TONGA CERT CASE STUDY

Presented by: Andrew Toimoana

OUTLINE

* About Tonga
* About Tonga National CERT
* Mandates and Procedures
* CERT Experience (Proactive and Reactive initiatives)
* From the Courts

About Tonga.

Total number of Islands	• 177 Islands
Total number of inhabited Islands	• 52 Islands
Total Population	• 103,252
Total land area:	• 750 Sq Kms

Fibre Optic Submarine Cable

* Submarine Fibre Optic was launched in August 2013
* One of the Tools to support economic and social developments of Tonga
* IT brings enormous benefits and open up opportunities
* This tool can be very dangerous if we cannot monitor and use it for the right purposes.

Cyber Challenges Task Force

* Cabinet approved the establishment of the Cyber Challenges Task Force in December 13th 2013,
* Cyber Challenges Task Force provides quarterly report to Cabinet.
* One of the mandates of the Cyber Challenges Task Force under its Terms of Reference was technical assistance which entailed the setting up of a Tonga Computer Emergency Response Team (CERT).

Acknowledgement

* In preparation, Tonga CERT engaged in difference training activities from different organization such as:
  * The Council of Europe
  * Sri Lanka CERT
  * Mauritius CERT
  * APNIC – Tonga CERT Technical advisor
  * Australian CERT
* With the assistant from APNIC, Tonga CERT was officially launch in July 2016.

Current procedures

CERT MANDATE:

1. PROACTIVE - AWARENESS/BULLETIN
2. RE-ACTIVE - INCIDENT HANDLING
3. FORENSIC /ADVISE* Record Keeping* Storage - Secured* Tool Kit- Mobile devices- Imaging -> Examine -> Analyse- Court Presentation - Expert Evidence- Verification Procedures

Procedure on receipt of report/complaint

1. Receipt of complaint / Report
2. 2. Summary of Fact (SOF) - Put this brief in template form. - date of receipt - Facts –
   * (Classification, Solution Option and Work to be done - Timeframe / Police involvement)
   * a. Approved b. Denied
     * Discuss Work done* Details* Consider Report Number
3. CERT.to Report to (REPORTING AGENCIES)
   * Internal agency - MEIDECC, CERT Board

Procedure on receipt of report/complaint

* SOPs are currently revised
  * Aim to reflect experiences and recommended solutions to challenges faced by CERT since initial drafting of SOP (more theoretical as opposed to based on concrete studies)
* MOU with 3 of the main Service Providers on Information Sharing and technical supports.

RE-ACTIVE - INCIDENT HANDLING
Ongoing work Case

* Case regarding letter alleged to have been written by a high government official which may be considered treason
  * Reported to Police, Police sought CERT assistance. Investigation is still ongoing with very little progress in terms of identifying culprit.

New Proactive initiatives

* Capacity building in Network security
  * Working together with the service providers (APNOC)
* Working with Anti-phishing Working Group (APWG)
  * Signed MOU and launching of the National stopthinkconnect website (www.stopthinkconnect.gov.to)
* Microsoft VIRTUAL SCHOOL OF GOVERNANCE (SOG)
* 24Microsoft Digital Crimes Unit (DCU)
  * A team of legal and technical experts who work to make the digital world safer
  * DCU identifies, investigates and disrupts malware, particularly by taking down botnet command and control infrastructure used by criminals.

Malware Microsoft

Trojan

Bladabindi
Citadel
Sirefef

Financial Worm

Conficker
Ramnit
Dorkbot

Cyber Threat Intelligence Program (CTIP)

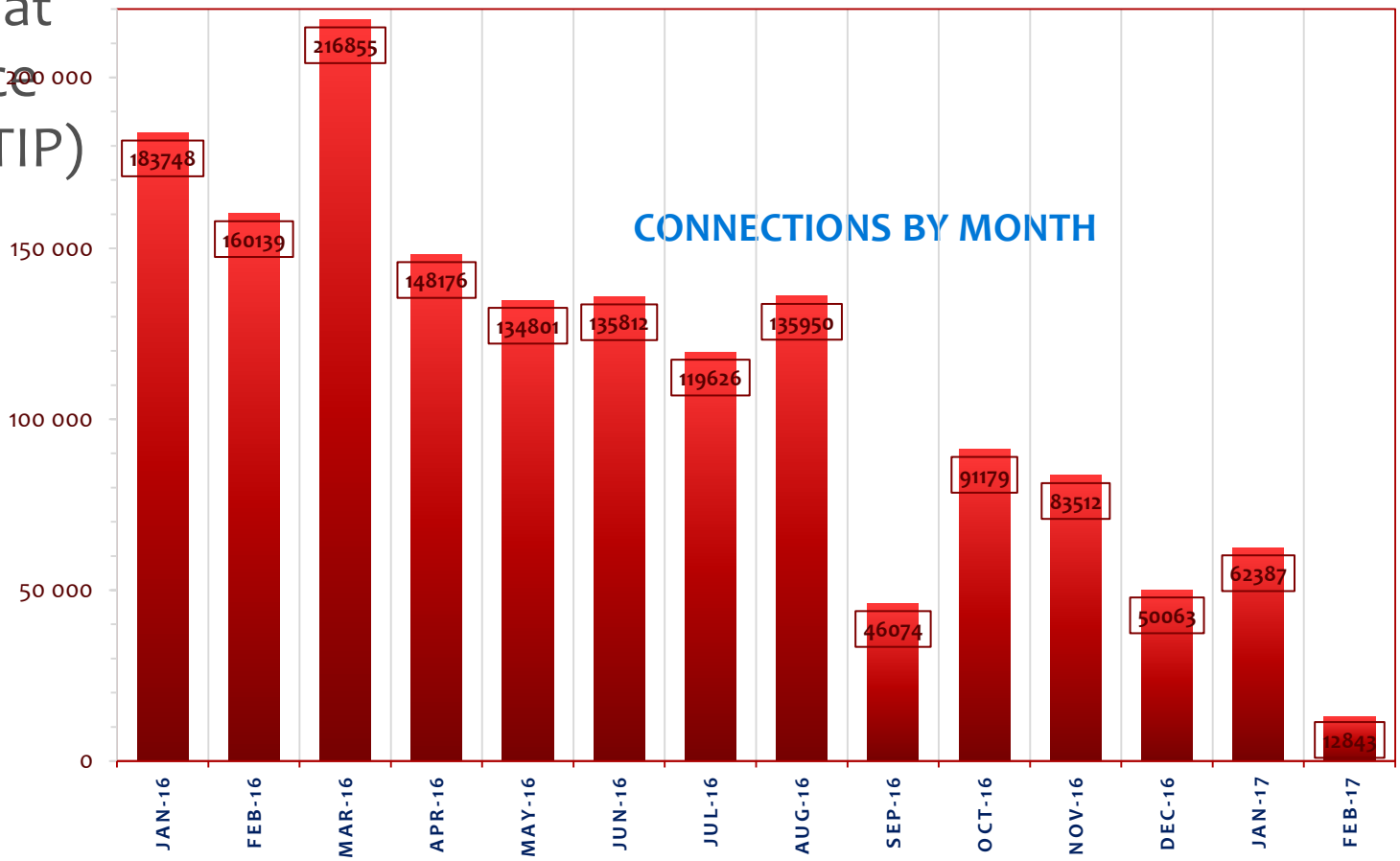
Threat Summary

Distinct IP addresses identified at DCU sinkhole: **1,739**

Number of connections with DCU Sinkhole: **1,581,165**

CTIP Period – Jan 2016 – Feb 2017 (**14 months**)

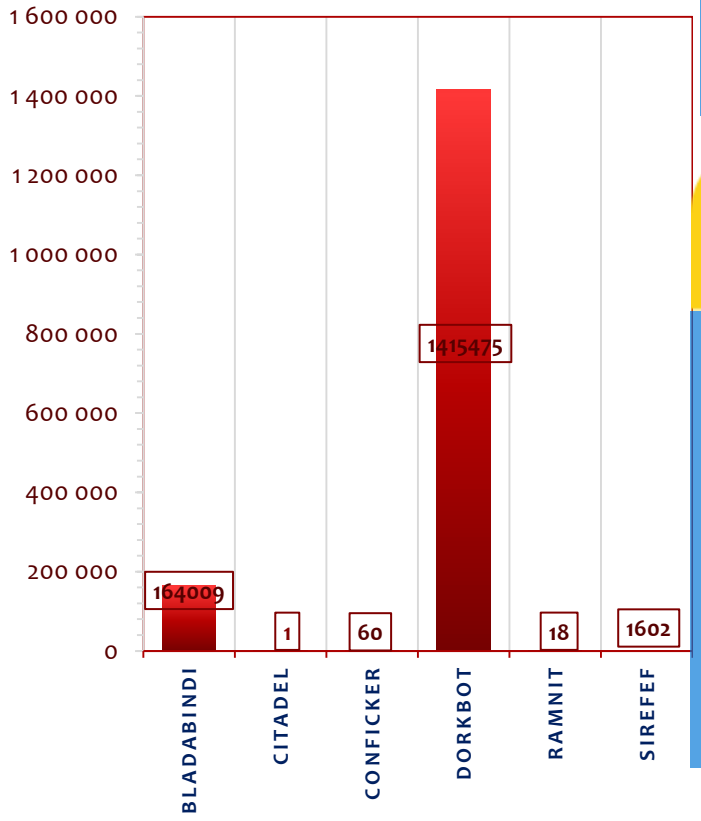
Number of Threat Groups: 6



Malware

Microsoft
Cyber Threat Intelligence
Program (CTIP)

Threat Summary



Financial Worm

Ramnit

- Steals sensitive information, such as login details & browser cookies
- Infects executable files, Microsoft Office Files & HTML Files
- Spreads via file infections, removable & network drives
- Running a full scan is advisable even if detected & cleaned

Financial Worm

Conficker

- Disables important security products
- Downloads files and runs malicious codes
- Infects PCs across a network
- Spreads via removable drives

Financial Worm

Dorkbot

- Steals user names & passwords
- Blocks websites related to Security updates
- Launches Denial of Service Attacks
- Spreads through USB, Instant Messaging Programs & Social Networks

Trojan

Citadel

- Stealthily logs any key strokes and transmits
- Steals Banking Credentials & Other Sensitive Information
- Initiates Continuous system slow downs, browser redirections
- Installs via spam mails & hacked websites

Trojan

Bladabindi

- Steals sensitive and confidential Info
- Downloads other Malware & gives backdoor access
- Disables automatically many of the antivirus applications, software, firewall and other security application
- Spreads via USB Flash drives

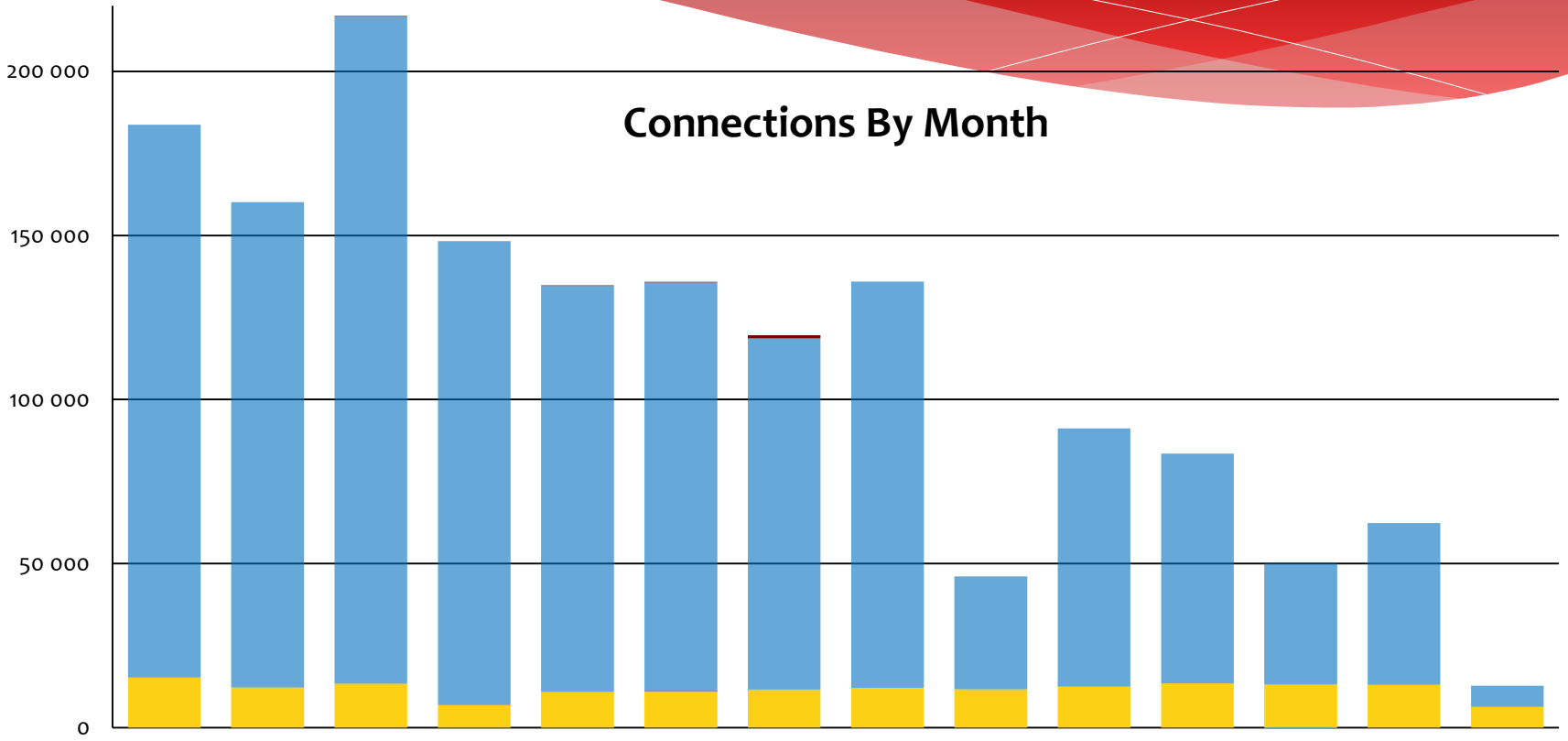
Trojan

Sirefef:

- Disables Security Features to hinder its detection and removal
- Moderates Internet experience by changing search results
- Downloads & runs unwanted files
- Comes packaged with other Malware

Microsoft Digital Crimes Unit

Malware Microsoft Cyber Threat Intelligence Program (CTIP) by Threat



	janv.-16	févr.-16	mars-16	avr.-16	mai-16	juin-16	juil.-16	août-16	sept.-16	oct.-16	nov.-16	déc.-16	janv.-17	févr.-17
Sirefef			184	74	190	167	987							
Dorkbot	168421	147890	203201	141232	123710	124474	107031	123800	34360	78606	70037	36922	49330	6461
Citadel						1								
Bladabindi	15327	12249	13470	6854	10899	11170	11608	12150	11714	12573	13475	13081	13057	6382
Conficker												60		
Ramnit				16	2									

FROM THE COURTS

- Cases heard by the Court reach it by way of prosecutions filed by Police or the DPP.
- Cases heard depend on the charges filed following investigations conducted by the Police

R v Potemani

* Accused approached over internet by a new Facebook friend
* Accused was asked to open a bank account
* Two deposits of TOP 21,000 and TOP 4,000 (12,500 USD)
* Instructions given to withdraw money and send to Facebook user – first to Singapore then to South Africa;
* Failed to send money due to Western Union requirements
* Attempted to purchase electronic goods and courier them to Facebook friend

R v Potemani

* Charges filed – receiving stolen property and money laundering
* Convicted on receiving stolen property; acquitted on Money Laundering charge as the predicate offence was not proved i.e. theft
* Court cited House of Lords decision regarding whether a debiting an account to credit another account in the bank amounts to theft. "True, it corresponded to debit entered into lending institution's bank account but it does not follow that the property which the defendant acquired can be identified with the property which the lending institution lost when account was debited."

R v Potemani

* In essence Supreme Court of Tonga decided that no theft was committed as is compliant with the offence of theft defined in legislation.
* Decision prompted amendment in legislation as to definition of **goods capable of being stolen** i.e.

  "(3) Money and all other property, real or personal, including things in action and other intangible property is capable of being stolen."

R v Kaumavae

Fraud and forgery

- Forgery – creation of a birth record for someone who does not exist with the intent of using it to issue a Tongan passport. The intended benefactor of the passport was a Tongan national living abroad.
- There is no reference in the judgment as to the cyber-enabled aspect of the charges.

Malo ‘Aupito

Thank

YOU

Funded by the European Union and the Council of Europe
Implemented by the Council of Europe
29-31 March 2017, Accra, GHANA