CERT-MU

eSecurity Newsletter

Featured:
Who makes the IoT under attack?

Volume 6 | Issue 2 | December 2016

CERT-MU

CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

Your Partner in Cyber Security

www.cert-mu.org.mu

CERT-MU SERVICES

Reactive Services:

* Incident Handling
* Vulnerability Scanning and Penetration Testing

Proactive Services:

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

What's Inside

4 Who makes the IoT under attack?

9 The Reign of Ransomware

12 Why Blockchain will Explode Next Year

15 Security Guidelines & Tips

Dear Readers,

Greetings from CERT-MU!

The year 2016 has witnessed a lot in terms of technology development and cyber attacks. Cybersecurity incidents continue to grow in frequency and impact to businesses. Every year breaches are on the headlines, with the resulting enterprise impact such as loss of customer confidence, financial loss and in some cases, the inability of an enterprise to recover and eventual shut down. Security breaches are not a distant problem any longer, rather they are now a fact. Of all the technology trends that are taking place right now, perhaps the biggest one is the Internet of Things, which is the one that's going to give us the most disruption as well as the most opportunity over the next five years.

In this edition, we have talked about the insecurity of the IoT that can affect a major part of the Internet. We have also observed that Ransomware has been at the top of the security landscape in early 2016 and seen how Blockchain will explode the year 2017, despite the various existing cyber threats.

The CERT-MU team is here to keep you updated on the latest information security news so stay tuned!

The eSecurity Newsletter Team

WHO MAKES THE IOT UNDER ATTACK?

The malware known as "**Mirai**," works by spreading to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default usernames and passwords. There are 68 username and password pairs in the "Mirai" source code. However, many of those are generic and used by multiple products, including routers, network-based security cameras, printers and digital video recorder (DVRs) and even printers.

The problem is that instead of hard-coding credentials or setting default usernames and passwords that many users will never change, hardware manufacturers should compel users to pick a strong password when setting up the device. Indeed, several IoT device makers, including **Hikvision**, **Samsung**, and **Panasonic**, have begun to require unique passwords by default, with most forcing a mix of upper and lowercase letters, numbers, and special characters.

How these various IoT devices could be exposed if users have configured them to operate behind wired or wireless routers?

The answer is that most consumer routers assign each device inside the user's home network so-called Network Address Translation (NAT) addresses that cannot be directly reached

HELP, I NEVER CHANGED THE DEFAULT PASSWORD!

from the Internet. However, because of the Mirai source code leak, many IoT devices will use a technology called Universal Plug and Play (UPnP) that will automatically open specific virtual "ports," essentially poking a hole in the router's shield for that device that allows it to be communicated with from the wider Internet.

It does not matter whether your device is listed above, if you own a wired or wireless router, IP camera or other device that has a Web interface and you have not yet changed the factory default credentials, your system may already be part of an IoT botnet. Unfortunately, there is no simple way to determine whether it has been compromised.

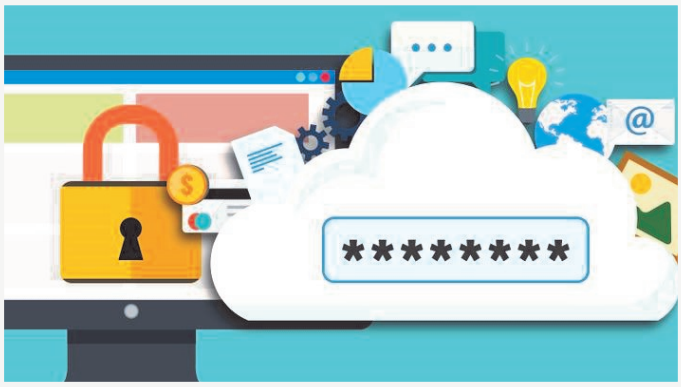
However, the solution to eliminating and preventing infections from this malware is not that complicated. Mirai is loaded into memory, which means it gets wiped once the infected device is disconnected from its power source.

An advice for users running devices with default credentials.

Make sure you know how to access the device's administration panel. If you are not sure how to reach the administration panel, perform an online search on the make and model of your device, you will get a web address and default credential pair that can be typed or pasted into a Web browser.

If possible, reset the device to the factory-default settings. This should ensure that if any malware has been uploaded to the device that it will be wiped permanently. Most devices have a tiny reset button that needs to be pressed and held down for a several seconds while powered on to reset the device back to the factory default settings.

When the device comes back online, open a Web browser, navigate to the administration panel, enter the default credentials, and then change the default password to something stronger and more memorable.



Unfortunately, many of these devices also require periodic software or "firmware" updates to fix previously unknown security vulnerabilities that the vendor discovers or that are reported to the hardware maker post-production. However, relatively few hardware makers do a good job of making this process simple and easy for users, let alone alerting customers to the availability of firmware updates.

When it comes to software updates, automatic updates are acceptable. Simple updates that notify the user and require intervention are considered secure. Updates that require the user to do some research to find and install manually are not helpful. Devices that do not have updates at all are completely worthless. And that can be applied to traditional computing as well. It's just that with IoT, you likely have even-less-technical users at the helm.

Only after fixing any problems related to default credentials should readers consider checking for firmware updates. Some hardware makers include the ability to check for updates through a Web-based administration panel, while others may only allow firmware updates manually via downloads from the manufacturer's site.

Firmware updates can be tricky to install, because if you fail to follow the manufacturer's instructions, you may mess up your device. So if you decide to go ahead with any firmware updates, you should proceed carefully and deliberately.

BUT WAIT, THERE'S MORE!

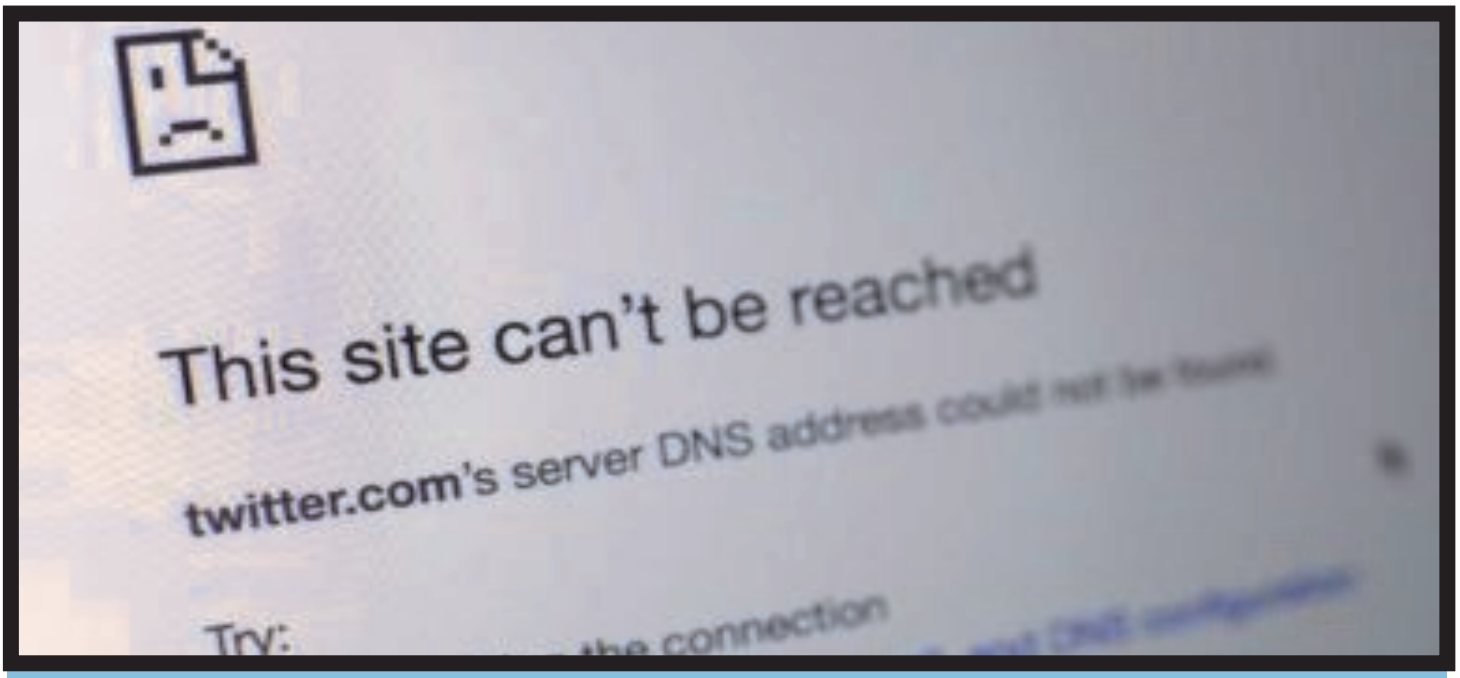
If IoT users change their default passwords via the device's Web interface it can be a security precaution. However, it may or may not address the fundamental threat. That is mainly because Mirai spreads via communications services called "telnet" and "SSH," which are command-line, text-based interfaces that are typically accessed via a command prompt (e.g., in Microsoft Windows, a user could click Start, and in the search box type "cmd.exe" to launch a command prompt, and then type "telnet" <IP address> to reach a username and password prompt at the target host).

The trouble is, even if one changes the password on the device's Web interface, the same default credentials may still allow remote users to log in to the device using telnet and/or SSH.

Telnet and SSH are an operating system-level login, and the Web interface tends to be more of an application level login. Sometimes changing a password on one changes the password on the other, but more often the Web interface is completely different, and changing the password there may not change the underlying password needed to access the device remotely via SSH and Telnet.

In February 2016, it has been observed that IP cameras sold by Chinese Web camera giant Foscam, by default included a feature which would quietly phone home to a vast peer-to-peer (P2P) network run by the company. While the Web interface for those P2P cameras included a setting allowing users to disable the P2P traffic, disabling that option didn't actually do anything to stop the device from seeking out other Foscam P2P cameras online.

MIRAI - THE CYBER ATTACK THAT CRIPPLED AMERICA'S INTERNET



Amazon, Twitter, CNN, PayPal, Spotify and many other websites were down on the early morning of Friday, October 21st, 2016. This was made possible because hackers unleashed a large distributed denial of service (DDoS) attack on the servers of **Dyn**, a major DNS host.

Who did it?

This is the biggest question, and right now we do not have a solid answer yet. There were rumours online that the attack might have been state-sponsored, but an unnamed intelligence official said they have ruled that out, saying it was a "classic case of internet vandalism."

How was the attack done?

In order to understand how one DDoS attack could take out so many websites, you have to understand how Domain Name Servers (DNS) work. Basically, they act as the Internet's phone book and facilitate your request to go to a certain webpage and make sure you are taken to the right place. If the DNS provider that handles requests for Twitter is down, accessing Twitter will be next to impossible.

The attack was unprecedented. It utilized the Mirai botnet , made up of "internet of things" (IoT) devices (smart TVs, DVRs, and internet-connected cameras) to take down a major piece of internet infrastructure.

This attack was not your conventional DDoS attack. Instead, it seemed to be the first large-scale attack using IoT devices. Due to the estimated billions of available unsecured IoT devices, these attacks could allow for an unprecedented amount of DDoS power, which is enough power to take down major pieces of internet infrastructure protected by some of the best DDoS mitigation in the business.

What comes next?

Some of the devices used in this botnet against Dyn came from one Hangzhou Xiongmai, a Chinese manufacturer that creates parts for internet-connected webcams. Hangzhou Xiongmai devices were vulnerable because they didn't force users to change the passwords that connect the devices to the internet, leaving the devices with default passwords. This, in turn, allowed hackers to co-opt them.

It remains to be seen if this attack will be launched again, but there is no doubt that it inspired would-be hackers to build more botnet armies using the wealth of unsecured IoT devices and readily available malware. It is still unclear what mischief they are planning, but if hackers are able to make much of the internet unusable, say, once or twice a month, it will totally change how the web works.

Never before have key pieces of internet infrastructure been so vulnerable, and there is no doubt that other hackers will further exploit this vulnerability while it still lingers.

THE REIGN OF RANSOMWARE

Ransomware continues to grow at a prevalent rate . The number of new ransomware families seen in early 2016 alone has already eclipsed the total 2015 volume by 172%. With ransomware attacks becoming more and more sophisticated and prevalent, it is believed that the threat will potentially cause more damage going into 2017.

New ransomware families we detected exhibited both new propagation and extortion techniques. **JIGWAW** deletes encrypted files whenever victims fail to pay the ransom on the given deadline. Similarly, **SURPRISE** increases the ransom every time victims miss a deadline.

The ransomware families were designed to target specific business-related files. **SURPRISE** and **POWERWARE**, for example, have been used to encrypt tax return files.

Organizations minimise the risk of ransomware infections through virtual patching and investing in multilayered security solutions that leverage file, web, and email reputation. They should also educate their employees about the threat as well as the proper handling of suspicious emails and documents.

Growing Number of Vulnerabilities Found In Adobe Flash Player and IoT

Discovered by Trend Micro (In partnership with TippingPoint)		Discovered through the Zero Day Initiative	
Product	#CVE	Product	#CVE
Adobe Flash	28	Web Access	108
Android	11	Adobe Reader DC	26
OS X	11	Storage Resource Monitor Profiler Module	24
iOS	8	Foxit Reader	23
Microsoft Office	5	Internet Explorer	22
Internet Explorer	3	Adobe Acrobat Pro DC	19
Qualcomm	1	OS X	17
Apache Active MQ	1	Application Testing Suite	15
ffmpeg	1	LeviStudio	14
Edge	1	Edge	13

The number of vulnerabilities found in Adobe Flash Player can be attributed to the number of attempted zero-day and ransomware attacks targeting the platform. Earlier this year there were a few zero-day attacks from the Magnitude Exploit Kit that targeted the vulnerability (CVE-2016-1019) found in some versions of Adobe Flash Players. The exploit kit that incorporated the said vulnerability to its code had been able to leave systems affected with ransomware.

The use of Adobe Flash Player vulnerabilities for zero-day attacks has been going on for a while now and is likely to continue in the future. Last year, there were several zero-day attacks abusing Adobe Flash Player vulnerabilities. One involved a zero-day attack using the Angler Exploit Kit for malvertisements, then another allowed attackers to control the affected system, while one more Adobe Flash zero-day exploit was used by attackers behind Pawn Storm, a ongoing campaign which targets several key figures around the world.

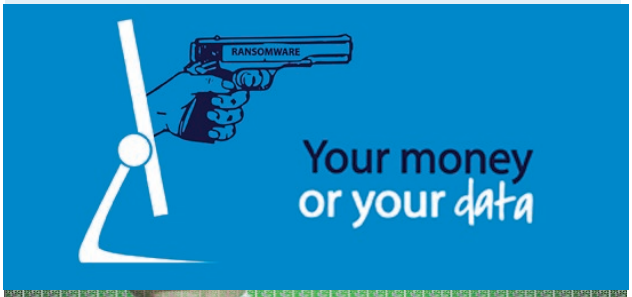
Other notable vulnerabilities were found earlier this year. Aside from the zero-day exploits using Adobe Flash Player, there were 21 new vulnerabilities discovered during the 2016 Pwn2Own competition, a yearly vulnerability research competition attended by a lot of security researchers around the globe. There were also six browser vulnerabilities and six kernel vulnerabilities that were unveiled during the event:

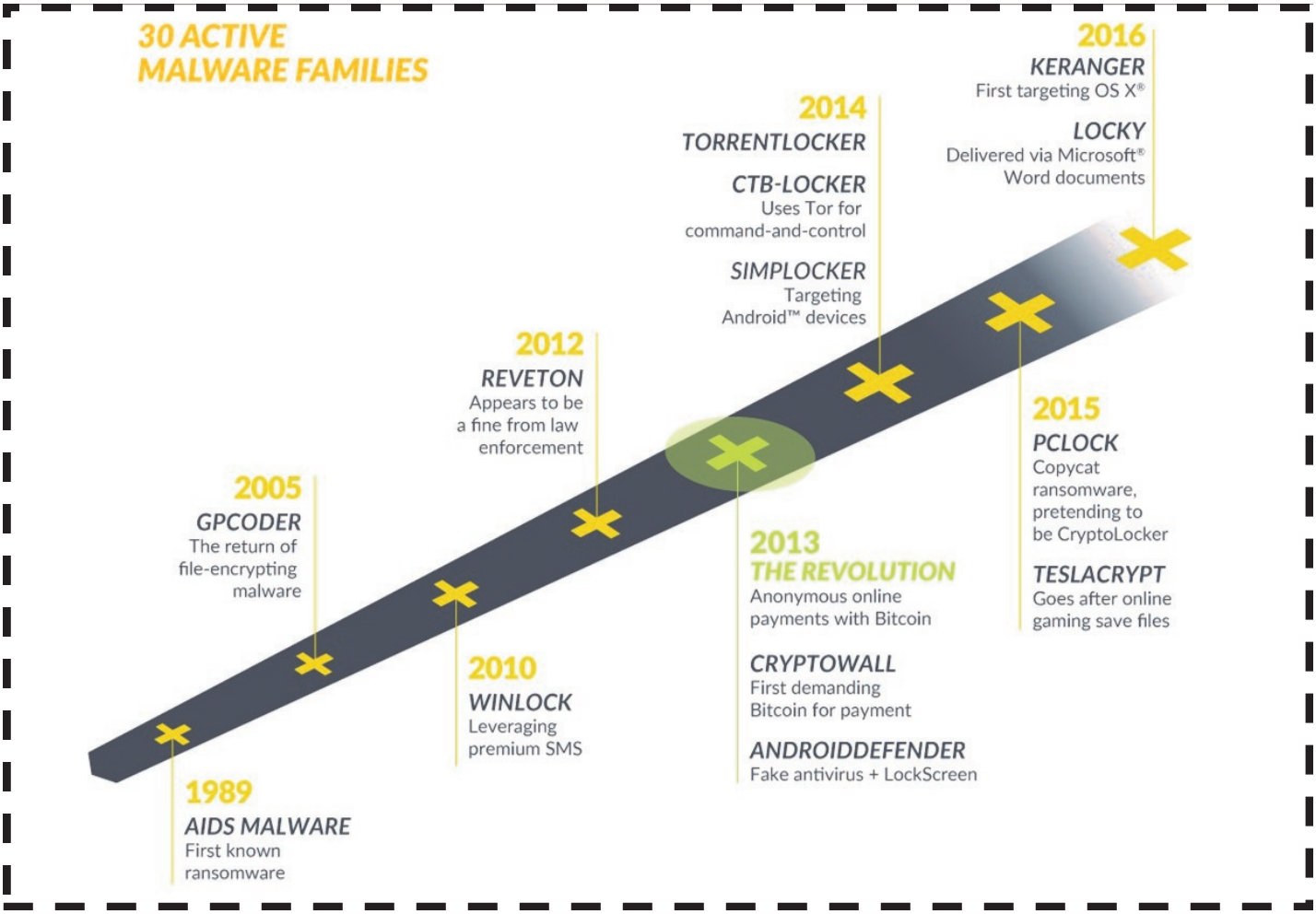
Microsoft Windows: 6
Apple OS X: 5
Adobe Flash: 4
Apple Safari: 3
Microsoft Edge: 2
Google Chrome: 1

As the race to either secure or abuse vulnerabilities continues among security researchers and malicious actors, it is crucial for the security industry and enterprises in general to try to deal with vulnerabilities as systematically as possible.

Although keeping abreast of the latest vulnerabilties may not entirely stop cybercriminals from abusing vulnerabilities, it will, however, help enterprises be one step ahead and have solid protection for their network, even against vulnerabilities that haven't been discovered yet.

For the times that software vendors haven't released an official patch or perhaps decide to discontinue support for a particular program, enterprises must put to use virtual patching solutions that are capable of providing strong and efficient protection that will shield vulnerabilities from exploits. Using such security filters allows organizations to take control of their systems without fear of becoming a victim to damaging attacks. In addition, solutions that provide diligent and timely updates of critical vulnerabilities found in the wild will also provide another layer of defense to enterprises.





Ransomware Is Not a "Malware Problem" – It's a Criminal Business Model

1. More Platforms

Ransomware has already moved from Windows to Android devices and, in one case, targeted Mac OS X. No system is immune to attack, and any device that an attacker can hold for ransom will be a target in the future.

This concept will become even more applicable with the growth of the "Internet of Things" (IoT). While an attacker may be able to compromise an Internet-connected refrigerator, it would be challenging to turn that infection into a revenue stream. But the ransomware business model can be applied in this or any other case where the attacker can achieve all five steps for a successful ransomware attack. After infecting the refrigerator, the attacker could remotely disable the cooling system and only re-enable it after the victim has made a small payment.

2. Higher Ransoms

The majority of single-system ransomware attacks charge a ransom between $200 and $500, but the values can be much higher. If attackers are able to determine that they have compromised a system which stores valuable information, and that infected organization has a higher ability to pay, they will increase their ransoms accordingly. There have been a number of high-profile ransomware attacks against hospitals this year, where the ransoms paid were well over $10,000.

3. Targeted Ransom Attacks

A targeted intrusion into a network is valuable to an attacker in many ways. Selling or acting on stolen information is a common technique, but it often requires additional "back-end" infrastructure and planning to turn that information into cash. Targeted ransomware attacks are an alternative for attackers who may not know how else to monetize their intrusion. Once inside a network, attackers can identify high-value files, databases, and backup systems and then encrypt all of the data at one time. These attacks, using the SamSa malware, have already been identified in the wild and proven lucrative for the adversaries conducting them.

WHY BLOCKCHAIN WILL EXPLODE NEXT YEAR

Blockchain is the form of technology and data structure that underlies the digital currency, Bitcoin. It acts as a public archive for all transactions and originated in early 2008. In other words, it is a large ledger that keeps a record of Bitcoin transactions.

As financial institutions and corporates face increasing challenges in data management, regulation and security, Blockchain has begun to emerge as the solution to verify transactions on a central network that excludes authority.

1. Better Regulation

Banking regulations have hindered the activities of European and American financial institutions since their rise to dominance. Blockchain acts with no trusted third party and therefore provides a more efficient process than investment bankers can offer. Regulators are showing an increasing interest in the activities of blockchain businesses and can provide real-time monitoring and financial advisory.

Since the introduction of BitLicenses, two have been awarded to Ripple Labs and Circle Internet Financial. This could also provide benefits to compliance departments as blockchain draws upon many data sources.

2. Fraud Minimisation

A growing number of financial institutions and corporates are looking into Blockchain after the security breaches seen in 2016 revealed the potential limitations of previous methods. Yahoo recently saw 500 million accounts stolen, and JP Morgan Chase last year had 83 million accounts compromised. Blockchain reduces counterparty risk as there is no need to trust a third party as agreements are codified and shared in an unalterable environment.

3. Simplification

Blockchain eliminates the manual processes that are required to perform reconciliation and to resolve disputes. This is hugely advantageous to trade financing but could see the number of traders reduced. Blockchain conversely could lead to a significant number of job reduction.

4. Blockchain Start-Ups

There has been a sharp increase in the number of start-ups, notably in Silicon Valley, that are innovating new applications for the blockchain technology. Venture capitalists have invested substantial sums in these corporates. This investment has led to an increase in 2nd and 3rd generation applications.

5. Central Banks And Governments

Blockchain has 40 experimental users that are key financial institutions, and many companies are progressing towards the transfer to safely manage the ownership of assets without the threat of fraud. The UK Government are seriously considering implementing the digital archive for their transactions.

6. Increased Liquidity

The technology archive condenses locked-in capital and offers transparency into locating liquidity for assets. Therefore blockchain provides opportunities for asset allocation enabling improved risk evaluation and decision-making. JP Morgan and PwC have both recommended blockchain as an "opportunity" for asset managers.

7. Shorter Times

Blockchain enables the near-real-time direct transfer of funds between financial institutions by removing obstacles and accelerating clearing.

The World Economic Forum detailed that Blockchain technology will become "the beating heart of finance" due to its simplicity and efficiency. One day, this technology could replace the need for banks altogether.

HOW EXACTLY DOES BLOCKCHAIN WORK?

Blockchain remains in the experimental phase inside many large firms and there are few tested use cases, experts and analysts caution. Here's a look at how this emerging technology works:

A blockchain is a data structure that makes it possible to create a digital ledger of transactions and share it among a distributed network of computers. It uses cryptography to allow each participant on the network to manipulate the ledger in a secure way without the need for a central authority.

Once a block of data is recorded on the blockchain ledger, it's extremely difficult to change or remove. When someone wants to add to it, participants in the network, all of which have copies of the existing blockchain , run algorithms to evaluate and verify the proposed transaction. If a majority of nodes agree that the transaction looks valid , that is, identifying information matches the blockchain's history, then the new transaction will be approved and a new block added to the chain.

The term blockchain today usually describes a version of this distributed ledger structure and distributed consensus process. There are different blockchain configurations that use different consensus mechanisms, depending on the type and size of the network and the use case of a particular company. The bitcoin blockchain, for example, is public and without "permissions", meaning anyone can participate and contribute to the ledger. Many firms also are exploring private or "permissioned" blockchains whose network is made up only of known participants. Each of these blockchain implementations operate in different ways.

Assume an organization has 10 transactions per second. Each of those transactions receives its own digital signature. Using a tree structure, those signatures are combined and given a single digital fingerprint, a unique representation of those transactions at a specific time. That fingerprint is sent up the tree to the next layer of infrastructure, such as a service provider or telecom company. This process happens for every organization in the network until there is a single digital fingerprint that encompasses all the transactions as they existed during that particular second. Once validated, that fingerprint is stored in a blockchain that all the participants can see. A copy of that ledger is also sent back to each organization to store locally. Those signatures can be continuously verified against what is in the blockchain, giving companies a way to monitor the state and integrity of a particular asset or transaction.

Anytime a change to data or an asset is proposed, a new, unique digital fingerprint is created. That fingerprint is sent to each client node for validation. If the fingerprints don't match, or if the change to the data doesn't fit with the network's agreed-upon rules, the transaction may not be validated. This setup means the entire network, rather than a central authority, is responsible for ensuring the validity of each transaction.

Blockchain's challenges

One obstacle to widespread enterprise adoption of blockchain technology is the need to get the network of participants, all of which have their own mix of back-office systems, to agree on a common network protocol and technology stack.

There are not yet clear standards to govern how blockchain will be implemented across the enterprise. Some companies may choose to use the bitcoin network, while others may opt for "permissioned" or semi-private blockchains. The development of the technology also will bring its own regulatory hurdles and potential cybersecurity threats.

Many questions around security and privacy still linger. In financial services, for example, it's still unclear exactly how much information about a trade each participant needs to be able to see to verify a transaction while still keeping the contents of a particular trade private.

CERT-MU CALENDER OF EVENTS 2016 - 2017

Computer Security Day 2016

CERT-MU has organised the annual CSD on 30 November 2016 at the Conference Hall, Cyber Tower 1, Ebene. The objective of the event was to raise awareness and promote best practices in Information Security and was targeted towards IT Professionals, System Administrators, Network & Database Administrators and IT Security Professionals.

The cyber security conference was officially opened by the Hon. Etienne Sinatambou, Minister of Technology, Communication and Innovation.

Technical Colloquium 2016

CERT-MU in collaboration with the Forum for Incident Response and Security Teams (FIRST) has organised a 3-day Technical Colloquium from 22-24 November 2016.

FIRST Technical Colloquia (TCs) provide a discussion forum for FIRST members and invited guests, including local organisations to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams.

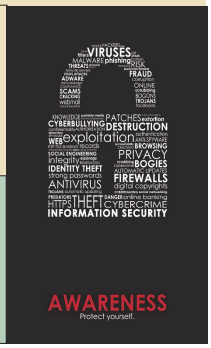
The TC event was open to FIRST members and invited guests. Some 90 people attended the event.

Cyber Security Drill 2017

CERT-MU is planning to organise a National Cyber Security Drill with the support of the International Telecommunications Union (ITU) tentatively during the month of September 2017. The Drill will target both public and private organisations.

The event will be dedicated to a series of workshops on current cybersecurity issues, followed by 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 capacity building sessions. IT professionals, system administrators, law enforcement officers and IT security professionals will benefit from this drill.

22-Nov-16	23-Nov-16	24-Nov-16
TC	TC	TC
30-Nov-16	07-Feb-17	Sep-17
CSD	SID	DRILL



Safer Internet Day 2017

Safer Internet Day (SID) is an international education and awareness-raising effort spanning more than 100 countries around the globe to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people.

A half day workshop in collaboration with the Ministry of Information Communication and Telecommunication and the Ministry of Education and Human Resources is planned on 7 February 2017 around the theme 'Be the change: unite for a better internet". The workshop will be targeted towards State and Private secondary school students to sensitize them on the impact of threats and consequences that improper use of the Internet may have on the youth.

SECURITY GUIDELINES & TIPS

LATEST GUIDELINES

Guideline on Mobile Payment Security

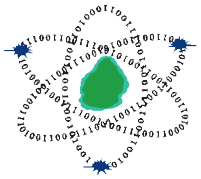
The purpose of this document is to educate users on the secure use of mobile devices when using such devices for payment.

Guideline on IT security for Academic Institutions

This document provides an overview of how academic institutions should manage network security, often referred to as cyber-security or e-security.

Cyber Security Guidelines for Employers and Employees

The purpose of this document is to give employers and employees some guidelines as to what precautions they should take on the Internet at their place of work.



CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudrière 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