The Threat of CYBER Attacks & Digital Forensics

Danny Myburgh - 2017
danny@cyanre.co.za
Hawks arrest Eskom employees in sting operation

Johannesburg - At least two Eskom employees have been arrested in connection with fraud that could have resulted in the power utility losing billions of rand, the Hawks said on Wednesday.

The Hawks, South Africa's Directorate for Priority Crime Investigation, have foiled an insider attempt to defraud the Gautrain Management Agency (GMA), potentially of millions of rand.

ITWeb understands an IT technician working at the GMA had come under scrutiny after suspicious behavior was detected during a security audit, leading to a lengthy investigation by the Hawks and culminating in the suspect's arrest today.

In a statement on the GMA's website, transport MEC Ismail Vadi thanked the Hawks for the "speedy arrest".

Ashley Madison hack list: South African details

Numbers from the Ashley Madison data dump give an idea of where South Africa's potential cheaters are from.

By Jan Vermeulen - August 21, 2015 32 Comments
According to MobiForge Report (2014) there is

- In 2014 276,7mil pc/ipt was sold, 270,7mil tablets, 1.8 bil mobile phones
• Everyday we send 108.7 billion (bil) e-mails, 2.8 bil Google searches, 144 mil tweets
• The average person receives and send 121 e-mails per day,
• 3.6 bil social media accounts in 2014
• Internet usage is growing by 10-15% yearly in SA
• The FBI already ranks SA 6/7th in its top 10 cyber crime perpetrators list. SA 23 most attacked
• 79% of Online victims in SA has some or none of their money back
• 52% of global Internet users becomes victims, 79% in SA
• $476 loss on average per incident in SA
• Distributed Denial of Service attacks (DDOS) increased Oct-Dec 2016 - attacks from Vietnam 22%, Russia 22%, China 21% Brazil 15% and USA 14% (Kaspersky Lab – IT Web 9 Feb 2017)
Threat Landscape

- Common Law Offences
- Employee
- 419 Scam
- Deposit Scams
- Accommodation scams
- Puppy Scams
- BYOD/BOYN
- Smishing
- Phishing
- Spear Phishing
- Code Injection
- Man in the Middle attack
- Session Hijacking
- Whaling
- Trojan
- Cyber Bullying
- Cyber Harassment
- ID Theft
- Black Hat
- Grey Hat
- Red Hat
- Cyber Terrorism
- Cyber Warfare
- Spyware
- Online mail hack
- Rasomeware
COMPUTER FORENSICS
Evidence Principles

**Principle 1** - No action taken by the Investigator should change the data. Where possible computer data must be ‘copied’ and that version examined.

**Principle 2** - In exceptional circumstances it maybe necessary to access the original data held on a target computer, however it is imperative that the person doing so is competent and can be accountable for their actions.
We place digital evidence at your fingertips™

MIRRORING/
ACQUISITION/
COPY

Danny Myburgh
082 781 2078

We place electronic evidence at your fingertips
www.cyanre.co.za

Danny Myburgh
082 781 2078
MD 5 & SHA1
The MD5 hash algorithm is a 128 bit hash value while the SHA1 algorithm is a 160 bit hash value and the SHA1 hash is considered to be a more complex and more secure algorithm (Thompson, 2005:39). Schneier (1996:436-441) explains that the MD5 hash value has a key size of 128 bits with $3.4 \times 10^{38}$ possible combinations. The chance of randomly finding two files that produce the same hash value should be computationally unfeasible. Digital forensic investigators can, therefore, mathematically – beyond a reasonable doubt – show in court that digital evidence has not changed by even one character.

“CAT”
MD5 hash value - c01ae1a5f122f25ce5675f86028b536a
SHA1 hash value - cf9b775c2c44520178d30c267440066c6eff6e8

If the word “CAT” is changed to “CATS“:
MD5 hash value - ee77f71f2b809c0f6d92320fc9b480f6
SHA1 hash value - c7da99899675795b2f1d94607dbe57b731dd2255
ANALYSIS
What does an analysis involve?

**Level 1** - Search active files and previously deleted file fragments for keywords stored in ASCII, Unicode, Hexadecimal, multiple languages.

**Level 2** - Search hidden, encrypted, encoded data (Most Email Data, Databases, Compressed or Zipped Files, and Enhanced Meta Files).

**Level 3** - Analyze logical and physical disk structure

**Level 4** - Locate additional evidence needed by investigator
Where to find evidence

- Mobile Devices
- Social Media
- Financial databases and systems
- E-mail
- Evidence no longer available in paper form
- Altered File Signatures
- System Artifacts
  - Temp files (.tmp)
  - Spool & Shadow Files
- File Archives & Backups
  - Auto Backup files (.bk)
- Swap File Content
- Registry Information
- Deleted files
What can be extracted

**Metadata**
- Create, Modify and Print Dates
- Original Author and up to last 10 Editors
- Previous Document Names and File Paths
- Hidden Data

**Embedded Information in Documents**
- Comments
- Red-line versions
- Formulas
- Speaker’s notes

**Dynamic Content**
- Databases
- Queries