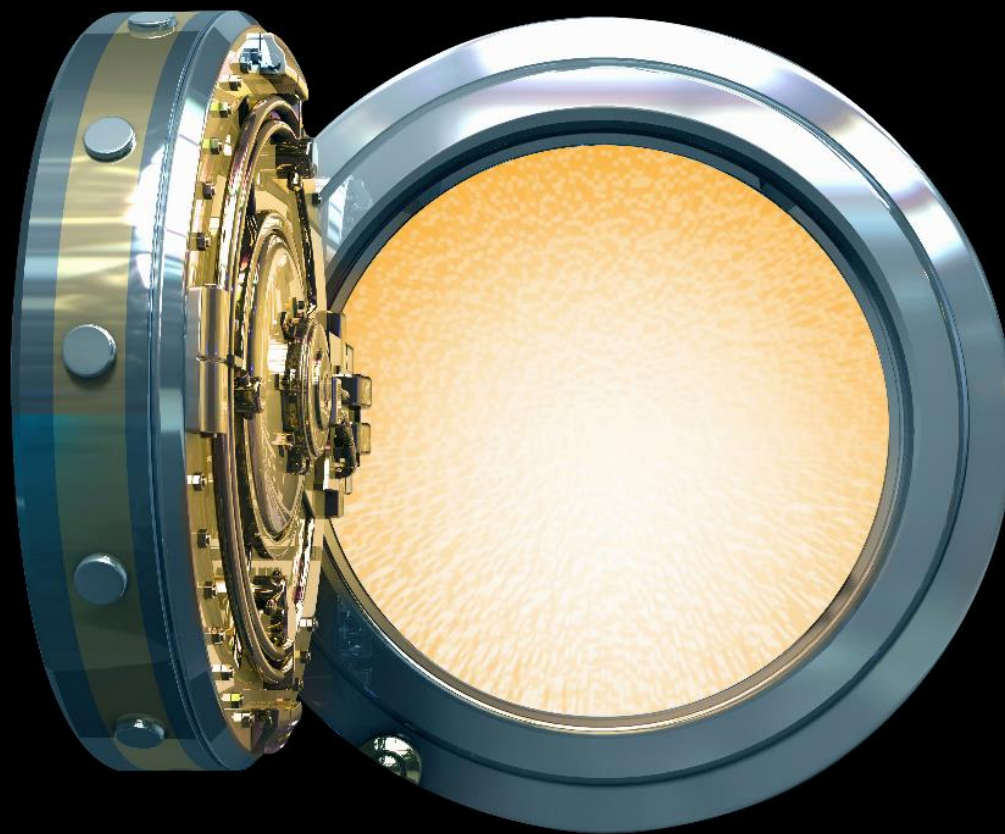


**Deloitte.**



**Fraud Awareness Seminar**  
From Princes to MuddyWater



## Lucas Chiloane

- Senior Manager – Risk Advisory
- Cyber Forensics



## Emmanuel Adigun

- Senior Manager – Risk Advisory
- Vulnerability Management (Ethical hacking)



# What is Cyber Crime



*Cyber crime*



Cyber crime – A crime or other offence committed through the use of the Internet aided by electronic communications/systems and/or devices. It is any criminal activity involving computers and networks.

## Traditional Criminal Vs. Cybercriminal

### Traditional Criminal

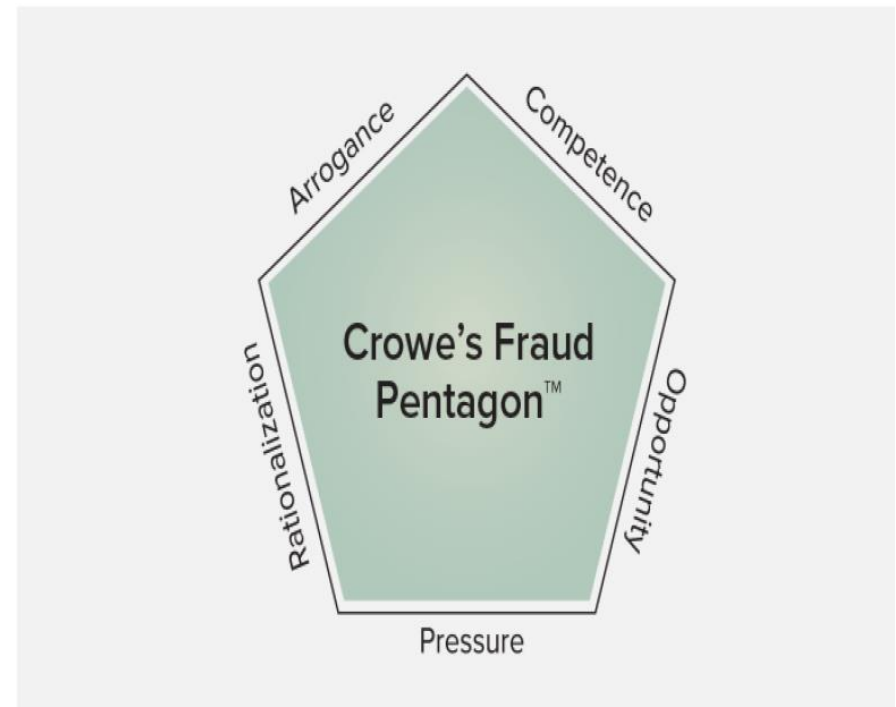
- Somewhat predictable
- Bound to specific location
- Paper trail
- Set motive
- ID

### Cybercriminal

- Could be anywhere
- No profile
- Bits and Bytes
- Unpredictable
- Volatile
- IP
- Open source



## Traditional Criminal Vs. Cybercriminal





# Cyber Crime

## Cyber Crime - Forms/Techniques



**Cyber  
Terrorism**

**Identity Theft**

**Espionage**

**Cyberattack**

**Cyber  
Bullying**

**Hacking**

**Fake Mobile  
Apps**

**Piracy**

**Phishing/  
Vishing**

**Crimeware**

**Cyber-  
squatting**

**Ransomware**

**Extortion**

**Social  
Engineering**

**Web  
Jacking/  
Hoax Email**

**Pharming**

**DDoS**

**Fake Job  
Offers**

**Salami  
Slicing**

**Cryptomining**



# Cyber Crime


## The Dark/Deep Web – Things that can be found...



### Assault Weapons

Showing all 6 results

Sort by popularity



IWI TAVOR SAR IDF Model  
\$1,850.00

Colt M4  
\$1,260.00

IWI G  
\$1,550.00

GAP2  
\$1,550.00

**Escrow Highly Sold** 1 oxy 60mg super sale !!!!! (5 left at this price)  
**\$17 / 0.013546 BTC**  
 Vendor: [View Listings] Ricky Spanish69 **+70, -0, 100%**  
 Category: Oxycodon  
 Ships From: Not Specified

**Escrow** 7G Early Skunk - UK  
**\$80 / 0.063745 BTC**

[View Listings] DS90 **+2115, -8, 100%** Level 3 ★★★ PGP Verified

pecified

MILL. BOTTLE LIQUID METHADONE  
 C

[View Listings] drjamesshu **+125, -0, 100%** Level 1 ★ PGP Verified

one  
 specified

id 2.0 Grams \*SAMPLE\* of High Quality Moroccan Pollen  
 C

[View Listings] Nextdaysmoke **+185, -0, 100%** Level 1 ★

Category: Hash  
 Ships From: United Kingdom

### Counterfeit 50 Euro Bills



Our notes are produced of co  
 incorporated, so they pass the  
 spent at most retailers.  
**FREE EXPRESS SHIPPING!**



Norway D

Denmark

Netherlands Drivers License 1150 EUR = 2.065 B

UK Drivers License 1000 EUR = 1.796 B

1 X [Buy now](#)

Intelligence acquisition  
(Sources)



**Categories:**

- Hosting
- Forums
- Private Sites
- Communication
- Hacking
- Libraries/Wikis
- Markets
- Link Lists
- Social
- Other
- Adult
- Security

**Hack Facebook Account** 419 143

Hack Facebook Account We hack Facebook accounts and we sell this service. Price per account: 0.1 BTC How does it works? Deposit 0.1 BTC to the address above and send us an e-mail to fbhackers@torbox3uiot6wchz.onion with the victim's facebook profile url (https://www.facebook.com/USERNAME). We will send you the account login info within 24 hours.

<http://facez25qzcuvu2t3.onion/> Online: GMT 2017-04-24 18:51:06  
50% up (last 7 days)

**HeLL Forum** 300 96

HeLL Reloaded is back!

<http://legionhidden4dqh4.onion> Online: GMT 2017-04-23  
50% up (last 7 days)

**Digital Gangster** 64

Hacking, DDOS, Social Engineering, Espionage, Malware Development.

**Personal scans & document**

HERE I GIVING OUT MIX OF PASSPORT SCANS  
TOGETHER 284 PERSONAL SCANS AND DOCUMENTS  
BETWEEN THEM ARE ALSO UTILITY BILLS, BANK STATEMENTS AND OTHER PERSONAL DOCUMENTS.  
SEE MY STORE FOR MORE TARGETED AND EVEN BETTER LOOKING SCANS \*WORLDWIDE\*

| Author  | Message   |
|---|---|
| <p><b>daveo</b> Offline</p> <p>★★</p> <p>Posts: 1<br/>Threads: 1<br/>Joined: 2017 Apr</p> | <p><b>Bank account info - how to?</b></p> <p>how do i sell bank account info?</p> |

**Anonymous DDoS Request**

**Description:**  
For all the target share and reason make the both attack groups to make all the people can join the #Ops  
Here we are Anonymous Team 4514

Respect The Citizens.  
Expect Us

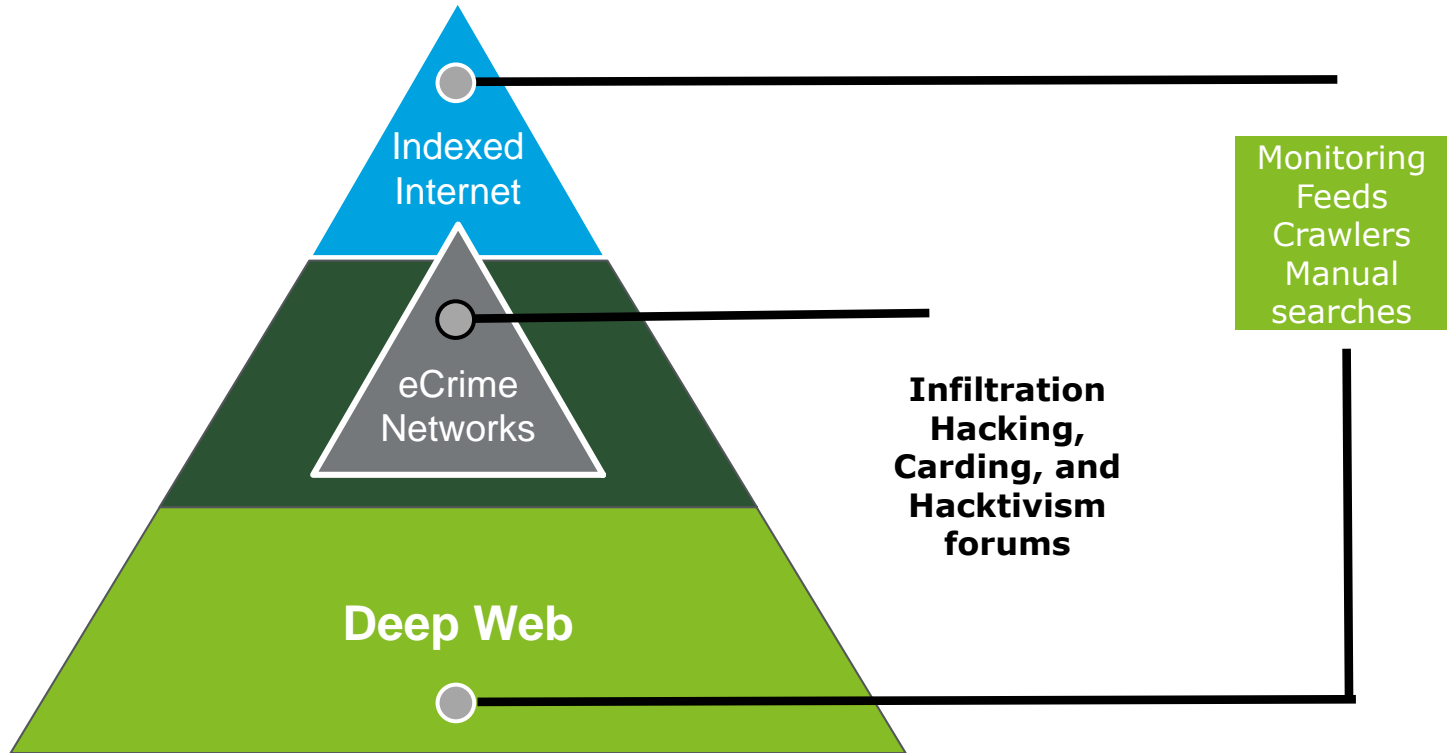
**Brief description:** DDoS Target share and always on the net Open Fire

**Tags:**  
#Anonymous, #DDoS, #4514

**Owner:** Messiah-T  
Group members: 82  
Open group

Intelligence acquisition  
(Sources)

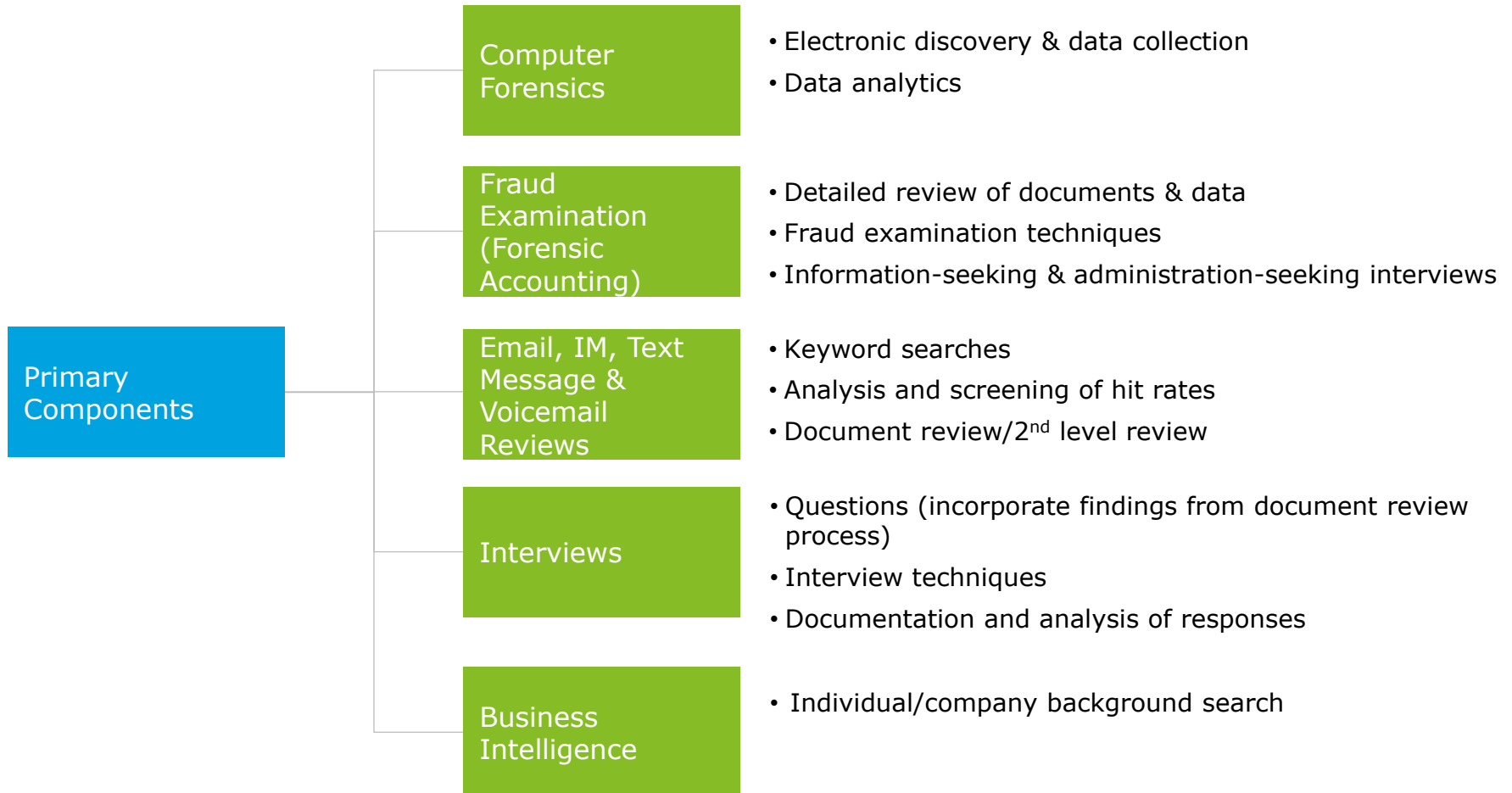


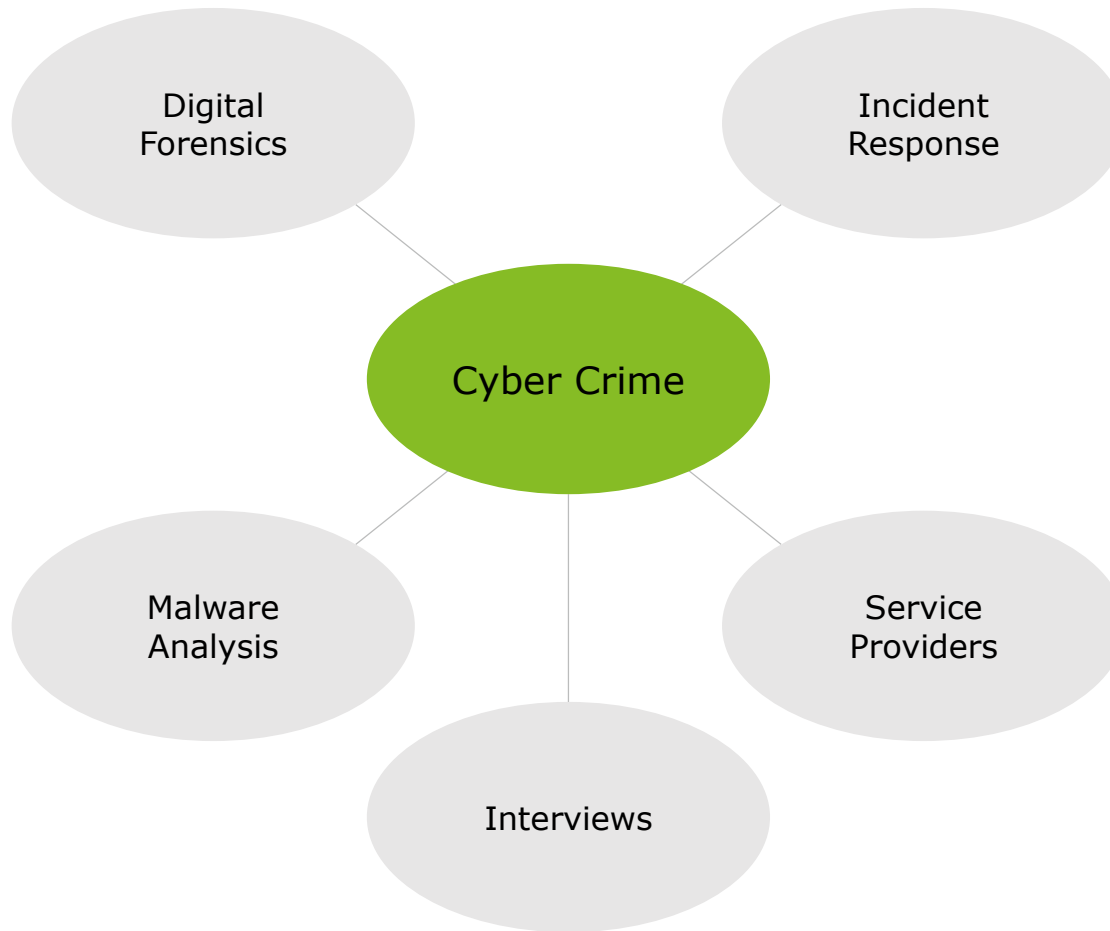


## The Dark/Deep Web



# Cyber Crime Typical Approach











# Cyber Crime

## Recent engagements



1



In early 2017, Deloitte Cyber Incident response (CIR) personnel was contacted by a software company to assist with ongoing incident response activities involving unusual behaviour detected on one of their servers.

As a result of this analysis, Deloitte was able to identify major points of interest regarding the timeline of a malware infection, portions of the communication activity initiated by the malware, and its general activities on the network.

Our analysis, based on the behavioural indicators from the malware analysis suggests that the malware packages appear to be relatively common and indicate that they were all related to a single hacker group named "legenda".

2



Deloitte assisted a major manufacturing client to investigate a case of fraudulent activity on their accounting system. Deloitte investigated the people, process and technology parts of the business.

By analysing system logs, we were able to identify access times and people involved in the fraud.

Deloitte was able to pinpoint the fraudulent activity to an employee within the client's organization



**Some wins...despite the challenges (Deloitte)**



**In September 2018, Deloitte investigated a ransomware infection at a major manufacturing client in SA via their subsidiary in the US**



## Ransomware Wannacry...Petya

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78nGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

DH3THk-J4uFvR-UJnTap-25P6W5-Ligtsd-KfBUou-AT8DLv-HRmxxq-PF2kdb-c5HHnC

If you already purchased your key, please enter it below.

Key: \_





Cryptomining





## Business Email Compromise



# Questions





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

This communication is for internal distribution and use only among personnel of Deloitte Touche Tohmatsu Limited, its member firms, and their related entities (collectively, the "Deloitte network"). None of the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited