half a million of payment cards used in hotels, grocery stores and other businesses around the world have been compromised by a malware known as "Nemanja". This piece of malware infected nearly 1500 point-of-sales (POS) devices around the world. The massive worldwide Nemanja botnet was discovered in March by cyber intelligence company IntelCrawler and includes more than 1,478 hosts in more than 35 countries across the world, including the U.S., UK, Canada, Australia, China, Japan, Israel and Italy, as well as other developing countries. The botnet is the work of a single group of cyber crooks believed to be located in Serbia, According to security researchers; it is one of those cases where a group of hackers developed their own malware for targeted attacks with a very clear commercialization scheme. Cybercriminals intercept credit cards from the infected POS devices and then sold the data on black market through their own shops and partners.

Spammers exploited Malaysian Airline MH17 Crash

The air crash of Malaysian Airline MH17 was exploited extensively by scammers in July 2014. The disaster is being used to spread objectionable links on the Internet. A link to a pornographic website disguised as a video of the Malaysia Airlines crash was posted on a Facebook page dedicated to one victim. Many tweets that were posted appeared to report the disaster, but actually included spam links. The perpetrators used software that could detect what was being posted regularly and reposted using the same hashtags. A Facebook community page dedicated to Liam Sweeney, one of the 298 people victims, used his name and picture. Its sole post is a link entitled: *"Video Camera Caught the moment plane MH17 Crash over Ukraine"*. However, the link redirected users to pornographic sites. Moreover, anyone who clicked on the links was asked to call a phone number in order to verify that they are aged 18 or older. Various tweets with spam links were also circulating on Twitter regarding the MH17 crash.

Qbot Botnet Sniffs 800,000 Banking Transactions from More than 500,000 Systems

The Qbot botnet infected more than half a million computers in October 2014 and was used predominantly for intercepting online banking sessions with five largest banks in the US. Once a system was infected, multiple pieces of malware were delivered. The operators of the infected computers were believed to belong to a Russian cybercrime group and most of the Qbot victims are located in the US. The cybercriminals managed to intercept the connection in the case of 800,000 encrypted online banking transactions, 59% of them related to undisclosed financial institutions in the United States. Other countries with an increased number of infections included Great Britain, Canada and Italy. Most of the victims run Windows XP (52%), but a large chunk of the total (39%) use the popular Windows 7.

New Variant of the Turla Malware Detected Targeted at Linux Systems

In December 2014, security experts discovered a new variant of the Turla malware dubbed as "Penquin Turla" that was designed to hit Linux systems. The investigation started after a new strain of malware was uploaded to a multi-scanner service. The malware was a previously unknown piece of a government malware, Turla, considered by the security experts as one of the most complex APTs in the history. Turla was detected for the first time by researchers who believe that the malware was developed by Russian cyber specialists, probably all these instances are part of a cyber-weapon program of the Government of Moscow. The security experts at BAE Systems Applied Intelligence who discovered the Snake campaign have linked the platform to the Uroburos rootkit, which is another malware used for cyber espionage.

The 2014 Mauritian Threat Landscape

The high Internet usage in businesses and households has brought huge benefits to Mauritius, but at the same time, is making our country more vulnerable to cyber threats. The threat from cybercrime is constantly evolving, with new opportunities to commit old crimes in new ways as well as high-tech crimes . Mauritius like other countries across the world is becoming victim to a number of cyber threats, whether for financial gain, or threats to children and the effect on the victims can be devastating.

During the past three years, new types of security threats have emerged in Mauritius such as electronic frauds, phishing and sextortion, amongst others. CERT-MU has noted a considerable increase in the number of incidents reported as compared to the previous years. The chart for reported incidents at CERT-MU for the year 2014 are shown below:

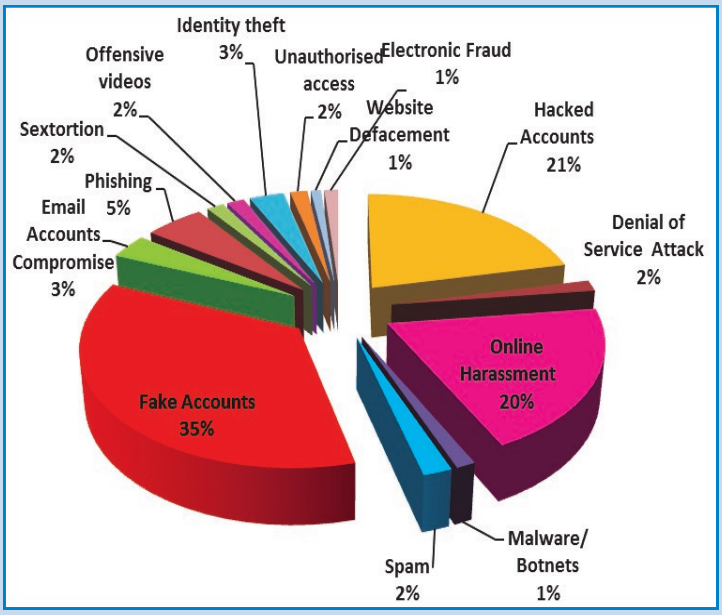
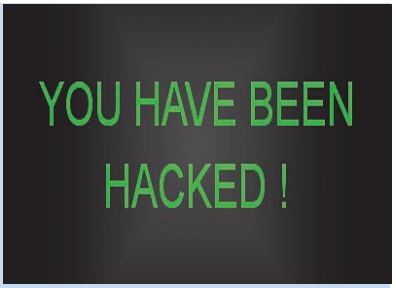


Figure 1

From the chart below, it can be found that 35% of the incidents reported consisted of fake Accounts. Fake accounts with stolen identities are created on social networking sites like Facebook, Twitter and Google+. Pictures of victims are stolen and posted on these fake accounts without their authorization. These profiles are used to carry out impersonation, post derogatory remarks, and communicate on behalf of the victim.



Another type of incident includes hacked accounts with 21% reported in 2014. Social network accounts are created with weak passwords, which make them vulnerable to attacks. Intruders can easily get into the accounts, change the passwords and take control of it. These hacked accounts are often misused to carry out illegal activities.

20% of incidents reported were based on online harassment, from mild to severe in 2014. Internet users experience online harassment mostly through social networking sites. The victims of online harassment include adults and teenagers. Victims are often bombarded by violent, personalized imagery and numerous disturbing comments. The addresses of their homes and workplaces may be publicized, along with threats of violence. Such online harassment can escalate to offline stalking, physical assault, and more.

Phishing attacks against financial institutions have also been on the rise. Fake emails have been created and circulated on behalf of banking institutions in Mauritius. Users were asked to click on a link where they are redirected to the phishing website. Once there, they are prompted to submit details such as user id and password for their Internet Banking Account. They are then redirected to the authentic website of the bank. Several financial institutions in Mauritius are falling prey to phishing attacks.

Sextortion is a new trend and is increasing considerably in Mauritius. Online predators are using fake profiles as their identity to chat and lure the victims on social networking sites. After gaining the trust and confidence of victims, they convince them to engage in video calls on Skype. They are eventually persuaded to perform indecent acts through webcams. These videos and images are captured and recorded by the online predators and are used to harass and blackmail them morally as well as for financial gains. It has been noted that in some cases that when victims refuse to act in favour of the online predators, their pictures posted on their social networking profiles are stolen and morphed to make them appear obscene and then used to blackmail them.

Other threats noted for 2014 include website defacements, malicious programs, and electronic frauds amongst others.

Emerging Threats of 2015

As 2014 reached to its end, security experts have started to make predictions about what web users, organisations and security professionals will expect to see in 2015. The emerging threats for 2015 are discussed below:

Old Code, New (Dangerous) Vulnerabilities

Recent allegations of deliberate tampering and accidental failures in crypto implementations and critical vulnerabilities in essential software (Shellshock, Heartbleed, OpenSSL) have left the community suspicious of unaudited software. The reaction has been to either launch independent audits of key software or have security researchers poke them in search of critical vulnerabilities (tantamount to unofficial audit). This means that 2015 will be another year of new, dangerous vulnerabilities appearing in old code, exposing the Internet infrastructure to menacing attacks.

Attacks on the Internet of Things (IoT) will focus on smart home automation

With the increasing popularity of smart home automation, it is expected that commoditized "plug and play" consumer devices such as CCTV cameras and remote access controls for alarms, lighting and climate control will be exploited by cybercriminals. While these devices continue to become more prevalent, not many of the devices are deployed with Internet Security in mind. These devices tend to have limited memory and system resources and do not have the computing power of a typical desktop. Obviously there is a search engine that allows people to do an online search for Internet-enabled devices, ranging from security cameras, to cars, home heating systems and more. Although the search engine does not reveal vulnerabilities, it makes it easier for IoT devices to be found, which cybercriminals can then target and exploit.

Escalation of ATM and POS Attacks

Attacks against cash machines (ATM) seemed to explode this year with several public incidents and a rush by law enforcement authorities globally to respond to this crisis. As most of these systems are running Windows XP and also suffer from frail physical security, they are incredibly vulnerable by default and, as the impersonal gatekeepers of the financial institutions' cash, cybercriminals are bound to come knocking here first. In 2015, it is expected to see further evolution of these ATM attacks with the use of APT techniques to gain access to the "brain" of cash machines. The next stage will see attackers compromising the networks of banks and using that level of access to manipulate ATM machines in real time.

Mobile devices will become even more attractive targets

Mobile devices will continue to become a target for cyber attackers especially when mobile devices store up a trove of personal and confidential information and are left switched on all the time, making them the perfect targets for attackers. Mobile devices will become even more valuable as mobile carriers and retail stores transition to mobile payments. For example, Apple Pay certainly addresses some of the weaknesses that have facilitated recent attacks on Point-of-Sale (PoS) systems. The wide adoption of

mobile devices with mobile penetration rate of 122% in Mauritius, including smartphones and tablets will also open up new avenues for attacks. Mobile apps are likely to be installed without proper verification and security defenses. It is estimated that attacks on mobile devices will make their apparition as new technologies expand the attack surface and app store abuse goes unchecked.

Privacy will continue to be sacrificed for mobile apps

Some mobile users will continue to trade their privacy in exchange for mobile apps. While many Internet users are reluctant to share banking and personal identifiable information online, others are willing to share information about their location, and mobile device battery life as well as allow access to photos, contact lists and fitness information, all in exchange for mobile apps. In addition, many consumers do not really know what they are agreeing to when downloading apps.

Scammers will continue to run profitable ransomware scams

This growth was largely due to the success of Ransomcrypt, commonly known as Cryptolocker. This particularly aggressive form of ransomware made up 55 percent of all ransomware in the month of October. The malware is designed to encrypt a user's files and request a ransom for the files to be unencrypted. Ransomware causes even more damage to businesses where not only the victims' files are encrypted but also files on shared or attached network drives. Holding encrypted files for ransom is not entirely new, but getting the ransom paid has previously proven problematic for the crooks. However, recently ransomware makers have started leveraging online and electronic payment systems such as Bitcoins, Webmoney, Ukash, greendot (MoneyPak) to get around this challenge. Cybercriminals like the relative anonymity and convenience of electronic payments and these are already available, putting businesses and consumers at greater risk from losing data, files or memories.

Distributed denial-of-service (DDoS) will continue to rise as a threat

Yet another trend seen in 2014 is the increase in Unix servers being compromised and their high bandwidth being used in DDoS attacks. The motivation of the attacker can vary widely, with hacktivism, profit, and disputes being the main reasons. Considering the ease of conducting large DDoS attacks, it is expected that the DDoS growth trend will continue in the future and 2015 will see the rise of DDOS attacks.

User behaviour will take centre stage as security moves beyond passwords

With the password system constantly under attack by cybercriminals, security vendors and providers are facing increasing challenges on ways to balance the need for convenience against complexity while providing users with the seamless experience that they demand. Adopting multi-factor authentication techniques such as one-time passwords or iris and fingerprint scanning may provide alternate safeguard methods, but at times they may not be the safest options. The true solution to protecting valuable information lies in users' behaviour, which is ultimately how we can prevent our personal online assets and identities from being compromised.

The Cloud will take us to Infinity and Beyond

In 2015, it is expected to see more and more data hosted in the cloud but as this move occurs, businesses will need to take a closer look at data governance and ensuring their data is cleaned before it is hosted in the cloud. Legacy data left unmanaged will continue to accumulate and present a persistent challenge for businesses. The cloud in 2015 represents an infinite amount of personal information being hosted remotely and debate around the right to access, control, and protect private data in the cloud will continue to escalate.

The front lines of cybersecurity will be strengthened by closer industry partnerships and collaborations

The fight against cybercrime cannot be won alone and the security industry together with telecommunication providers and governments from around the world are joining forces to beat the war on cybercrime. The security industry is one of few in the world that has a 'nemesis industry' constantly working against it to bring it down. That is why cybercrime needs to be tackled with a different approach. In 2015, while attackers will continue to look for new vulnerabilities, open source platforms will continue to address these vulnerabilities through greater industry coordination, collaboration and response. This represents a positive sign and it is expected that open source platforms can only get better in the future.

Mac Attacks: OSX Botnets

Despite efforts by Apple to lock down the Mac operating system, we continue to see malicious software being pushed via torrents and pirated software packages. The increasing popularity of Mac OS X devices is turning heads in the criminal world, making it more appealing to develop malware for this platform. The closed-by-default ecosystem makes it harder for this malware to successfully take hold of the platform, but there remains a subsection of users who will disable Mac OS X security measures – especially people who use pirated software. This means that those looking to hack OS X systems for a variety of reasons know that they simply need to bundle their malware with desirable software to enjoy widespread success. Due to widespread myths about the security of the OS X platform, these systems are also unlikely to have an antimalware solution installed that will flag the infection so once the malware is installed, so it is likely to go unnoticed for a very long time.

Phishing Attacks

The convenience and universal accessibility of electronic payment systems and online banking services attract huge numbers of users, and like many countries, financial institutions in Mauritius is promoting the use of Internet Banking. The dramatic growth in the number of users using Internet Banking has attracted cybercriminals, and they are investing ever-growing resources into fraud schemes with which they can first gain access to users' financial data and then to their actual money. Although financial attacks are among the most complicated and expensive types of attacks, they are also highly lucrative because, once successful, they provide direct access to the victims' money. Once an online banking account is accessed, all that remains is to take the money and cash it in. It is therefore expected that this type of attack will continue to increase in 2015.

Social networks will remain an easily exploitable surface

The use of Social networks amongst Mauritians, especially the youth, is growing extensively. Mauritians are using social networks as platforms to communicate, share their views and opinions as well as to post information about themselves. However, people are likely to "over-share" things, which can be exploited by other people. Online predators and cybercriminals always find ways to look for victims. Attacks on social networks can spread quickly because users are often sent links and offers to scams from people they trust. In 2015, it is expected that attacks on social networks will increase.

Sextortion – a growing menace

Cybercrimes involving online harassment and blackmailing also known as sextortion is rising in Mauritius. Cybercriminals have become quite savvy in their attempts to lure people and the growing use of chat rooms and social networks especially amongst youngsters will create more opportunities for such types of attacks to occur.

To prevent or minimize these threats, it is important to implement security measures within the organisations to achieve a good level of defense. This can be achieved by implementing the following:

1. Boundary firewalls and Internet gateways – basic protection related to connections to the Internet.
2. Secure configuration – essential security elements when installing and commissioning systems and networks, forming the bedrock of your security.
3. Access control and administrative privilege management – establishing basic controls for users to safely and securely access accounts.
4. Patch management – the very important ongoing update of systems to ensure that they will at least be resistant to well-known and widely prevalent attack vectors.
5. Malware protection – establishing a base level of protection against a range of malicious software such as viruses.

news FOCUS

The Superfish Flaw

Recently security researchers have discovered a software known as Superfish pre-installed in Lenovo laptops. The Superfish technology is meant to help users find and discover products visually and instantly by analysing images on the web and presenting identical and similar product offers that may have lower prices. But what it actually ends up doing is serving up unwanted adverts on existing web pages. This kind of software is called adware and represents a security risk. This is because the software includes a proxy - a component that intercepts network traffic outside your browser so that it can keep track of what users are doing. Thus, if Superfish software is installed, it will monitor the websites you visit, and its contents, it can keep its eye out for related sites, all based on images instead of relying on old-fashioned keywords. From October 2014 to December 2014, Lenovo shipped Superfish on a number of its consumer notebooks.

This security issue could also be exploited to conduct attacks. Superfish make use of a man-in-the-middle proxy component to interfere with encrypted HTTPS connections, undermining the trust between users and websites. It does this by installing its own root certificate in Windows and uses that certificate to re-sign SSL certificates presented by legitimate websites. Security researchers found two major issues with this implementation. Firstly, the software used the same root certificate on all systems and secondly, the private key corresponding to that certificate was embedded in the program and was easy to extract. With the key now public, malicious hackers can launch man-in-the-middle attacks via public Wi-Fi networks or compromised routers against users who have Superfish installed on their systems.

Superfish relied on a third-party component for the HTTPS interception functionality: an SDK (software development kit) called the SSL Decoder/Digestor made by an Israeli company called Komodia. Researchers have now found that the same SDK is integrated into other software programs, including parental control software from Komodia itself and other companies. And as expected, those programs intercept HTTPS traffic in the same way, using a root certificate whose private key can easily be extracted from their memory or code.

More information about the vulnerability is available on CERT-MU website: www.cert-mu.org.mu

PrivDog Security Issue

"Secure" Advertising Tool PrivDog Compromises HTTPS Security

New cases of insecure HTTPS traffic interception have been discovered as researchers probe software programs for implementations that could enable malicious attacks. The latest software to open a man-in-the-middle hole on users' PCs is a new version of PrivDog, an advertising product with ties to security vendor Comodo. PrivDog is marketed as a solution to protect users against malicious advertising without completely blocking ads. The program is designed to replace potentially bad ads with safer ones that are reviewed by a compliance team from a company called Adtrustmedia. However, the software also raises security risks. In order to replace ads on websites protected with HTTPS (HTTP with SSL/TLS encryption), PrivDog installs its own self-generated root certificate on the system and then runs as a man-in-the-middle proxy. When users access HTTPS sites, PrivDog hijacks their connections and replaces the legitimate certificates of those sites with new ones signed with the locally installed root certificate. Since the root certificate installed by PrivDog on computers is trusted by browsers, all certificates that chain back to it will also be trusted. This means that users will think that they are securely communicating to the websites they accessed, while in the background, PrivDog will decrypt and manipulate their traffic.

CERT-MU Events 2014

Safer Internet Day 2014

Safer Internet Day is an international event organised by Insafe in February each year to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people across the world. The theme for this year's Safer Internet Day was ***"Lets Create a Better Internet together"***. On this occasion, the National Computer Board organized a workshop targeting towards secondary school students, rectors and ICT teachers. A number of ongoing activities were conducted to celebrate the Safer Internet Day including a national level online quiz competition on Information Security for secondary school students. The objective of the quiz was to assess the understanding level of Internet security amongst students. The winners were awarded during the workshop. In addition, a guideline on ***"Internet Safety for youngsters"*** was also launched. Some 700 students attended the workshop.As a continuation of the SID, the National Computer Board, in collaboration with Ministry of Education and Human Resources have conducted awareness sessions on Internet Safety and Security in schools and colleges in the four zones of the country. Some 1400 students have been sensitized. In addition, this year, some 80 women have also been sensitized in women centres across the island on the issues of child online safety.

National Cybersecurity Strategy Validation Workshop

Cyber attacks are increasing and becoming more sophisticated than before. There is a growing misuse of electronic networks for criminal purposes or for objectives that can adversely affect the integrity of a nation's critical infrastructures. To address these issues, countries are implementing a cyber security strategy that will provide reasonable assurance of resilience and security to support national missions and economic stability. Mauritius recognises that the development of a national cyber security will help in managing deliberate and unintentional disturbances in the cyber space as well as recover from them. With this vision, a draft national cyber security strategy was developed by the National Computer Board and other stake holders. On 24th March 2014, a workshop was organized by the National Computer Board to validate the Strategy. The objective of the workshop was to discuss on the strategy goals, to finalise the recommendations and any other amendments required in the strategic document. The strategy was approved in October 2014 in Cabinet and is being implemented.

Professional IT Security Trainings

The following professional IT Security trainings were carried out during the month of June 2014:

⇒ Secure Software Development Life Cycle Practices (SSDLC)

This course was conducted in collaboration with STQC, India and provided a foundation for those professionals who are responsible for designing, architecting, coding and testing software solutions, through a series of lectures and hands on labs. It focused on how attacks are being directed towards software applications and how to design software to protect against attack is becoming more of a necessity.

⇒ STQC - Certified Network Security Manager (STQC – CNSM)

This course covered key security issues of computer network and means of securing them, addressing wireless LAN security and provide an overview of Vulnerability Assessment (VA) and Penetration Testing. Furthermore, this training provided interactive sessions and hands-on practise on tools. This course can help organisations in assessing and securing their network and protect their critical assets. The course was conducted in collaboration with STQC, India

Computer Security Day 2014

Computer Security Day is an annual event that is observed worldwide on the 30th November. It is designed to raise awareness and to promote best practices in Information Security. The event provides insight into the privacy and security issues surrounding electronically stored sensitive information and offers ways to keep your computer and data safe. To observe this day, CERT-MU, a division of the National Computer Board organized a full day cyber security conference on the 28th November 2014 at the Conference Hall, Swami Vivekananda International Convention Centre (SVICC). On this day, an exhibition was also organized to showcase the latest products on computer security. Exhibitors such as Leal Communications and Informatics, Blanche Birger, Secure Services Mauritius Ltd, amongst others were present. In addition, a professional training programme on Digital Forensics Investigation was also conducted. The target audience for the training were executives, IT professionals and Information Security Professionals.

Security Guidelines 2014

CERT-MU publishes Information Security Guidelines on a regular basis to help and guide users in adopting best practices and implement them whenever possible. The following guidelines were published in 2014:

⇒ **Guideline on Audit Log Management**
The purpose of the guideline is to provide advice and principles regarding the use of audit logs, the content of audit logs and the actions that are required as a result of a specific auditable event action occurring. The target audience for this guideline are computer security staffs, program managers, network and applications administrators, computer security incident response teams and others who are responsible for performing duties related to computer security audit and log management.

⇒ **Guideline on Incidents and Digital Evidence**
The purpose of the guideline is to assist staffs in dealing with allegations of crime which involve a high-tech element and to ensure they collect all relevant evidence in a timely and appropriate manner. The target audience of this guideline are cybercrime investigators, Information Security Consultants, Incident Handlers, System Administrators and Network Administrators.

⇒ **Guideline on Cloud Security**
The Guideline on Cloud Security provides a practical reference to help IT staffs and business decision makers when they analyse and consider the security implication of cloud computing within their organisations. The target audience for this guideline include information technology and security staffs responsible for the implementation of the cloud environment.

⇒ **Guideline on Vulnerability and Patch Management**
The purpose of this guideline is to assist organisations in identifying the vulnerabilities in their IT systems and patch them accordingly. It focuses on how to create an organizational model and test its effectiveness. It also covers technical solutions that are available for vulnerability management. This guideline has been developed for security managers responsible for designing and implementing security patch and vulnerability remediation strategies. Other target audience also include system administrators and security operations officers who are responsible for applying patches and deploying solutions.

⇒ **Guideline on Firewall**
The purpose of this guideline is to give organisations an insight of the different firewall technologies that are available and the different firewall architectures that could be applied to protect the network of an organization. The target audience includes CIOs, CISO Information Security staffs, network administrators and other relevant parties involved in the maintenance of the IT infrastructure.

⇒ **Guideline on Safe BYOD Management**
The purpose of this guideline is to give organisations an insight of the risks associated with Bring Your Own Device and how the adoption of a Mobile Device Management solution could help in mitigating some of those risks. The target audience includes CIOs, CISO Information Security staffs, network administrators and other relevant parties involved in the maintenance of the IT infrastructure.
The above mentioned guidelines are available on CERT-MU website: **www.cert-mu.org.mu.**

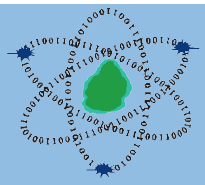
Security Tips

Never respond to an email asking for personal information

Companies you do business will never ask for account information, credit card numbers or PIN information in an email message. If you have any questions about an email you receive from your financial institution, call them for confirmation and **Do NOT** respond to the email.

Do not let spyware control your computer. Lower your risk by taking the following steps:

⇒ Update your operating system and Web browser software, and set your browser security high enough to detect unauthorized downloads.
⇒ Use anti-virus and anti-spyware software, as well as a two-way firewall, and update them all regularly.
⇒ Download free software only from sites you know and trust. Enticing free software downloads frequently contain other software, including spyware.
⇒ Do not click on links in pop-ups.
⇒ Do not click on links in spam or pop-ups that claim to offer anti-spyware software



CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu