CERT-MU eSecurity Newsletter

Featured:

Cybercrime-as-a-Service: A Look Inside the Bustling Cybercrime Marketplace

NCB

Volume 6 | Issue 1 | July 2016

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 technological and social issues facing Internet users .

The Portal consists of Internet best practices for:

* Organisations
* Parents
* Kids
* Home users

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

in this ISSUE

Dear Readers,

Greetings from CERT-MU

The cybercrime marketplace or dark markets are gaining widespread attention as they are being linked to more attacks. The evolution of the cybercrime marketplace has resulted in the rise of the as-a-service acronym “aaS” which depicts a market offering multiple variants of hosted services such as stolen records, exploit kits and zero-day vulnerabilities. Despite the efforts of law enforcement agencies to tackle the cybercrime phenomena, the black market still remains resilient and is growing. This eSecurity Newsletter discusses the growth of the as-a-service nature of cybercrime by looking inside this bustling marketplace and analysing its offerings.

This edition also focuses on drones and the security implications of using them. Other issues highlighted in this e-security newsletter include latest information security news, CERT-MU events, recent security guidelines published, best practices and tips.

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

The eSecurity Newsletter Team

Cybercrime-as-a-Service:-
A Look Inside this Bustling Marketplace

The Cybercrime marketplace also known as the black, hacker or underground markets is grabbing widespread attention. Watering holes attacks based on exploit kits available for sale on black markets, the growing prevalence of malware inserted into online advertisements, stolen data, websites strangled by Distributed Denial of Service (DDoS) attacks implemented by rented botnets available on the black market are all contributing to the growth and complexity of such markets. The hacker market which was once a varied landscape of discrete and ad hoc networks of individuals has emerged into a playground of financially driven, highly organised, and sophisticated groups. Today's cybercrime marketplace is a multi-billion dollar ecosystem where buyers can buy tools, technology, services, and stolen goods from sellers through a combination of familiar e-commerce tools, digital currencies, and secure communication protocols. Understanding this market in its entirety is difficult due to the fact that it is geographically spread out, diverse, segmented and usually hidden under the cloak of darknets (such as TOR), anonymisation and cryptographic features. Access to such markets is getting tighter as there is rigorous and aggressive screening of individuals. More transactions are taking place on virtual private networks and darknets, with anonymisation and encryption capabilities enabled. Despite increased efforts by law enforcement to disrupt and shut down various parts of the market—from its financing to popular marketplaces - the hacker economy has proved to be quite resilient. The cybercrime market represents a challenge and threat to businesses, governments and individuals operating in the digital world. Increasing sophistication and specialisation describes how the market operates and the types of goods and services that are being sold. As with any other market, products and vendors tend to be reliable, but with the black market, people can be scammed. Numerous examples of the services-based nature of cybercrime have already caused significant damage. Such types of incidents are increasing and the evolution in the “as-a-service” nature of cybercrime fuels this exponential growth. This “business model” allows cybercriminals to execute attacks at considerably less expense than ever before. Examples include the ability to rent services that offer financial return or that claim to be able to bring down entire sites or systems for a relatively small sum. With the rise of the as-a-service nature of cybercrime, it is therefore important to have a look inside this bustling marketplace and analyse its offerings.

The evolution of the cybercrime marketplace has resulted in the rise of the as-a-service acronym “aaS” which depicts a market offering multiple variants of hosted services such as stolen records and exploit kits to “stolen-to-order” goods, such as intellectual property and zero-day vulnerabilities. Despite these markets being generally illicit, they follow the same economic laws and practices as other markets, for instance, customers communicate through various channels, place their orders, and get their products.

There are 4 categories of services that are managed by cybercriminals and they are as follows:

⇒ Research-as-a-Service

⇒ Crimeware-as-a-Service

⇒ Cybercrime Infrastructure-as-a-Service

⇒ Hacking-as-a-Service

1. RESEARCH-AS-A-SERVICE

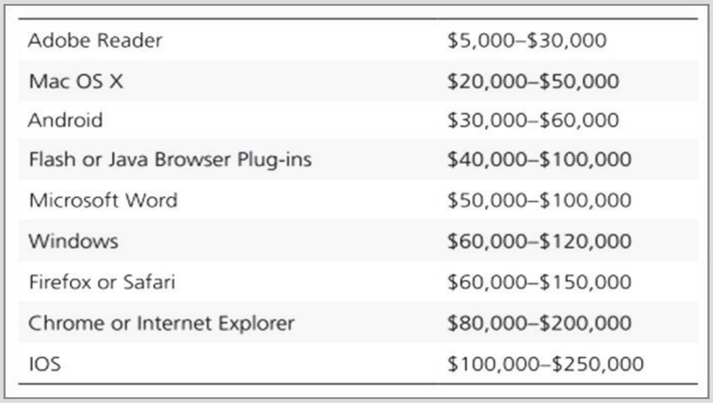
This service includes the identification of unknown vulnerabilities, also known as zero-day vulnerabilities within targeted systems. Despite the threat of legal actions by affected software vendors in certain countries, the sale of unknown vulnerabilities has recently become a growth area for researchers and brokers. Today, security researchers are presented with a number of options when they identify zero-day vulnerabilities. Each represents differing outcomes in publicity and monetary compensation.

⇒ Vulnerabilities for Sale

Today's marketplace provides those looking to acquire zero-day vulnerabilities with many options. Initially, this may appear to be detrimental to underground marketplaces. However, since many organisations selling zero-day vulnerabilities limit their sale to specific buyers, the underground market continues to flourish. Furthermore, restrictions are placed on the geographic location whereby customers are from predefined countries.

Although the acquisition of vulnerabilities can be conducted via a commercial entity, there is an opportunity to connect with a brokering service, which can be defined as a single individual who acts as a middleman to facilitate the sale to a third party, as per a report issued by McAfee. For example, a broker who acted as a middleman for the sale of exploits to government agencies was able to facilitate the sale of an Apple IOS exploit for $250,000 and pocket 15% commission.

The table below provides an example of the price range that were quoted for zero-day exploits



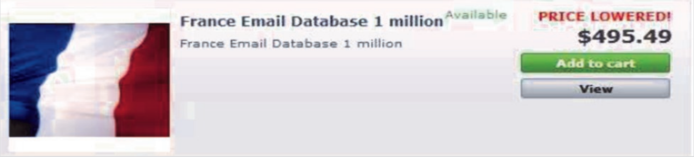
Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

Source: McAfee Cybercrime Exposed Report 2013

⇒ Spam services

Spam service is another service which is offered by the cybercrime market. A successful spam campaign relies on a number of factors. The cybercrime marketplace offers this service by providing list of email addresses that have been hacked. These email addresses are then sold for spamming purposes. Other services associated with spam include supplying email addresses belonging to individuals from a specific state, geography, specific professions or even a particular gender. The examples below show list of email addresses for sale in France and in Florida. In addition, services that support campaigns to propagate unsolicited emails are also provided. For instance, the infrastructure required to distribute the mail as well as the back-end systems used to host malicious content.

2. CRIMEWARE-AS-A-SERVICE



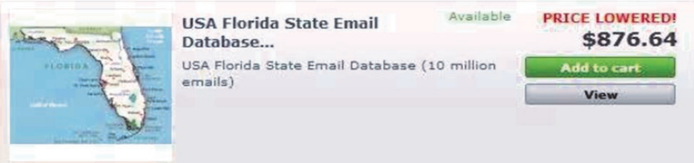
France Email Database 1 million

Available

France Email Database 1 million

PRICE LOWERED!

$495.49



USA Florida State Email Database...

Available

USA Florida State Email Database (10 million emails)

PRICE LOWERED!

$876.64

Crimeware-as-a-Service (CaaS) has become a prominent component of the underground economy. It is used as a business model in the underground market where illegal services are provided to help underground buyers to conduct cybercrimes such as attacks, propagating infections, and money laundering in an automated manner. CaaS provides a new dimension to cybercrime by making it more organised, automated, and accessible to criminals with limited technical skills.

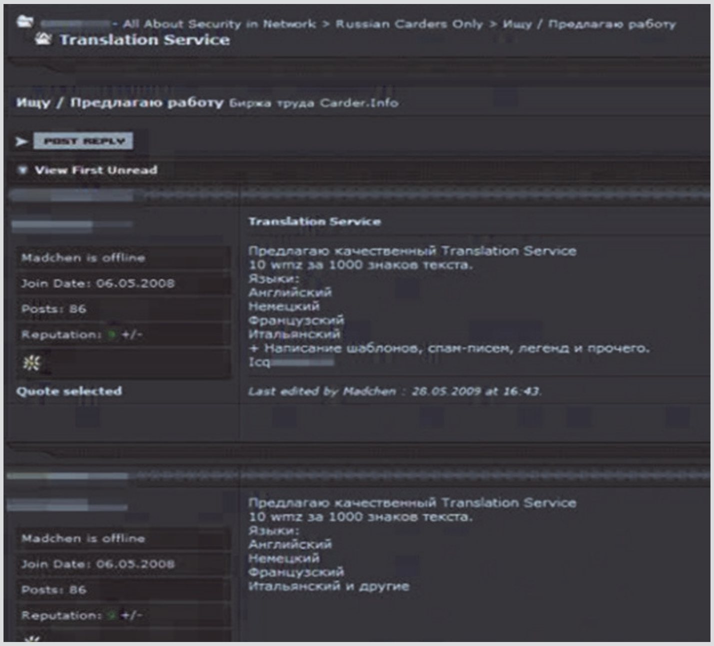
CaaS incorporates the identification and development of the exploits used for the intended operation and can also include development of additional materials such as droppers, downloaders, keyloggers, bots, and more for supporting the attack. This also includes tools used to conceal malware from security protection mechanisms (cryptors, polymorphic builders, joiners, crackers, and the like), as well as spammer/robot tools like XRumer. In addition, this category includes the availability of hardware that may be used for financial fraud, for instance, card skimming or equipment used to hack into physical platforms.

The categories of Crimeware-as-a-service include:

⇒ Professional services

The cybercrime market also provides professional services that require a degree of technical expertise and programming skills. An example of such service is code development for exploiting specific vulnerabilities. Much like the outsourcing market for commercial software, there are services that offer such code for nefarious purposes. The outsourcing of this particular element of attack has been around for some time, with some specific examples of malware being outsourced to a third party. For instance in 2005, with the Zotob worm, a programmer was paid to develop the malware which was estimated to cost affected companies $97,000 to clean up (source: *McAfee Cybercrime Exposed Report 2013*).

Translation service is another professional service that is provided by the dark market. This type of service is offered for crafting an email to lure victims in a targeted country with a specific language. The figure below shows a forum that offers translation services to would-be buyers. In this example, a communication method is defined, but also included is a reputational indicator. Much like the modern social media tools that are used today, there is an indicator as to the reputation of the individual behind the profile.



[redacted] - All About Security in Network > Russian Carders Only > Ищу / Предлагаю работу
Translation Service

Ищу / Предлагаю работу Биржа труда Carder.Info

POST REPLY

View First Unread

Madchen is offline
Join Date: 06.05.2008
Posts: 86
Reputation: +/-

Translation Service

Предлагаю качественный Translation Service
10 wmz за 1000 знаков текста.
Языки:
Английский
Немецкий
Французский
Итальянский
+ Написание шаблонов, спам-писем, легенд и прочего.
Icq[redacted]

Quote selected

Last edited by Madchen : 26.05.2009 at 16:43.

Madchen is offline
Join Date: 06.05.2008
Posts: 86
Reputation: +/-

Предлагаю качественный Translation Service
10 wmz за 1000 знаков текста.
Языки:
Английский
Немецкий
Французский
Итальянский и другие

⇒ **Malware services**

Numerous malware variants are available for sale. Buyers can acquire developed code to conduct their attacks. For example, attackers who want to obtain information can buy a malicious program concealed within a legitimate file, also known as Trojan Horse. Other examples include rootkits - surreptitious code that conceals itself within the compromised system and performs actions as programmed.

⇒ **Ransomware**

The services offered by the cybercrime market place are constantly evolving. The rapid rise of the crypto ransomware over the past several years is undoubtedly one of the biggest security concerns that security researchers are yet to tackle along with law enforcement agencies. The use of strong cryptography to make victims' data inaccessible and hold it for ransom is the biggest hurdle. Cybercriminals have now started an affiliate distribution scheme known as Ransomware as a Service or RaaS whereby there are two types of groups. The first group is the crypto ransomware creators and the second group is the one who spread the infection. The developer writes the malicious code and provides an intuitive administrative panel for any cyber perpetrator to use. The procedure for using such a campaign is to go through a registration process, which is usually free of charge. The customer then gets access to a dashboard which provides customised features. For instance, the desired amount of the ransom can be customized and the bitcoin address for payments can be configured. When using a RaaS kit, "customers" are obliged to share their revenue with the "merchant" typically ask for 20% of the ransoms submitted by victims.

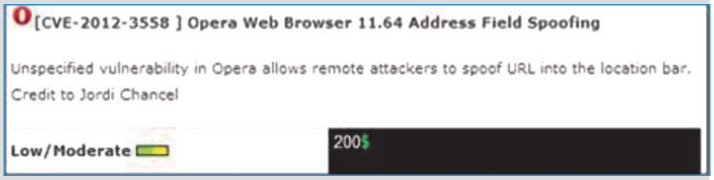
Examples of ransomware kits used for RaaS are Tox, Fakben, Encryptor RaaS, Hidden Tear and Ransom32.

⇒ **Exploits**

Long time ago, a hacker was recognised mainly as a researcher interested to measure its skills and capabilities against infrastructures and applications with the intent to find vulnerabilities to exploit. But today, this approach has changed. In fact, the discovery of unknown vulnerability for an application may be a business opportunity for the hacker. For example, the hacker can contact the manufacturer to request a fee to avoid the vulnerability disclosure and its usage by cyber criminals and ill intentioned. He may also choose to illustrate the vulnerability during scientific meetings or international competitions in order to increase his visibility. Recently, a trend has developed towards buying and selling these exploits.

A fundamental factor in this new market is the "instantaneity" of any transactions involving information regarding any vulnerability once identified. In a short lapse of time, the hacker must be able to identify a customer, negotiate the price and complete the sale before security researchers discover the vulnerability and name it as "zero day vulnerability".

The cybercrime marketplace also provides many options to purchase exploits that take advantage of vulnerabilities. Their prices vary based upon the target system and whether the vulnerability has been previously identified. The figures below show examples of the sale of such exploits.

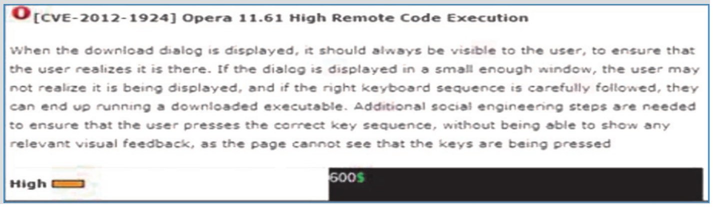


[CVE-2012-3558] Opera Web Browser 11.64 Address Field Spoofing

Unspecified vulnerability in Opera allows remote attackers to spoof URL into the location bar.
Credit to Jordi Chancel

Low/Moderate

200$



[CVE-2012-1924] Opera 11.61 High Remote Code Execution

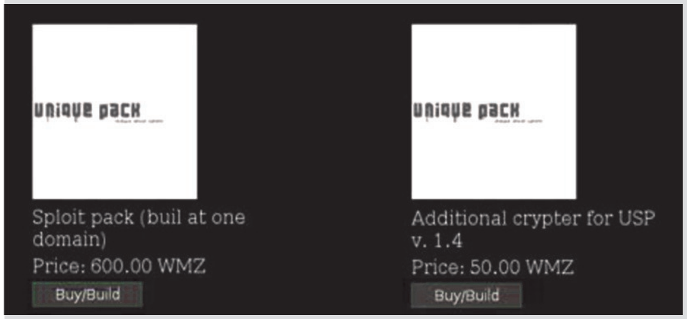
When the download dialog is displayed, it should always be visible to the user, to ensure that the user realizes it is there. If the dialog is displayed in a small enough window, the user may not realize it is being displayed, and if the right keyboard sequence is carefully followed, they can end up running a downloaded executable. Additional social engineering steps are needed to ensure that the user presses the correct key sequence, without being able to show any relevant visual feedback, as the page cannot see that the keys are being pressed

High

600$

The figures above include the details of the targeted system, a brief description, and its price. The prices of the exploits are aligned with the potential impact of the exploit. Those classified as high impact are approximately three times as expensive as those classified as low/moderate.

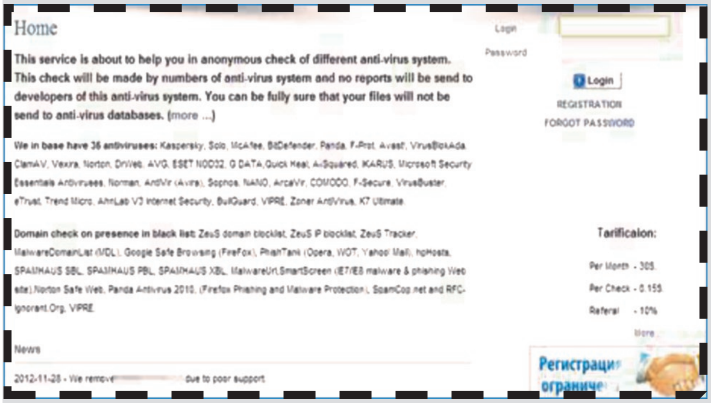
Exploit packs that offer encryption services are also available and are used to conceal an attack to avoid detection. This may include encrypting particular files, which may be used in combination with other techniques using encryption to further disguise the malicious code. An example of such exploit packs, with the crypter capability as an additional feature, is depicted in Figure below:



Sploit pack (buil at one domain)
Price: 600.00 WMZ
Buy/Build

Additional crypter for USP v. 1.4
Price: 50.00 WMZ
Buy/Build

Other service which is provided by the underground market is the checking of files against security software. Cybercriminals offer services of testing the malware against antivirus vendors' solution. In addition, they provide a service that tests the sending domain against a known list of domain blacklists. Such lists are used by companies and service providers to block email from domains that are known to send content against their policies, such as spam.



Home

Login
Password
Login
REGISTRATION
FORGOT PASSWORD

This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system. You can be fully sure that your files will not be send to anti-virus databases. (more ...)

We in base have 36 antiviruses: Kaspersky, Solo, McAfee, BitDefender, Panda, F-Prot, Avast!, VirusBlokAda, ClamAV, Vexira, Norton, DrWeb, AVG, ESET NOD32, G DATA,Quick Heal, A-Squared, IKARUS, Microsoft Security Essentials Antiviruses, Norman, AntiVir (Avira), Sophos, NANO, ArcaVir, COMODO, F-Secure, VirusBuster, eTrust, Trend Micro, AhnLab V3 Internet Security, BullGuard, VIPRE, Zoner AntiVirus, K7 Ultimate

Domain check on presence in black list: ZeuS domain blocklist, ZeuS IP blocklist, ZeuS Tracker, MalwareDomainList (MDL), Google Safe Browsing (FireFox), PhishTank (Opera, WOT, Yahoo! Mail), hpHosts, SPAMHAUS SBL, SPAMHAUS PBL, SPAMHAUS XBL, MalwareUrl,SmartScreen (IE7/IE8 malware & phishing Web site),Norton Safe Web, Panda Antivirus 2010, (Firefox Phishing and Malware Protection), SpamCop.net and RFC-Ignorant.Org, VIPRE

Tarificaion:
Per Month - 30$
Per Check - 0.15$
Referal - 10%
More

News

2012-11-28 - We remove [redacted] due to poor support

Potential buyers can engage in as much activities such as programming or researching, with the only constraints being how deep their pockets are, their technical competence, and available time. In some instances, certain services in this category are not illegal, with commercial companies offering their expertise on public forums.

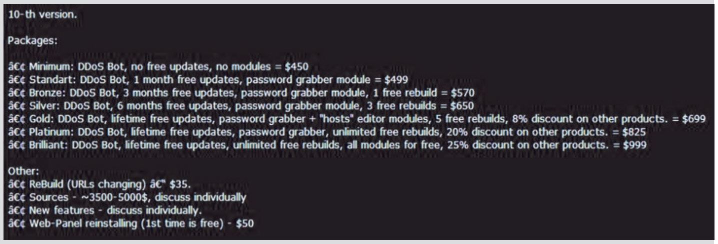
3. CYBERCRIME INFRASTRUCTURE-AS-A-SERVICE

A number of infrastructure services are available to support a cybercrime operation. These range from the availability of services to conduct denial of service attacks to host malicious content. Examples of cybercrime infrastructure- as-a-service are described below:

⇒ Botnets

A botnet is a network of infected computers under the remote control of an online cybercriminal. The botnet can be used for a number of services, such as sending spam, launching DoS, and distributing malware. Botnets have been one of the largest enablers of cybercrime from the mid-2000s. Not surprisingly, their presence and offerings are significant on the black market. Botnets started gaining ground in the market during the years 2003–2004, when they were used mainly for spamming. Botnets originally operated on Internet Relay Chat (IRC) and could be taken down by shutting down the IRC server. Nevertheless, the number of botnet variants doubled between 2004 and 2005, when the source code and a graphical user interface for creating botnets became available on the black market. This availability enabled lower-skilled users to create botnets by simply pointing and clicking. By 2007, more botnets using peer-to-peer (P2P) protocols appeared, making them harder to take down because of their distributed control.

The cybercrime marketplace offers the service of renting a botnet and various options are made available to suit the budget of the customer. An example is shown below:



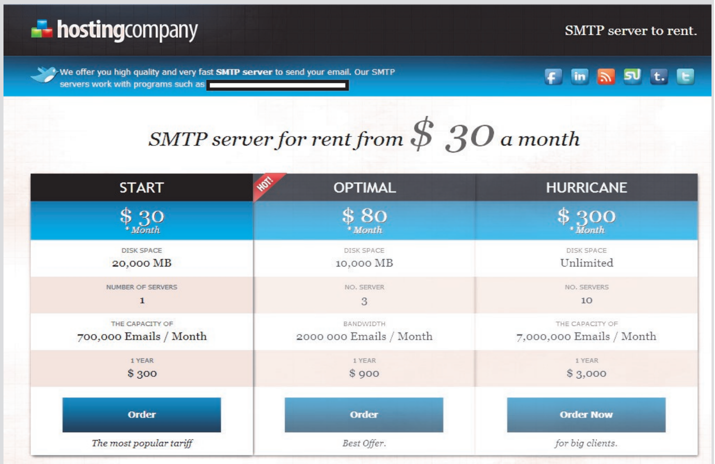
```
10-th version.

Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = $450
â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = $499
â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = $570
â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = $650
â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = $699
â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = $825
â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = $999

Other:
â€¢ ReBuild (URLs changing) â€" $35.
â€¢ Sources - ~3500-5000$, discuss individually
â€¢ New features - discuss individually.
â€¢ Web-Panel reinstalling (1st time is free) - $50
```

⇒ Hosting Services

Another service which is provided is hosting services, whereby a hosting provider provides web or domain hosting or other related services to cybercriminals. In addition, they ignore complaints by turning a blind eye to the malicious use of their services.

⇒ Professional Spam Services

Numerous services are available for the would-be spammer. These include the availability of services that support sending of unsolicited mail, alternatively known as a mail relay. The Figure below shows a service capable of sending 7,000,000 emails. The service proposition is well presented in the advertisement. For instance, it offers different packages for a month as well as payment options that many of us are accustomed to in the legitimate world. The "as-a-service" nature of the proposition is further emphasised by the fact that the would-be cybercriminal is provided the relay for just one month (with an upper limit of 7,000,000 emails). As mentioned above, an infrastructure is not enough to support an unsolicited email campaign. Email addresses and back end set of systems are required to be able to continue the deception. The latter could be hosted through bulletproof hosting services, which the cybercrime market is already offering.



SMTP server to rent.

We offer you high quality and very fast **SMTP server** to send your email. Our SMTP servers work with programs such as [redacted]

SMTP server for rent from $ 30 a month

START	OPTIMAL	HURRICANE
$ 30 * Month	$ 80 * Month	$ 300 * Month
DISK SPACE 20,000 MB	DISK SPACE 10,000 MB	DISK SPACE Unlimited
NUMBER OF SERVERS 1	NO. SERVER 3	NO. SERVERS 10
THE CAPACITY OF 700,000 Emails / Month	BANDWIDTH 2000 000 Emails / Month	THE CAPACITY OF 7,000,000 Emails / Month
1 YEAR $ 300	1 YEAR $ 900	1 YEAR $ 3,000
Order	Order	Order Now
The most popular tariff	*Best Offer.*	*for big clients.*

4. HACKING-AS-A-SERVICE

Cybercrime was once performed only by experienced and skilled hackers. But now, this is no longer the case. With the rise of Hacking-as-a-Service, fully commercialised tools with live chat support and guides are made available that allow non-tech savvy criminals to perform cyber-attacks. Under the category of hacking -as-a-service, the following services are offered:

⇒ Password cracking services

Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. Password cracking services is another service which is provided by the cybercrime market. Little technical knowledge is required for buyers to use this service. This makes it easy for a buyer to retrieve an email password, with no technical expertise. All that is required is the email address and name of the target. Afterwards, all that remains to be done is enter the password and pay for the service.

⇒ Denial-of-service

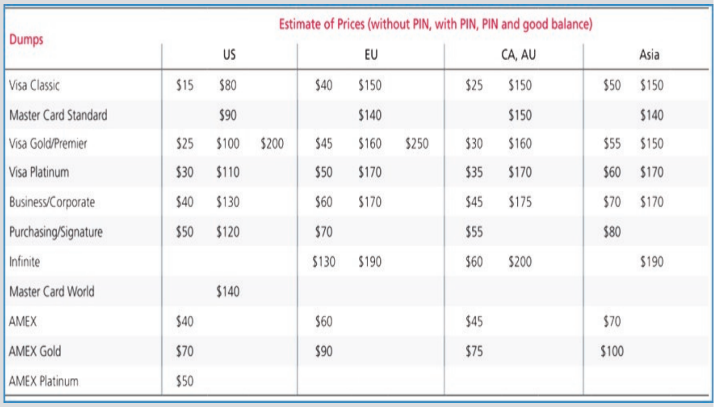
Denial of Service attacks or distributed denial of service attacks send huge volume of traffic to the victim and prevent them from conducting normal business operations. The cybercrime market now affords this service, which requires deep technical knowledge against a low payment. The figure below shows the price list for a "Cheap Professional DDOS Service." This service simply requires attackers to inform the service of which site they wish to launch a DDoS attack against, decide how much they are willing to pay, and then initiate the service.

Optima
HTTP
ICMP
SYN
UDP
DARKNESS X
Powerful DDoS Bot with premim admin-panel "Optima"
[From Russia with love]
4 types of DDoS Attacks/ Additional modules / 7 packages / Amazing Support
2009-2012. SW_Team

The figure below shows how cybercriminals are marketing their service for conducting an attack. Different packages are also offered for this service. This may demystify the sophisticated portrayal of today's hacker.

⇒ Sale of Credit Card Information

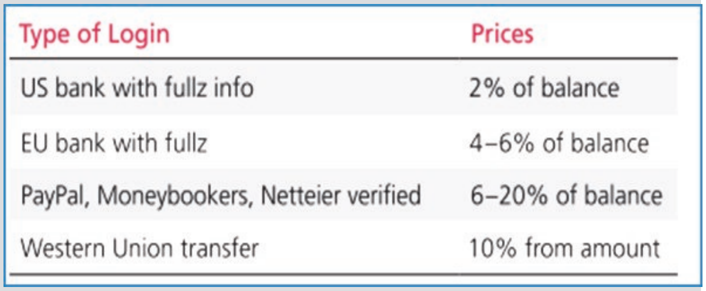
The cybercrime market also sells sensitive information such as credit card details and victims' credentials that has been gathered during data breaches. The table below shows an example of the prices for the stolen credit card numbers:



Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US			EU			CA, AU		Asia	
Visa Classic	$15	$80		$40	$150		$25	$150	$50	$150
Master Card Standard		$90			$140			$150		$140
Visa Gold/Premier	$25	$100	$200	$45	$160	$250	$30	$160	$55	$150
Visa Platinum	$30	$110		$50	$170		$35	$170	$60	$170
Business/Corporate	$40	$130		$60	$170		$45	$175	$70	$170
Purchasing/Signature	$50	$120		$70			$55		$80	
Infinite				$130	$190		$60	$200		$190
Master Card World		$140								
AMEX	$40			$60			$45		$70	
AMEX Gold	$70			$90			$75		$100	
AMEX Platinum	$50									

Source: McAfee Cybercrime Exposed Report 2013

Apart from credit card information, other banking details are also sold in the cybercrime market. An example is the login credentials for online banking. The table below shows the pricing structure for this type of information.



Type of Login	Prices
US bank with fullz info	2% of balance
EU bank with fullz	4–6% of balance
PayPal, Moneybookers, Netteier verified	6–20% of balance
Western Union transfer	10% from amount

Source: McAfee Cybercrime Exposed Report 2013

Since the mid-2000s, the hacking community has been steadily growing and maturing, as has its market. It took more than a decade of continuous development and innovation. The black market does not differ much from a traditional market as participants can communicate through various channels, place their orders, and get products. However, buying goods and services from this market is not reliable, often illegal and people may get scammed. Due to increase in recent takedowns, more transactions are moving to the darknet; stronger vetting of individuals is taking place; and greater encryption, obfuscation, and anonymisation techniques are employed, thereby restricting access to the most sophisticated parts of the black market. While law enforcement is making efforts to tackle the cybercrime phenomena, these black actors are going after bigger targets. Despite the growing rate of takedowns, the cybercrime marketplace remains resilient and is growing at an accelerated pace, continually getting more creative and innovative as defenses get stronger, law enforcement gets more sophisticated, and new exploitable technologies and connections appear in the world.

Come Spy with Me: Drones and Security Implications

Drones also known as unmanned aerial vehicles (UAVs), are aircrafts either controlled by 'pilots' from the ground or controlled remotely by an operator or installed with an automated function. The history of Drones shows peaks and valleys in their development, with most advances occurring during times of war. Drones gained notoriety during their use in the post-9/11 armed conflicts in the Middle East. The United States government use drones to conduct detailed surveillance on countries such as Afghanistan, Iraq, and Iran, as well as to drop targeted missiles. In early 2007, more than 700 drones were utilized in Iraq alone. Due to the heights at which drones can fly, they are often beyond the range of sight for most people. While their popularity in the civilian population has risen only recently, drones have been around for decades. In fact, one of the earliest drones was used by the U.S. in Vietnam. Drones were used in the military, but now its usage is not restricted to a particular function. Currently, drones are being used for several purposes such as to carry out surveillance and fight terrorism. Businesses are also looking to drones for advantages to rise above their competition. Undoubtedly, the use of drones is beneficial, but it has also various security implications that need to be addressed.

Drones can be used for a variety of purposes. Some people buy them to get impressive photographs from up in the air. Others use it for recording videos, some which go viral on sites like YouTube. Organizations and institutions can also use drones for crop-dusting, mapping out areas, and capturing footage of live sporting events. In the future, businesses could utilize drones for things like package deliveries. Basically, drones are used for the following purposes:

⇒ **Protection of population**

Drones are used to assist services like firefighting and wildfire detection, disaster relief, search and rescue. Drones could operate in risky areas or could be deployed to monitor specific areas to prevent incidents or to provide all the necessary support to the forces of intervention in the event of environmental disasters or accidents. Using UAVs, supplies can be transported rapidly into critical areas requiring medical attention, or any other kind of support, including food rations and other medicines. Drones can also be used by firefighting squads to monitor the progression of fires in wide areas, avoiding the need to involve civil personnel, or can be exploited to locate missing persons. UAVs could be equipped with thermal sensors or night vision cameras, and they can be used to quickly inspect a wide area, providing detailed information on it to the control center.

⇒ **Mineral prospection and mining**

Drones equipped with specific sensors can cover in-flight large areas for mineral detection. UAVs can be used to build a map of the territory by analysing the rock composition. Large areas with differing elevations could be inspected with high accuracy on a regular basis.

⇒ **Agriculture**

The agriculture industry is one of the sectors that most of all is benefiting of UAV usage, drones can rapidly map the fields, and could be also used to spray the crops with water or to fertilize the fields.

⇒ **Construction and Infrastructure Inspection**

Drones could be used to monitor critical infrastructure in a large area, taking pictures of pipelines, bridges and power lines. The goal is to support maintenance activities and assess the structures.

In the near future, drones could also be used to operate reparations to minimise the risk of any injury to human workers.

The increasing popularity of drone aircraft on the domestic, commercial, and military front has introduced a whole host of new concerns. Uncertainly, drone usage will bring different benefits but it also raises numerous implications under security and privacy perspectives. Surveillance drones are equipped with sophisticated imaging technology that provides the ability to obtain detailed photographs of land, people, homes, and even small objects. Gigapixel cameras used to outfit drones are among the highest definition cameras available, and can provide real-time video streams at a rate of 10 frames a second. On some drones, operators can track up to 65 different targets across a distance of 65 square miles. Drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of video surveillance were unable to achieve. By virtue of their design, their size, and how high they can fly, drones can operate undetected in urban and rural environments. Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers. In the near future these cameras may include facial recognition technology that would make it possible to remotely identify individuals in parks, schools, and at political gatherings.

The U.S Federal Aviation Administration (FAA) has approved their use for police and government agencies, issuing about 1,400 permits over the past several years, and it will authorize civilian air space use by 2015. The situation is quite similar in Europe, where the use of drones for civilian use is expected to start by 2016.

Apart from privacy concerns, as the use of drone increases, both for commercial applications and for recreational purposes, new risks also emerge. The principal risks are represented by the possibility that groups of criminals and cyber terrorists could hack unmanned aerial vehicles, with intent of harming the population. Drones could be attacked for several purposes, and hackers could be intentioned to interfere with the services they provide and could abuse them for cyber espionage or could hijack them for sabotage. Some of the main security risks of using drones are highlighted below:

⇒ **Reconnaissance and Surveillance:** In this scenario, an actor could use a drone to look targets for attack or monitor the actions of individuals or law enforcement. The utility of off-the-shelf drones for reconnaissance and surveillance has already been proven in battle spaces like the civil war in Ukraine. The rapid spread of drones makes this scenario both the most likely threat involving drones and the most difficult to identify. Just in the past few years, there have been many cases in which it was difficult to determine whether the drone was being used for recreational use, newsgathering, activism, or for an activity that could result in harming public safety. The challenges in recognising the threat could pose an additional harm: an overreaction by individuals on the ground, leading to a potentially violent escalation.

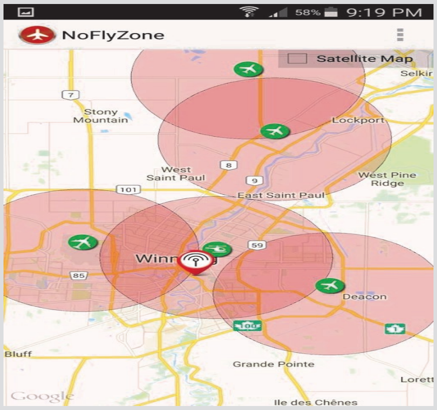
⇒ **Smuggling:** There have been multiple cases around the world where criminal organisations or individuals have used drones to smuggle illicit material, usually across borders or into prisons. In November 2013, a drone was spotted flying over the walls of a prison in Quebec, and in March 2014, a similar event occurred in Australia. Earlier this year, a drone carrying drugs was discovered crashed just south of the U.S.-Mexico border.

⇒ **Electronic Attack:** At the 2014 Black Hat security conference in Singapore, information security firm SensePost revealed “Snoopy”, a drone that can hack into WiFi and steal the data on those networks. In what is known as a “karma attack,” Snoopy can also impersonate a network that an unsuspecting user might join, whereupon the code would steal that users’ data. This method could be used to particular effect in a crowded environment where many people have their cell phones automatically searching for WiFi networks. In February, it was revealed that AdNear, a Singapore-based marketing firm, was experimenting with commercially available drones that would help to deliver targeted advertisements by collecting data on cell phones.

⇒ **Kinetic Attack:** In this scenario, an attacker might strap guns or explosives to a drone and fly it into people or structures to inflict physical damage or loss of life. The targets of these attacks may be individuals, buildings, or transportation infrastructure such as commercial airliners. In 2011, 26-year-old Rezwan Ferdaus was arrested in an FBI undercover operation and accused of planning to build small explosive-laden drones to attack the Pentagon and the U.S. Capitol, according to law enforcement officials. In an article at Wired, it was reported that, at a conference hosted by the Department of Homeland Security in January, counterterrorism officials displayed several models of drones that were outfitted with inert explosives.

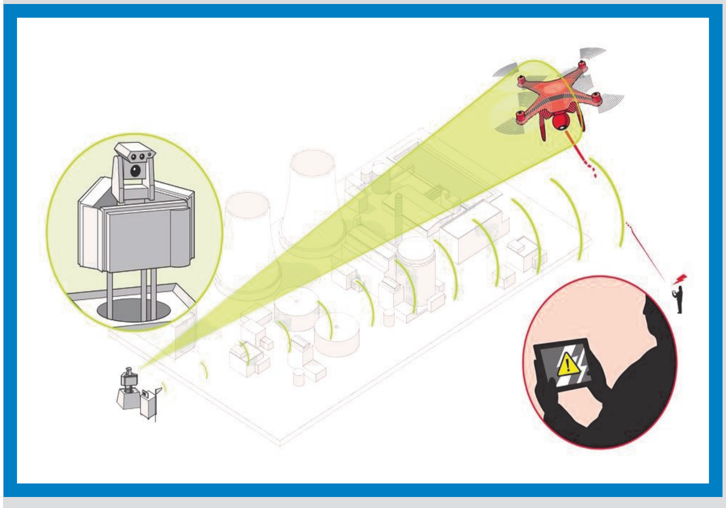
⇒ **Weapon of Mass Destruction (WMD) Attack:** An attacker could use a drone to spray a weaponized chemical or biological agent over, for example, a crowd of people or in a downtown area. This scenario predates the rise of mass-market drones like the Phantom.

A number of countermeasures have been proposed to defend against potential threats posed by drones. Some of these defenses are already being developed by university researchers and private companies while others are being considered by law enforcement and the military.



⇒ **Geo-fencing:** Unlike most of the other defenses, this method is already in place before the drone takes off. With geofencing, the drone manufacturer engineers into the firmware of the drone a virtual boundary on the geographical areas where the operator cannot fly, forcing the drone to ground if operators trespass into these areas.

⇒ **Spoofing:** This involves fooling the GPS on the drone by creating a series of false coordinates that allows the defenders to take control of the drone. This defense mechanism was demonstrated in 2012 by a team led by Professor Todd Humphreys at the University of Texas-Austin. It is also believed that the Iranians used spoofing to bring down a U.S. Sentinel spy drone in 2011.



⇒ **Jamming:** This is another electronic attack that attempts to sever the command link between the attacking drone and the ground station, forcing the drone to fly without intervention by the operator or, in extreme cases, transferring command of the drone to the defender. However, by switching to autonomous flight mode, the drone can avoid some forms of jamming.

⇒ **Lasers:** Lasers are believed to have potential to be effective for countering drones. In November 2014, China unveiled a laser system that is designed specifically for shooting small drones. According to Chinese state media Xinhua, the laser will "play a key role in ensuring security during major events in urban areas.

⇒ **Firearms:** This is one of the most common ways to bring down small drones. Shooting a gun at a drone is the most likely scenario to result in someone on the ground getting injured from falling parts -particularly in a metropolitan area—or, obviously, from stray bullets.

⇒ **Drone-on-Drone:** This countermeasure involves defending drones that would intercept attacking drones in the air. For the most part, this countermeasure is purely speculative. It could involve drones equipped with large nets catching smaller drones in the air. Or, swarms of drones could intercept larger manned or unmanned attackers. In 2012, Timothy Chung, an assistant professor at the Naval Postgraduate School, experimented with a project called Aerial Battle Bots that pitted swarms of UAVs against each other.

Drones can be used for many purposes and are beneficial in many sectors. It is widely used for military purposes and by law enforcement agencies. However, usage of drones also raises privacy issues. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of video surveillance were unable to achieve. In the future, it may also include sensors and cameras that have facial recognition capabilities, which can likely intrude an individual privacy. Apart from privacy issues, there are also risks of using drones. Ideally, access to drones would be limited to only those people and organisations that could be trusted to use them responsibly. Nevertheless, it can also fall into the wrong hands, which can pose a threat to public safety. It is therefore important that substantial legal and constitutional issues involved in the deployment of aerial drones be addressed.

Ransomware - Most Dominant Threat

Ransomware has become the new dominant threat for this year. Since January, there has been an increase in the number of infected victims as new families of ransomware are making their apparitions. It is becoming a hugely profitable business for cybercriminals. Before, ransomware victims were consumers and small businesses. But bigger institutions such as hospitals and universities are also becoming victims. In June 2016, one site that tracks ransomware logged more than 120 separate families of the malicious code being used in different campaigns.

The European police agency Europol is teaming up with cybersecurity companies in an initiative aimed at slowing an exponential rise in ransomware. The scheme revolves around a website that connects victims and police, gives advice and helps with data recovery. The number of ransomware victims tripled in the first three months of 2016, according to one estimate. "**The No More Ransom**" site will be updated as ransomware gangs are tackled as per security researchers. Co-ordinated by Europol, the initiative also involves the Dutch national police, Intel Security and Kaspersky Labs.

No More Ransom brings together information about what ransomware is, how to avoid falling victim and what to do if a person or company is caught out. Right now the only option victims have is to pay the ransom or not. But with the coming of this website, this will give people another option. Often, people struggle to find out what they can do when they are hit. With this website, victims will be able to upload scrambled files to identify which strain of ransomware has locked up their data.

The site will be kept up to date with information gleaned from international action against gangs that run ransomware campaigns. Other police forces, security companies and researchers will be encouraged to contribute to the site and add advice or tools to help victims. At present, the site links to decryption software for four well-known families of ransomware - Coinvault, Shade, Rannoh and Rakhni.

Security Tips to protect from ransomware:

⇒ **Use an antivirus software and a firewall.** Maintaining a strong firewall and keeping your security software up to date are critical.

⇒ **Do regular back up** . If you back up files to either an external hard drive or to an online backup service, you diminish the threat. If you back up your information, you should not be afraid to just turn off your computer and start over with a new install if you come under attack.

⇒ **Enable your popup blocker** - Popups are a prime tactic used by the bad guys, thus avoid even accidentally clicking on an infected popup. If a popup appears, click on the X in the right-hand corner. The buttons within a popup might have been reprogrammed by the criminals, do not click on them.

⇒ **Exercise caution -** Do not click on links inside emails, and avoid suspicious websites. If your PC does come under attack, use another computer to research details about the type of attack. But be aware that the bad guys are devious enough to create fake sites, perhaps touting their own fake antivirus software or their de-encryption program.

⇒ **Disconnect from the Internet**. If you receive a ransomware note, disconnect from the Internet so that your personal data is not transmitted back to the criminals.

⇒ **Do not pay the ransom** — Ransomware is a serious form of extortion. Do not be tempted to give in and pay the ransom. Paying them would be a mistake because they will further extort you and most likely not release your information. Taking precautions to protect your information and maintaining vigilance are the best solutions to avoid becoming a victim in the first place.

CERT-MU Event - Cyber Security Drill 2016

Societies are becoming increasingly dependent on information and communication technologies, which are globally interconnected. However, with these growing dependencies, new threats to network and information security have emerged. Preparation is the key to mitigate the damage that cannot be prevented. To protect their critical infrastructures, many countries worldwide are now engaging in cyber security drills.

Cyber Security Drills are carried out to assess organizations' preparedness to resist cyber threats and enable timely detection, response, and mitigation and recovery actions in the event of cyber-attacks. By detecting and responding to simulated cyber security incidents, organisations will be in a better position to know about the vulnerabilities present in their infrastructure and how they can improve their security practices.

In line with the Government's vision to make Mauritius secure and resilient, CERT-MU in collaboration with the International Telecommunication Union (ITU) organised an International Cyber Security Drill from 4-8th April 2016. This kind of event was conducted for the first time in Mauritius and was the third regional Africa drill with the support of ITU as part of their Global Cybersecurity Agenda. Delegates from 21 countries participated in the drill.

The objective of the event was to raise awareness on incident response and assess organisations' preparedness to resist cyber threats and enable timely detection, response, and mitigation and recovery actions in the event of cyber attacks. By detecting and responding to simulated cyber security incidents, organisations will be in a better position to know about the vulnerabilities present in their infrastructure and how they can improve their security practices.

The event was planned over a period of five days and the activities organised included one day workshop focusing on Incident Handling, two days cyber drill exercises and two days of training sessions.

The first day was dedicated to a series of workshops on current cybersecurity issues, followed by two days of cyber drill exercises structured around various scenarios involving the most common types of cyberattacks while the sharing sessions provided a platform for cooperation and discussions on cybersecurity and the last two days were dedicated to capacity building session. The cyberdrill exercises were centered on developing threat intelligence capability, malware reengineering and attack scenarios.

The benefits of the drill were:

⇒ To enhance communication and collaboration among participating partner countries.

⇒ To build capacity and improve the incident response capabilities of participants.

⇒ To gauge and improve the preparedness of member states in the identification, response, prevention and resolution of computer incidents.

⇒ To demonstrate Mauritian organisations to evaluate the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

The target audience for the cyber security drill were Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

COMING SOON

TECHNICAL COLLOQUIUM

CERT-MU is collaborating with Forum for Incident Response and Security Teams (FIRST) to host a 3-day Technical Colloquium for Mauritius from 22nd – 24th November 2016. This will be the 1st regional Africa Technical Colloquium to be conducted in Mauritius with the support of FIRST. The event is planned over a period of three days, which will be as follows:

- One-day workshop focusing on Cybersecurity- 22nd November 2016.
- Two-days training programme on Computer Security Incident Handling - 23-24th November 2016.

More information will be available on:
www.cert-mu.org.mu

Security Guidelines & Tips

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 latest guidelines published are as below:

- **Guideline on Malware Incident Response**

The purposes of this guideline is to provide process and tasks to help determine the nature of the malware problem, limit the spread of malware, and return the system to operation. The target audience for this guideline includes mainly incident handlers and security professionals.

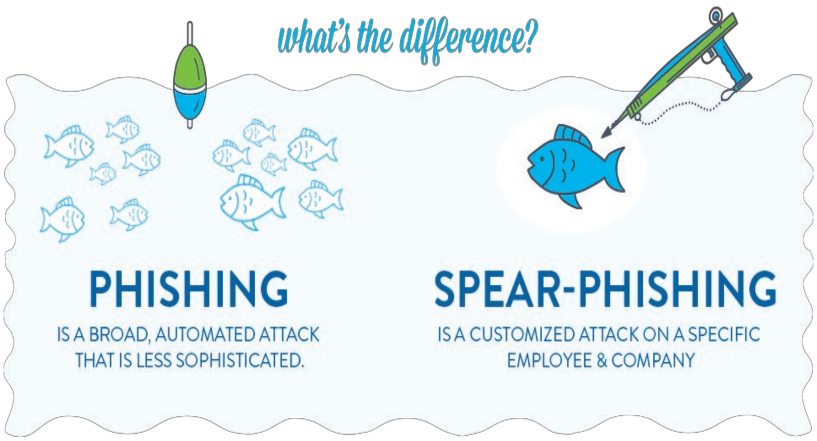
- **Guideline on Internet of Things (IoT)**

The purpose of the document is to provide a generic set of security controls for security and privacy in the IoT. The target audience for this guideline include early adopters of IoT and smart devices.

- **Guideline on Online Identity Theft**

The purpose of the guideline is to provide an insight on online Identity Theft, how it can happen and what precautions can be taken so as not to fall victims of the crime.

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



PHISHING
IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.

SPEAR-PHISHING
IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

CYBERSECURITY IS OUR SHARED RESPONSIBILITY

PROTECT YOUR INFORMATION

- ✓ *NEVER* share your password
- ✓ Run updates regularly
- ✓ Use a strong password
- ✓ Use anti-virus and anti spyware
- ✓ Use encryption

i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I 5hal! u53 $4r0ng-p@5sw0rdz!

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.

Beware of Phishing Scams. Don't take the Bait.

- Phishing attacks use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses.
- No legitimate organization will ever ask for your password over email or on the phone.
- Pay attention to the website's address. Malicious websites may look like a legitimate site, but the web address may use a variation in spelling or a different domain (e.g., .com versus .net).

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