CERT-MU eSecurity Newsletter

Addressing Information Security Needs for the Mauritian Cyber Community

Risk Management :- Principles to better Cyber Risk Oversight

The 5 Stages of Vulnerability Management

Gameover Zeus Malware Returns from the Dead..

Volume 4| Issue 2 | October 2014

NCB

CERT-MU

Dear Readers,

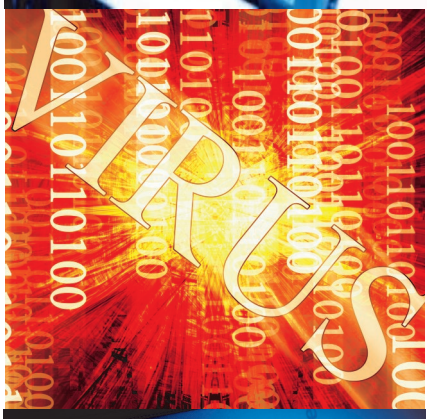
Greetings from CERT-MU,

Organisations depend on technology intensive information to successfully carry out their missions and business functions. However, these systems are subject to serious threats that can have adverse effect on organizational operations by exploiting known and unknown vulnerabilities to compromise the confidentiality, integrity and availability of information being processed, stored or transmitted. As such, the impact of a security incident on an organization can be significant. It is therefore imperative that leaders and managers at all levels understand the risks associated with the operation and use of information systems that support business functions. Managing security risks is like risk management in general. It brings together the best collective judgments of individuals within the organization, responsible for strategic planning, oversight management, day-to-day operations - providing necessary and sufficient risk response measures to adequately protect the missions and business functions of the organisations.

In this line, this eSecurity Newsletter focusses on the importance of managing cyber security risks. It also provides a complete insight of a well-known security bug known as "HeartBleed" that grabbed the attention of the world. Other issues which are highlighted in this are the 5 stages of vulnerability management, the latest information security news, CERT-MU events. New security tools have also been presented in the technology watch section. Finally, it provides an overview of the security guidelines published.

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

The e-Security Newsletter Team



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
* Organisation 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

For more Information:
www.cybersecurity.ncb.mu

Risk Management: 5 Corporate Principles to better Cyber Risk Oversight

One of the biggest challenges facing heads of information security is the ability to effectively communicate the value of their team's efforts across the organization, especially to the decision-making executives that lack the technical understanding of the cybersecurity threat and risk landscape.

To reduce the knowledge gap and raise awareness at top management level, the National Association of Corporate Directors (NACD), in collaboration with the Internet Security Alliance (ISA) and the American International Group (AIG), released the *NACD Directors' Handbook on Cyber-Risk Oversight*. Endorsed by the Department of Homeland Security (DHS), the handbook is the first publicly available document designed to guide board executives through five key principles to enhanced cyber risk oversight in a language that connects security to key business decisions. The handbook outlines the following five principles all corporate boards should consider:

1 Principle

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an it issue

- This principle highlights the importance of managing cybersecurity from "A strategic, cross-departmental and economic perspective," in which corporates should ensure that management is evaluating cybersecurity with regards to the larger ecosystem that the company operates in. Cybersecurity should be addressed regularly along with other strategic business plans.

2 Principle

Directors should understand the legal implications of cyber-risks as they relate to their company's specific circumstances.

- This principle suggests top management should be aware of the legal risks posed to the corporation in the event of a high-profile attack, including disclosure procedures.

3 Principle

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

- Recent studies show that top management often do not receive regular, comprehensive reports on privacy and security risks, making it difficult to adequately oversee these priorities. In addition to increasing access to cyber risk expertise, this principle recommends that boards should receive enhanced reports that disclose actionable metrics and beneficial information.

4 Principle

Directors should set the expectation that management will establish an enterprise-wide,cyber-risk management framework with adequate staffing and budget.

- This principle offers an integrated approach to managing cyber risk, including establishing ownership of responsibilities, appointing cross-organizational management teams and developing a proper budget of sufficient resources.

5 Principle

Discussion of cyber-risks between boards and senior managers should include identification of which risks to avoid, accept, mitigate or transfer through insurance as well as specific plans associated with each approach

- This principle discusses various critical questions that directors and management teams should contend, such as referencing the organization's risk-tolerance, investments, choosing the right solutions and conducting impact assessments.

Heartbleed: Post Analysis and its impacts

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 is one of the biggest security issues to have faced the Internet to date. The bug exists 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" is regarded as one of the most critical vulnerability in the OpenSSL cryptographic software library.

The bug affected OpenSSL version 1.0.1 through 1.0.1f (inclusive). Installations of the affected versions are vulnerable unless OpenSSL was compiled with -DOPENSSL_NO_HEARTBEATS. The Heartbleed bug existed because of improper input validation due to missing bounds check in the implementation of the TLS heartbeat extension. This vulnerability is classified as a buffer over-read, a situation where software allows more data to be read than should be allowed. The Heartbeat Extension tests TLS/DTLS secure communication links by allowing a computer at one end of a connection to send a "Heartbeat Request" message, consisting of a payload, typically a text string, along with the payload's length as a 16-bit integer. The receiving computer then must send the exact same payload back to the sender. The affected versions of OpenSSL allocated a memory buffer for the message to be returned based on the length field in the requesting message without checking the actual size of that message's payload. Due to improper bounds checking, the message returned consists of the payload, followed by other strings to be in the allocated memory buffer.

Heartbleed is exploited by sending a malformed heartbeat request with a small payload and large length field to the vulnerable party (usually a server) in order to elicit the victim's response, permitting attackers to read up to 64 kilobytes of the victim's memory that was likely to have been used previously by OpenSSL. Where a Heartbeat Request might ask a party to "send back the four-letter word 'bird', resulting in a response of "bird", a "Heartbleed Request" (a malicious heartbeat request) of "send back the 500-letter word 'bird'" would cause the victim to return "bird" followed by whatever 496 characters the victim happened to have in active memory. Attackers in this way could receive sensitive data, compromising the confidentiality of the victim's communications. Although an attacker has some control over the disclosed memory block's size, it has no control over its location, and therefore cannot choose what content is revealed. OpenSSL typically responds with the chunks of memory it has most recently discarded. The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests.

Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service. An attack against a server may also reveal the server's private master key which would enable attackers to decrypt communications (future or past stored traffic captured via passive eavesdropping, unless perfect forward secrecy is used, in which case only future traffic can be decrypted if intercepted via man-in-the-middle attacks). An attacker having gained authentication material may impersonate the material's owner after the victim has patched Heartbleed, as long as the material is accepted (for example, until the password is changed or the private key revoked). Heartbleed therefore constitutes a critical threat to confidentiality. However, an attacker impersonating a victim may also alter data. Indirectly, Heartbleed's consequences may thus go far beyond a confidentiality breach for many systems.

At the time of disclosure of the bug, some 17% of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, thus allowing theft of the servers' private keys and users' session cookies and passwords. In addition, as of May 20, 2014, 1.5% of the 800,000 most popular TLS -enabled websites were still vulnerable to Heartbleed.

Reverse Heartbleed

After the discovery of the heartbleed bug, vulnerable companies ranging from Facebook to Cisco implemented security patches, issued advisories and urged users to change their passwords. However, a few months later, another variation of the Heartbleed Bug was discovered. Dubbed by security researchers as "Reverse Heartbleed", this bug exploits the same vulnerability in OpenSSL. In the case of the Heartbleed bug, a client attacks a web server to steal data from its memory whereas in Reverse Heartbleed, the roles are reversed. In this scenario, a web server attacks a client to steal data. The bug can allow remote attackers to steal usernames, passwords and other confidential information from a user's computing device (PC, laptop or smartphone). These devices run OpenSSL when using certain web browsers, PDF readers and file sharing applications that run locally. Therefore, any computing devices running a vulnerable version of OpenSSL such as OpenSSL versions 1.0.1 and 1.02 beta would be affected. Reverse Heartbleed takes advantage of the same hitherto unnoticed programming mistake in OpenSSL, but essentially does so in reverse.

Exploitation of the HeartBleed Bug

Cybercriminals did not leave any opportunities unturned to exploit the Heartbleed bug. In April 2014, the system of Canada Revenue Agency (CRA) was hacked since it was vulnerable to the heartbleed bug. Over a period of 6 hours, around 900 social insurance numbers belonging to taxpayers were stolen from the CRA systems. The breach was notified by the Government of Canada's lead security agencies. When the attack was discovered, the agency had to shut down its website and extended the taxpayer filing deadline from April 30 to May 5, 2014. Later, it was found that an engineering student was charged for this data breach. It was also reported that anti-malware researchers exploited the vulnerability to access secret forums by cybercriminals.

Tools for testing the Heartbleed bug

Security researchers and firms have made security tools available for testing the Heartbleed bug.
Some of the tools are listed below:

- ⇒ Tripwire SecureScan
- ⇒ Arbor Network's Prevail Security Analytics
- ⇒ Norton Safeweb Heartbleed Check Tool
- ⇒ Critical Watch Free Online Heartbleed Tester
- ⇒ Metasploit Heartbleed scanner module
- ⇒ Lookout Mobile Security Heartbleed Detector (an app for Android devices) that determines the OpenSSL version of the device and indicates whether the vulnerable heartbeat is enabled
- ⇒ Heartbleed checker hosted by LastPass
- ⇒ Online network range scanner for Heartbleed vulnerability by Pentest-Tools.com
- ⇒ Official Red Hat offline scanner written in the Python language
- ⇒ Qualys SSL Labs' SSL Server Test which not only looks for the Heartbleed bug, but can also find other SSL/TLS implementation errors.
- ⇒ Browser extensions, such as Chromebleed and FoxBleed

Many lessons could be learned from the discovery of the heartbleed bug. Once it was determined that there were insufficient resources dedicated to maintaining and developing OpenSSL, the extended community responded immediately. This also prompted enterprises to identify other critical software that might not have sufficient resources devoted to maintaining it. Additionally, the relatively well-coordinated, industry-wide response to Heartbleed resonated, showing that it is easier to plan for vulnerability disclosure, determine how to test for the vulnerability and prioritize remediation rather than have to perform incident response without planning.

However, one lesson that does not seem to have received much attention is the difficulties in patching all the devices and software that were vulnerable but not included in standard enterprise-patching processes. Enterprises must learn that their standard patching and vulnerability management plans should include procedures for all systems, applications and software components in their network, regardless of whether they are part of the monthly or quarterly patching process. Apache Web server and Oracle database updates do not come nearly as frequently as monthly patches from Microsoft and Adobe, but in cases when an urgent patch must be applied quickly, the security team should ensure that the organization is able to do so. It is therefore important for organisations to keep an updated inventory of all systems – applications, endpoints, servers and other devices, with documentation on how to patch them while reducing business interruption.

In addition, if an enterprise has the ability to patch a high - risk vulnerability but does not do so, it must accept the risk that the vulnerability could be exploited on a system and potentially used to attack another one. In the case of heartbleed bug, not every organization might have patched the flaw immediately. This is because many organizations have limited resources, which in the security realm means making decisions based on risk. The best course of action is to prioritize high-risk flaws for remediation first and lesser ones later. Having a risk-based process in place can therefore help organizations to manage unexpected major incidents like Heartbleed.

Another key lesson enterprises can take away from the Heartbleed vulnerability and put into practice is the importance of minimizing the attack surface of a system or network. Removing unnecessary or outdated software before vulnerabilities can be found and exploited will prevent future attacks. This is part of the basic system hardening process that will help reduce the amount of time required to maintain the security of the system.

The Heartbleed security bug was also used to gain access to the contents stored in memory, such as passwords, but it did not directly result in remote code execution. Using any password acquired would require remote access to a system. Thus, while a system could have had passwords extracted from memory by Heartbleed, unless SSH, Remote Desktop Protocol (RDP) or some other access occurred where malicious code could be executed, additional access would not be gained. Having SSH, RDP or other direct access from the Internet setup is not common on notable systems like e-commerce Web servers because of the high-risk nature of this access. However, it is common on many systems that might fall through the cracks in an enterprise vulnerability management plan, like printers, video conferencing systems, embedded systems and any number of emerging Internet of Things-type devices.

To protect remote access connections, enterprises can block and minimize their attack surfaces with a network firewall, a host-based firewall or by outright disabling the connections on a system under attack. A network or host-based firewall could have blocked all but the required port(s) necessary to prevent the Heartbleed security bug from being exploited. Alternately, the OpenSSL heartbeat functionality that led to the Heartbleed vulnerability could have been disabled to prevent a potentially vulnerable system from being infiltrated.

On the other hand, a number of systems identified as vulnerable to Heartbleed were not the result of the primary application, but due to third-party software or hardware included in the system – most frequently this seemed to be the case with application or systems management tools. Installing third-party software patches on a timely basis would reduce the risk. Additionally, access to these applications or systems could be restricted to a secured administrative network if the software was even needed to reduce this risk. Should the risk be sufficiently high and a patch is found to be too hard to implement, application or system management software could be uninstalled if it was not necessary to prevent

Moreover, enterprises that used diverse operating systems or multiple layers of protection, for example, SSL load balancers or a Web application firewall were not vulnerable to attack. An attack dumping the full contents of memory could potentially be blocked if the attack triggered a firewall rule about a large number of network connections in a short period of time, but this could also block unexpected spikes in legitimate network traffic and cause business disruptions to an enterprise.

Following the news of the Heartbleed security bug, the IT industry has assembled around OpenSSL to devote more resources to the maintenance and the advancing development of the open source software as part of the critical infrastructure on the Internet. Growing attention to Heartbleed has resulted in the bug being remediated on most systems, but like Slammer, it will still be with us for more than 10 years. Inevitably, new systems will be released with this vulnerability present even after the patch, and may need to be alleviated in the future. Enterprises should therefore learn from past mistakes and do whatever possible to prevent falling victim again.

THE FIVE STAGES OF VULNERABILITY MANAGEMENT

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security. A vulnerability management process should be part of an organization's effort to control information security risks. This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. By identifying and mitigating vulnerabilities in the IT environment can help an organization to prevent attackers from penetrating their networks and stealing information.

A vulnerability management program should be part of any information security programs within an organization. In addition, Continuous Vulnerability Assessment & Remediation is listed as one of the Top 20 Critical Security Controls by the Council of Cyber Security based in Washington, USA. A Capability Maturity Model (CMM) has been developed by the Software Engineering Institute (SEI) at Carnegie Mellon to evaluate and measure the maturity of the software development process of an organization. The CMM is a model that helps to develop and refine a process in an incremental and definable method. It offers a set of guidelines and was built combining the best components of individual disciplines of CMM (Software CMM, People CMM etc.). It can be applied to product manufacturing, People management, Software development, amongst others.

There are 5 stages of the CMM and they are:

⇒ Initial
⇒ Managed
⇒ Defined
⇒ Quantitatively Managed
⇒ Optimising

This is shown in figure 1.

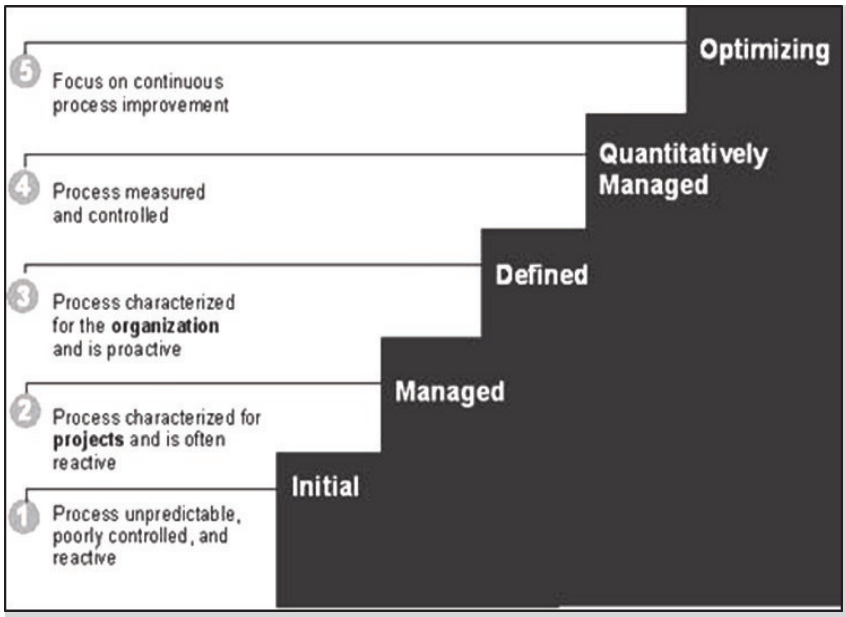


Figure 1

STAGE 1: INITIAL

In the 'Initial' stage of a vulnerability management program there are generally minimal processes and procedures. The vulnerability scans are done by a third-party vendor as part of a penetration test or part of an external scan. These scans are typically done from one to four times per year at the request of an auditor or a regulatory requirement. The vendor who does the audit will provide a report of the vulnerabilities within the organization. The organization will typically remediate any 'Critical' or 'High' risks to ensure that they remain compliant. The remaining information gets filed away once a passing grade has been given.

STAGE 2: MANAGED

In the 'Managed' stage of a vulnerability management program the vulnerability scanning is brought in-house. The organization defines a set of procedures for vulnerability scanning. It can purchase a vulnerability management solution and begin to scan on a weekly or monthly basis. Unauthenticated vulnerability scans are run and the security administrators are able to see vulnerabilities from an exterior perspective. Most organizations in this stage do not have support from top management, therefore leaving them with a limited budget. This results in purchasing a relatively cheap solution or using a free open source vulnerability scanner. While the lower-end solutions do provide a basic scan, they are limited in the reliability of their data collection, business context and automation. Using a lower-end solution could prove to be problematic in a couple of different ways. The first is in the accuracy and prioritization of your vulnerability reporting. Reports that are sent to the system administrators must be accurate in order to win the trust of the system administrators. Having the trust of the system administrators is a crucial component of an effective vulnerability management program. The second issue is that after verifying the vulnerabilities, it should be prioritized as per their severity - High, Medium and Low.

STAGE 3: DEFINED

In the 'Defined' stage of a vulnerability management program the processes and procedures are well-characterized and understood throughout the organization. The information security team has support from their executive management, as well as trust from the system administrators. At this point, the information security team has proven that the vulnerability management solution they chose is reliable and safe for scanning on the organization's network. Authenticated vulnerability scans are run on a daily or weekly basis with audience-specific reports being delivered to various levels in the organization. The system administrators receive specific vulnerability reports, while management receives vulnerability risk trending reports. Vulnerability management state data is shared with the rest of the information security ecosystem to provide actionable intelligence for the information security team.

STAGE 4: QUANTITATIVELY MANAGED

In the 'Quantitatively Managed' stage of a vulnerability management program, the specific attributes of the program are quantifiable and metrics are provided to the management team. The following is a summary of the automation metrics recommended by the Council on Cyber Security:

⇒ What is the percentage of the organization's business systems that have not recently been scanned by the organization's vulnerability management system?

⇒ What is the average vulnerability score of each of the organization's business systems?

⇒ What is the total vulnerability score of each of the organization's business systems?

⇒ How long does it take, on average, to completely deploy operating system software updates to a business system?

⇒ How long does it take, on average, to completely deploy application software updates to a business system?

These metrics can be viewed holistically as an organization or broken down by the various business units to see which business units are reducing their risk and which are lagging behind.

STAGE 5: OPTIMIZING

Lastly, in the 'Optimizing' stage, the metrics defined in the previous stage are targeted for improvement. Optimizing each of the metrics will ensure that the vulnerability management program continuously reduces the attack surface of the organization. The information security team should work together with the management team to set attainable targets for the vulnerability management program. Once those targets are met consistently, new and more aggressive targets can be set with the goal of continuous process improvement.

As one of the top four of the Top 20 Critical Security Controls, vulnerability management is one of the first things that should be implemented in a successful information security program. Ensuring the ongoing maturation of a vulnerability management program is a key to reducing the attack surface of an organization.

Gameover Zeus or GOZ Malware returns from the dead...

In 2014, Law Enforcement Agencies combined forces to carry out an international inter-agency collaboration known as "Operation Tovar" against the cybercrime group behind the malware family known as Gameover, Gameover Zeus or GOZ. The operation was successfully conducted and led to the shutting down of the activities from the Gameover botnet. Botnets are collections of malware infected computers individually referred to as bots or zombies that can be controlled remotely by criminals or botmasters. These cybercriminals can steal information such as banking credentials from each computer in the botnet, send commands to all computers in the botnet at the same time, thus giving them a huge distributed "network cloud" of computing resources. Botnets can be therefore used to send massive quantities of spam and to carry out online attacks, amongst others. Such types of attacks are difficult to block since they originate simultaneously from thousands of computers. One of such type of botnet ever discovered is Gameover.

Gameover ZeuS is a peer-to-peer botnet based on components from the earlier ZeuS Trojan. It is believed to have been spread through use of the Cutwail botnet. Unlike its predecessor the ZeuS Trojan, Gameover ZeuS uses an encrypted peer-to-peer communication system to communicate between its nodes and its command and control servers. According to a report by Symantec, Gameover Zeus has largely been used for banking fraud and distribution of the CryptoLocker ransomware. Just six weeks after the takedown operation took place, the Gameover Zeus malware made its apparition again. The malware came back from the dead and is linked to the even more infamous CryptoLocker ransomware. Gameover Zeus spams include attachments pretending to be an account statement with a message body such as:

The new Gameover variant has various common characteristics as the other variants. Gameover has scrambled most of its text messages (*strings*, in programming parlance) using a custom algorithm that has been the same since the source code to the original Zeus was leaked in 2011. This algorithm and the string table are still present in this new version and decrypted strings have also been used in this case similar to the earlier variants. In particular, the strings around _SUBBOTNET_ are the same as before.

> Dear Customer
>
> Your June 14, 2014 E-Statement for account number xxxxxxxxxxx3599 from Cards OnLine is now available.
>
> For more information please check attached copy
>
> Thank you
> Cards OnLine

However, some key differences have also been noted between the new variant and the other versions of Gameover Zeus. For example, in other variants, the malware writers used the Necurs rootkit, which made removal more difficult. Thus, without Necurs rootkit, the new Gameover variant can be cleaned up simply by deleting the .EXE file containing the malware and rebooting the machine.

The second key change is that the peer-to-peer (P2P) protocol that was used as a primary means of controlling the botnet is no longer used. A P2P bot does not rely on a pre-configured list of command-and-control (C&C or C2) servers to contact for instructions on what to do next. Infected computers can search out and connect to other bots in the botnet to fetch commands, making the botnet as a whole much more resistant to a takedown of one or more of the centralised C&C servers. However, there is still evidence of the P2P protocol commands in the malware program, but the sample is not seeded with a starting list of peer addresses and the code that attempts to find and use peers in the botnet is absent.

GOZ activity has led to the loss of millions of dollars through fraudulent Automated Clearing House (ACH) transactions and wire transfers. Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks. About 234,000 computers were infected around the world and Gameover Zeus is estimated to have pulled in $100m in illicit income.

Workarounds

To remediate the Gameover Zeus, the following actions can be taken:

- ⇒ Use and maintain anti-virus software - Anti-virus software recognizes and protects your computer against most known viruses. It is important to keep your anti-virus software up-to-date.
- ⇒ Change your passwords - Your original passwords may have been compromised during the infection, it is therefore advised to change them
- ⇒ Keep your operating system and application software up-to-date - Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it
- ⇒ Use anti-malware tools - Using a legitimate program that identifies and removes malware can help eliminate an infection. Users can consider employing a remediation tool that will help with the removal of GOZ from your system.

NEWS FOCUS:

Russian Hackers Amass Over a Billion Internet Passwords

A Russian crime ring has collected the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses as per security researchers.

The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420,000 websites, including household names, and small Internet sites. Hold Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems.

Due to nondisclosure agreements, the names of the companies whose sites remained vulnerable were not revealed. However, the information of several big companies was stolen. As per the security experts, hackers did not just target U.S. companies; they targeted any website they could get, ranging from Fortune 500 companies to very small websites.

The hacking ring is based in a small city in south central Russia, the region flanked by Kazakhstan and Mongolia. Their computer servers are thought to be in Russia. They began as amateur spammers in 2011, buying stolen databases of personal information on the black market. But in April, the group accelerated its activity. Since then, the Russian hackers have been able to capture credentials on a mass scale using botnets - networks of zombie computers that have been infected with a computer virus to do their bidding. Any time an infected user visits a website, criminals command the botnet to test that website to see if it is vulnerable to a well-known hacking technique known as an SQL injection, in which a hacker enters commands that cause a database to produce its contents. If the website proves vulnerable, criminals flag the site and return later to extract the full contents of the database.

By July, criminals were able to collect 4.5 billion records — each a user name and password — though many overlapped. After sorting through the data, it was found that 1.2 billion of those records were unique. Because people tend to use multiple emails, they filtered further and found that the criminals' database included about 542 million unique email addresses.

Community Health Systems hack hits 4.5 million data

A major hospital in US was victim of a cyber-attack resulting in the theft of 4.5 million people's personal data. The attack, which Community Health Systems believed originated in China, happened in April and June this year. The data included patient names, addresses, birthdates, telephone numbers and social security numbers. The firm, which runs 206 hospitals in 29 states, is now in the process of notifying affected patients. Security experts warned that the data could be used to steal people's identity. The FBI is investigating the breach. As per the Community Health Systems no medical or credit card records were taken. News of the attack follows several warnings, from both law enforcement and security experts, that medical equipment is at risk from hack attacks due to poor security measures.

CERT-MU EVENTS

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.

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.

Awareness Sessions on Internet Safety

As a continuation of the Safer Internet Day, 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.

Technology Watch: Security Tools

FakeNet Malware Analysis

FakeNet is a tool that aids in the dynamic analysis of malicious software. The tool simulates a network so that malware interacting with a remote host continues to run allowing the analyst to observe the malware's network activity from within a safe environment.

Advantages of the tool:

⇒ It is easy to install and use; the tool runs on Windows and requires no third party libraries
⇒ It supports the most common protocols used by malware
⇒ It performs all activity on the local machine to avoid the need for a second virtual machine
⇒ It provides python extensions for adding new or custom protocols
⇒ It keeps the malware running so that you can observe as much of its functionality as possible
⇒ It has a flexible configuration

Features

⇒ Supports DNS, HTTP, and SSL
⇒ HTTP server always serves a file and tries to serve a meaningful file; if the malware request a .jpg then a properly formatted .jpg is served, etc.
⇒ The files being served are user configurable
⇒ Ability to redirect all traffic to the localhost, including traffic destined for a hard-coded IP address
⇒ Python extensions, including a sample extension that implements SMTP and SMTP over SSL
⇒ Built in ability to create a capture file (.pcap) for packets on localhost
⇒ Dummy listener that will listen for traffic on any port, auto-detect and decrypt SSL traffic and display the content to the console

How it works

The tool FakeNet can be used on Windows and third party libraries. It uses a custom HTTP and DNS server to respond to those requests. It uses OpenSSL to wrap any connection with SSL. It uses a Winsock Layered Service Provider (LSP) to redirect traffic to the localhost and to listen for traffic on new ports. It uses python 2.7 for the python extensions. It creates the .pcap file by reconstructing a packet header based on the traffic from send/recv calls.

The tool can be downloaded on:
http://sourceforge.net/projects/fakenet/

LogRhythm v6.2

Combining SIEM, log management, file integrity monitoring and analytics with powerful forensic tools, LogRhythm v6.2 offers security professionals a powerful monitoring and auditing platform to keep them informed, and an excellent investigatory tool in case things go wrong. The tool is comprised of a series of modules. The Console provides the user interface and offers a single pane of glass for viewing logs, events, alerts and reports, conducting investigations and managing workflows. Designed to support fast access to millions of records, the console enables users to quickly correlate, search and pivot through their data rapidly. The integrated case management system enables events to be easily assigned to users for later analysis. In addition to the robust installable console, new to v6.2 is an attractive web GUI. While it is obviously in its infancy, it nevertheless enables quick, at-a-glance views of a number of reports and alarms and allows limited investigation. The Event Manager provides centralized event and incident management, analysis, reporting and configuration management across the entire deployment.
The Log Manager provides centralized log storage, log processing and archiving functions. The Artificial Intelligence Engine is the analytics platform and is the real meat of the tool. Taking log data from the Log Manager, it performs log correlation, pattern recognition and behavior analysis before sending results to the Event Manager. Finally, the System Monitor Agent does the actual log collection. Installed locally or on remote systems, it provides log collection services to Windows, Linux, AIX, HPUX and Solaris systems. All logs received are parsed and metadata is derived from them, which is then loaded into a database, greatly increasing performance while searching or performing analysis.

More information about the tool can be obtained:
www.logrhythm.com

Security Tip :-

Be careful while using the File sharing technology. This popular way of exchanging or sharing files can make your computer susceptible to risks such as infection, attack or exposure of personal information.

Security Guidelines, Tips & Events

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 guidelines can be downloaded from CERT-MU website: www.cert-mu.org.mu.

The latest guidelines published are as follows:

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.

CYBER SECURITY

The International Conference on Information Security and Cyber Forensics (InfoSec2014)
October 9 – 10, 2014
Universiti Sultan Zainal Abidin (UniSZA), Kuala Terengganu, Malaysia

Black Hat Europe
October 14 – 17, 2014
Amsterdam, Netherlands

SecureWorld Cyber Security Conference Colorado
October 16, 2014
Denver, United States

Cyber Security Summit
October 20, 2014
Bahrain

2014 Information Security Summit
October 30 – 31, 2014
Cleveland, Ohio USA

Cybercrime Prevention Summit
November 5 – 7, 2014
La Quinta, CA, United States

Cyber Security Awareness Week
November 13 – 15, 2014
Brooklyn, NY, USA

Security Tip: Understanding Patches

Patches are updates that fix a particular problem or vulnerability within a program. Sometimes, instead of just releasing a patch, vendors will release an upgraded version of their software, although they may refer to the upgrade as a patch. When patches are available, vendors usually put them on their websites for users to download. It is important to install a patch as soon as possible to protect your computer from attackers who would take advantage of the vulnerability. Attackers may target vulnerabilities for months or even years after patches are available. Some software will automatically check for updates, and many vendors offer users the option to receive automatic notification of updates through a mailing list. Make sure that you only download software or patches from websites that you trust. Do not trust a link in an email message - attackers have used email messages to direct users to malicious websites where users install viruses disguised as patches. Beware of email messages that claim that they have attached the patch to the message as these attachments are often viruses

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-mu.gov.mu

Vulnerability Reporting
Email: vulnerability@cert-mu.gov.mu

For Queries
Email: contact@cert-mu.gov.mu

Subscription to Mailing Lists
Email: subscribe@cert-mu.gov.mu