New Technologies Used In Cybercrime

Challenges with Investigation

Herbert Gustav Yankson
Chief Supt Of Police
Head, Cybercrime Unit
CID Headquarters, Accra
PRESENTATION OUTLINE

Ghana’s Digital Statistics

Cybercrime Landscape In Ghana

Prevalent Cybercrime Cases

The Ghana Cybercrime Statistic

The Challenges For Investigations

Conclusion
GHANA’S LOCATION
GHANA’S DIGITAL STATS

TOTAL POPULATION: 29.15 MILLION
URBANISATION: 56%

INTERNET USERS: 10.11 MILLION
PENETRATION: 35%

ACTIVE SOCIAL MEDIA USERS: 5.60 MILLION
PENETRATION: 19%

MOBILE SUBSCRIPTIONS: 34.57 MILLION
PENETRATION: 119%

ACTIVE MOBILE SOCIAL USERS: 4.90 MILLION
PENETRATION: 17%

SOURCE: Population data from UN, U.S. Census Bureau, and UNESCO. Internet users data from Internet World Stats, Facebook, and Google. Social media users data from Hootsuite and We Are Social. Mobile phone subscriptions data from GSMA. Mobile social users data from Hootsuite and We Are Social. Note: Penetration figures are for total population (all ages).
CYBER CRIME LANDSCAPE

- Cyber Fraud
- Advance Persistent Threat
- Phishing
- Hacking
- Data Breaches
- Spamming
- CrimeWare
- DDOS Attack/Botnet
- Charlatantic Advertisement
- Child Pornography
- Sextortion
- Publication of Fake News
PREVALENT CYBERCRIME CASES

- PHISHING AND SPEAR PHISHING
- CYBER FRAUD
- SEXTORTION
- RANSOMWARE
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims.

Phishing emails may contain links to websites that are infected with malware.
Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
SPEAR PHISHING

- Spear-phishing is a more targeted form of phishing.

- Whereas ordinary phishing involves malicious emails sent to any random email account, spear-phishing emails are designed to appear to come from someone the recipient knows and trust—such as a colleague, business manager or human resources department—and can include a subject line or content that is specifically tailored to the victim's known interests or industry.
Hello,

You have an important email from Human Resources Department with regards to updating your info for this month’s payroll. The email is enclosed on the secure server, please access it using the link below.

Access the documents here.

Helpfully,

Julie

Julie Monical
Director of Human Resources and Administration

Office: 888.883.2463
Direct: 657.229.7699
www.TechMD.com
BANK RELATED FRAUD

- BUSINESS EMAIL COMPROMISE
- SIM SWAP ASSISTED FRAUD
- ATM FRAUD
- INTERMEDIATE PLATFORM ASSISTED FRAUD
- CREDIT CARD FRAUD
- POS ASSISTED FRAUD
- CLONED CHEQUES FRAUD
A business email compromise (BEC) is an exploit in which the attacker gains access to a corporate email account and spoofs the owner's identity to defraud the company or its employees, customers or partners of money.
Business Email Compromise

• Account intercepted using social engineering
• Accounts intercepted using malware via phishing emails
• Using spoofed emails- they obtain a domain to mimic the targets email address
• Creating email address to mimic the email of the target using free Web-based e-mail service
  • smartamfo@yahoo.com ✔
  • smartarnfo@yahoo.com ✗
• Using anonymous remailer websites to create email address similar to that of their target
MOBILE MONEY FRAUD

SCHEMES EMPLOYED

- TELCO RAFFLES
- LONG SERVICE AWARD
- FALSE SMS
- SPIRITUAL
- SICK CHILD
- ROMANCE
- TRANSACTION REVERSAL
- POLICE ARREST
- IDENTITY THEFT
- ONLINE INVESTMENT
- BITCOIN INVESTMENT
- PEER TO PEER INVESTMENT
• Ransomware is a malware that targets your critical data and systems for the purpose of extortion
• Victim’s computer is infected with malware
• Malware encrypts the victim’s data and/or computer making them unreadable
• Attacker demands a ransom before the files/system/network is decrypted
• Payment is usually demanded through Bitcoins
• Ransomware is frequently delivered through spear phishing e-mails
RANSOMWARE

Deployment models
Recent wannacry attacks targeted organization, government and end users, making awareness and training a critical preventive measure.

Wannacry is a ransomware CRYPTOWORM, which targets computers running the Microsoft Windows operating system that have not been updated with recent security updates.

Global impact – victims spread over around 200 countries

Maximum diffusion – The malicious code is automatically copied onto each PC in the same network who presents the same vulnerability.
WANNACRY RANSOMWARE
Sextortion is a form of sexual exploitation that employs non-physical forms of coercion to extort sexual favors from the victim.

Sextortion also refers to a form of blackmail in which sexual information or images are used to extort sexual favors, money or information from their victim.
SEXTORTION

How images and videos are acquired

• Relationship-freewill sharing (mostly with unknown partners online) and through secret recording during video chat
• Phone repairers
• Seeking help from technologically savvy friends
• WhatsApp web and other forms of intrusion methods
• Loosing digital devices through stealing or any other means particularly with no security
• Improper Idle time setting
• Cracking passwords
• Use of female criminal syndicate
PERCENTAGE OF CASES REPORTED AT THE CYBERCRIME UNIT FOR THE YEAR 2016
<table>
<thead>
<tr>
<th>OFFENCES</th>
<th>AMOUNT DEFRAUDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOBILE MONEY FRAUD</td>
<td>$22,692</td>
</tr>
<tr>
<td>ATM FRAUD</td>
<td>$35,360</td>
</tr>
<tr>
<td>REMITTANCE FRAUD</td>
<td>$96,168</td>
</tr>
<tr>
<td>SOCIAL MEDIA FRAUD</td>
<td>$1,236,930</td>
</tr>
<tr>
<td>BUSINESS EMAIL COMPROMISE</td>
<td>$8,439,876</td>
</tr>
<tr>
<td>CYBER FRAUD</td>
<td>$25,810,394</td>
</tr>
<tr>
<td>SEXTORTION</td>
<td>$48,000</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$35,689,420</strong></td>
</tr>
</tbody>
</table>
Cases Received at Cybercrime Unit in the year 2017

SAKAWA FRAUD: 140 cases
BUSINESS EMAIL COMPROMISE: 70 cases
REMITTANCE FRAUD: 60 cases
FORGERY OF DOCUMENT: 50 cases
MOBILE MONEY FRAUD: 30 cases
SOCIAL MEDIA PERSONATION: 20 cases
THREAT OF DEATH: 10 cases
THREAT OF HARM: 8 cases
FAILURE TO REGISTER: 5 cases
GHOSTS AND VAMPIRES ADVERTISEMENT: 4 cases
SEXORTION: 3 cases
RECRUITMENT SCAM: 2 cases
STEALING: 2 cases
ISSUE OF FALSE CHEQUE: 1 case
CLONED WEBSITE: 1 case
COPYRIGHT INFRINGEMENT: 1 case
CREDIT CARD SCAM: 1 case
Graph Showing Types of Cases and Amount Lost to Criminals($) for the Year 2017
<table>
<thead>
<tr>
<th>Type of Case</th>
<th>Amount ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sakawa Fraud</td>
<td>35,382,198</td>
</tr>
<tr>
<td>Business Email Compromise Fraud</td>
<td>2,820,475</td>
</tr>
<tr>
<td>Remittance Fraud</td>
<td>73,067</td>
</tr>
<tr>
<td>Mobile Money Fraud</td>
<td>21,357</td>
</tr>
<tr>
<td>Social Media Personation Fraud</td>
<td>22,027</td>
</tr>
<tr>
<td>Sextortion Fraud</td>
<td>11,552</td>
</tr>
<tr>
<td>Recruitment Scam</td>
<td>806,139</td>
</tr>
<tr>
<td>Stealing</td>
<td>30,080,684</td>
</tr>
<tr>
<td>Issue of False Cheque</td>
<td>7,469</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>9,118</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>69,234,085</strong></td>
</tr>
</tbody>
</table>
Global Nature - Multiple territorial connections

- The **action of the criminals reach computers and victims in countries other than their countries**

- Evidence may be found in different jurisdictions
  - Gmail/Yahoo Webmails

- National law enforcement agencies are limited to their geographical borders while criminals have unlimited borders?
  - International assistance in criminal investigations require proper legal channels?
  - Mutual legal assistance Treaty (MLAT) Required
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

• Evidence is volatile

• States, citizens and economies depend internet creating heavy network traffic and huge amounts of data generated. Data is easily overwritten as result.

• Security vs. business challenge (collaborating with Telecommunication companies)
Investigation units are understaffed and not adequately trained/ skilled

• Increasing number of cases which makes investigators ineffective

• Huge backlog of computers to be examined

• Understanding changing Modus Operandi and knowing what evidence to collect

• Investigations into possible forms of Organized Crime vs. Single criminal
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

Coping with new technological paradigms

New illegal activities are being “invented” everyday

Hacking as a service
- Outsourcing of a complete cyber-enabled attack
- Technical support for cybercrime activities

Crimeware as a service
- Sophisticated exploit kits and other malware for rent
- Development of malware for niche markets

Research-as-a-service
- Legal or illegal collection of information on victims
- Resale of stolen personal data or email addresses

Infrastructure as a service
- Hosting of malware on secure networks
- Rental of established botnets for Distributed Denial-of-Services
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

Coping with new technological paradigm
Coping with new technological paradigms

- TOR Networks provides anonymity and privacy by shielding them from LEA
- Darkweb refers to websites on a darknet
Coping with new technological paradigms

• Cloud Computing – “Evidence in the Cloud

• Cryptocurrency provides anonymous transaction eg Bitcoin
  • Digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
  • Monies obtain through crime are laundered through bitcoins

• Anonymous remailers help spoof email
  • An anonymous remailer is specialized kind of mail server designed to send e-mail messages without identifying the sender. Many of them are provided as a free service.
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

Coping with new technological paradigms

• Use of technology including VPN and Proxy poses a challenge

  • A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.

  • A proxy or proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the proxy server which then processes your request and returns what you were wanting.
Coping with new technological paradigm

- **IoT – Internet of things**
  - Every device is connected to the Internet and addressable via its’ own IP address
  - Devices communicate with their owners and with each others

- **Challenges**
  - These devices become targets because the product have security vulnerabilities.
  - Many of these devices are compromised and used as be used as botnets

- **Technical knowledge** is required to investigate such cases hence difficult for an average investigator
• **Instant Messaging and Social Networking site** have taken over as the communications tool of choice in recent years with many well known examples providing instant and user friendly access by the use of encryption technology which reduce the chances of detection

• Request for Content requires MLAT which takes months/year
ENCRYPTION CHALLENGE

The intentional storage of information in encrypted form on devices of victims, witnesses or suspects.
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

ENCRYPTION CHALLENGE

Volume Type

- **Standard VeraCrypt volume**
  Select this option if you want to create a normal VeraCrypt volume.

- **Hidden VeraCrypt volume**
  It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

  More information about hidden volumes
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

**Limited technical capabilities** to support a successful investigation
- Digital forensics laboratories outdated
- Malware forensics and reverse engineering capacities
- Collaboration with local telecommunication service providers (understanding their operation)

**International cooperation**
- Police to Police
- International Judicial Cooperation
- Interactions with international large service providers (Social Networks, etc.)
CHALLENGES WITH CYBERCRIME INVESTIGATIONS

• Different countries with different cultures, with different legal tradition and different criminal law frameworks see these criminal activities different

• Cybercrime legislation – Harmonization
  Definition of cybercrimes
  Where was Crime Committed? Which Country has jurisdiction?
  Need to adopt global standards, International Treaties

• Lack of common understanding on cybercrime amongst the criminal justice authorities
CONCLUSION

• Requires local and international Collaboration

• Comprehensive programme to train all Law Enforcement Officer, Prosecutors and Judges.

• Technical Capacity Built

• Increase Awareness Creation

• International legal instrument required

• Strengthen our laws to be in harmony with international Legal Instrument