Detecting Computer Intrusions: Are You Pwned?

FORWARD
DISCOVERY

Steve Anson

FORWARD DISCOVERY

- Former computer agent for the U.S. Department of Defense and Federal Bureau of Investigation (FBI)
- Former computer crime investigation instructor at the FBI Academy
- Co-author of *Mastering Windows Network Forensics and Investigations*
- Instructor for U.S. State Department
- CISSP, MCSE, EnCE, blah, blah, blah

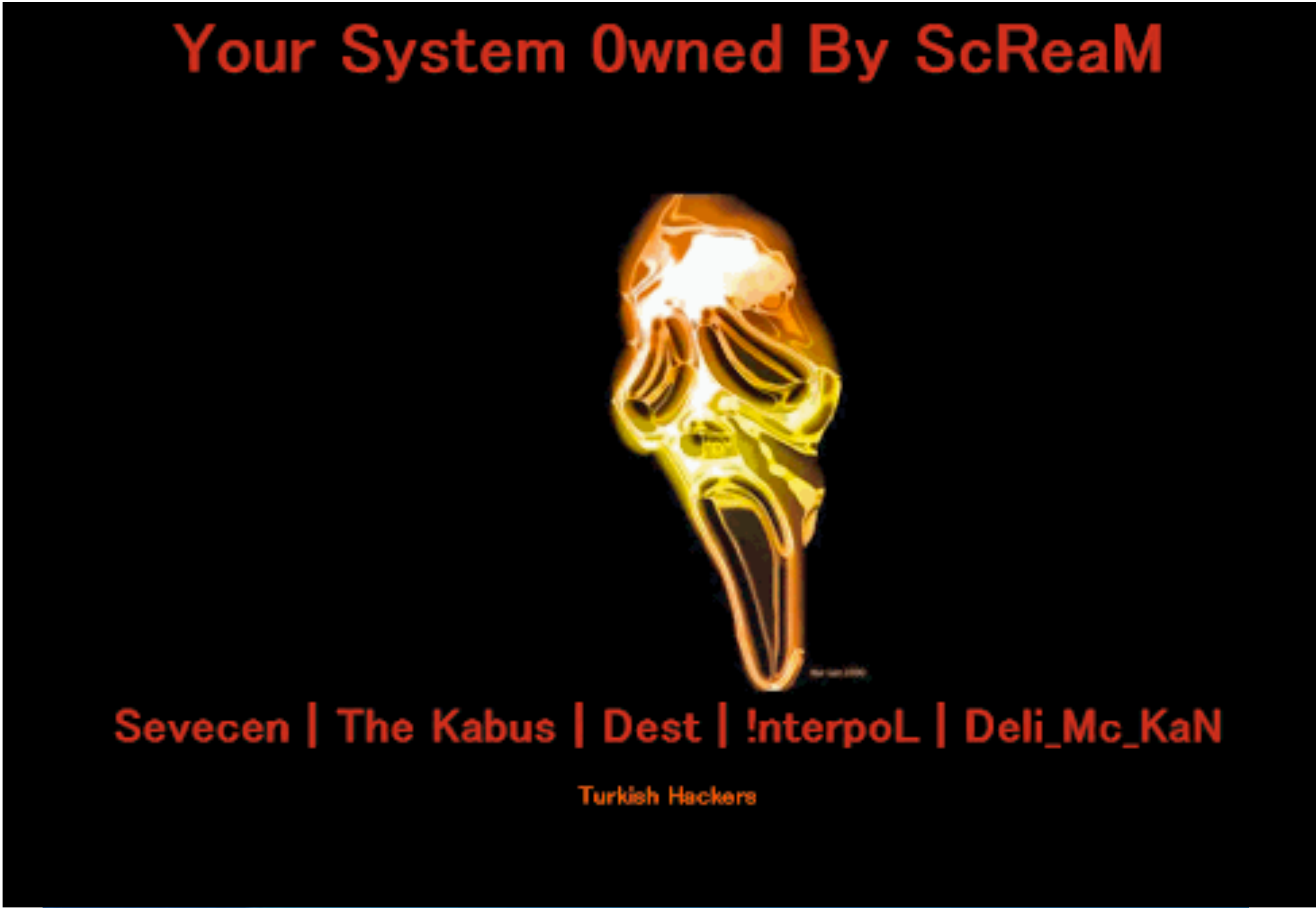
Detecting Intrusions

Behavioral Indicators

Forensic Indicators

Behavioral Indicators

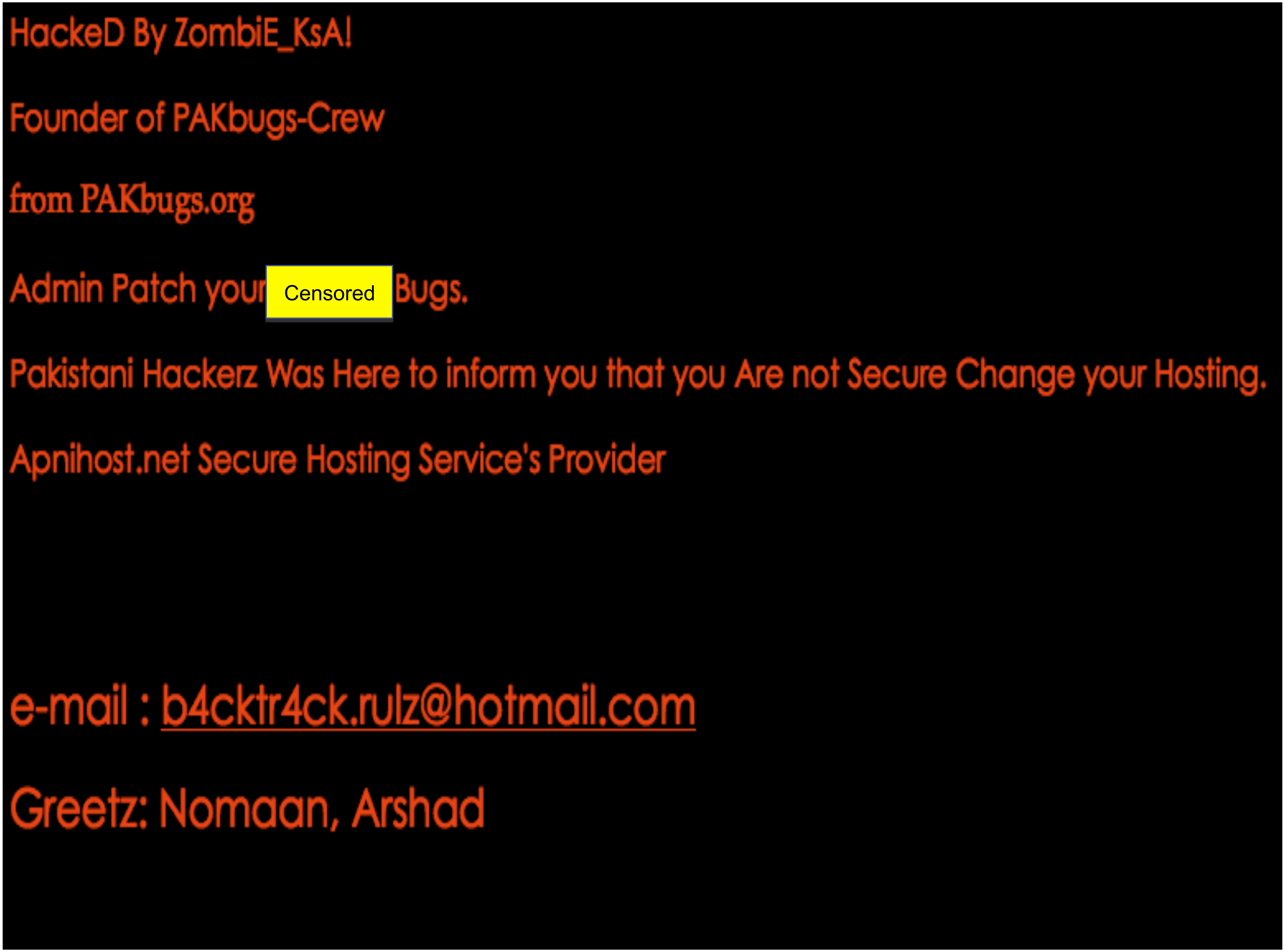
- **“Clues” you may be hacked**



Your System 0wned By ScReaM

Sevecen | The Kabus | Dest | !nterpoL | Deli_Mc_KaN

Turkish Hackers



HackeD By ZombiE_KsA!

Founder of PAKbugs-Crew

from PAKbugs.org

Admin Patch your Censored Bugs.

Pakistani Hackerz Was Here to inform you that you Are not Secure Change your Hosting.

Apnihost.net Secure Hosting Service's Provider

e-mail : b4cktr4ck.rulz@hotmail.com

Greetz: Nomaan, Arshad

Behavioral Indicators

IDS / IPS Alert

- Sorting False Alarms Takes Time

Antivirus Alert

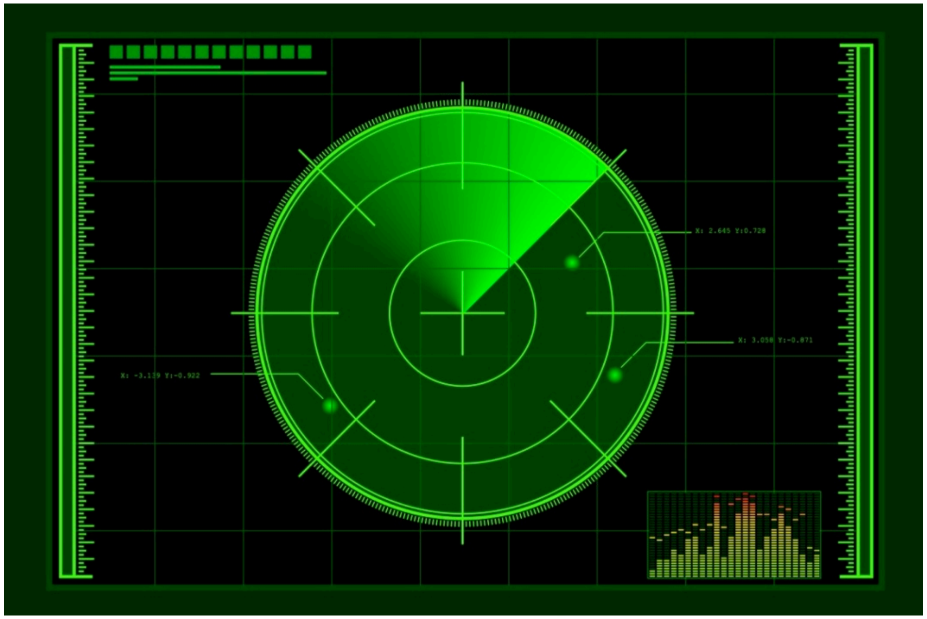
- Inbound or Already Installed?

SEIM Alert

- Again, Tricky to Configure

Behavioral Indicators

- **Scanning**
  - **Can be quite loud (lamers, worms)**
  - **Often more controlled (more dangerous)**



Behavioral Indicators

- **E.T. Phones Home**
  - **Beaconing**

Behavioral Indicators

- **The massive sucking sound of all your data leaving**
  - **Data exfiltration can be rapid and massive in scope**
  - **Attacker may stage for years and then pull data over one weekend**

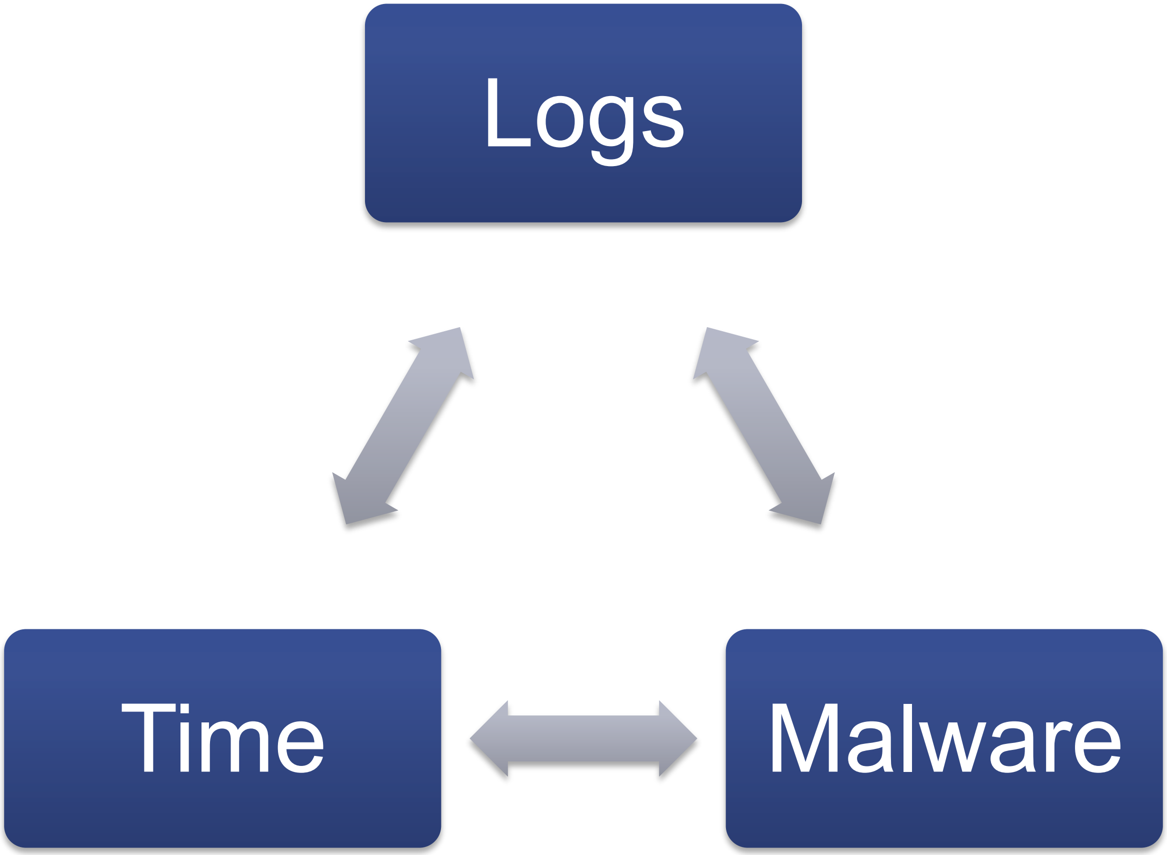
Behavioral Indicators

- **Traffic that's just not right**
  - **Large file transfers over port 53**
  - **Lots of extraneous SSL traffic**
  - **SSL traffic on port 80**

Behavioral Indicators

- **Unexplained user accounts**
  - **Old accounts that are reactivated**
  - **New accounts**
  - **Old accounts with new permissions**

Forensic Indicators



Logs

IDS / IPS

- Great if you have them

Firewall

- Track connections in and out

Authentication Servers

- Unusual logon times or locations

Windows Logs

Remote Logon

- Event ID 528 (Logon Type 10), 540, 672, 673

Psexec

- Event ID 7035, 7036

Password Guessing

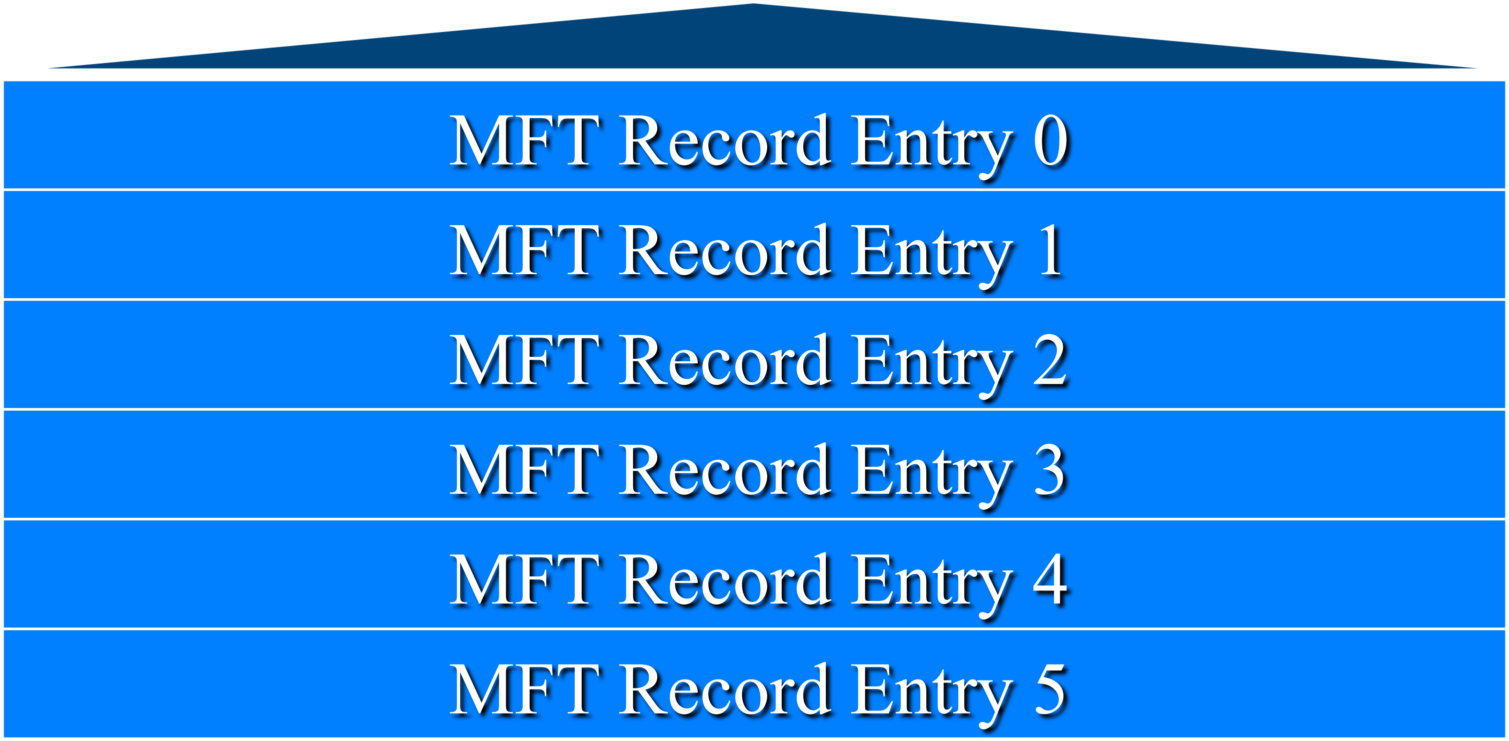
- Event ID 672 (Failure), 675, 676, 680, 681

File System Forensics

Timestamps

- **Standard of analysis**
- **Used to detect changes**
- **Some say its time has passed**

File System Forensics



MFT Record Entry 0

MFT Record Entry 1

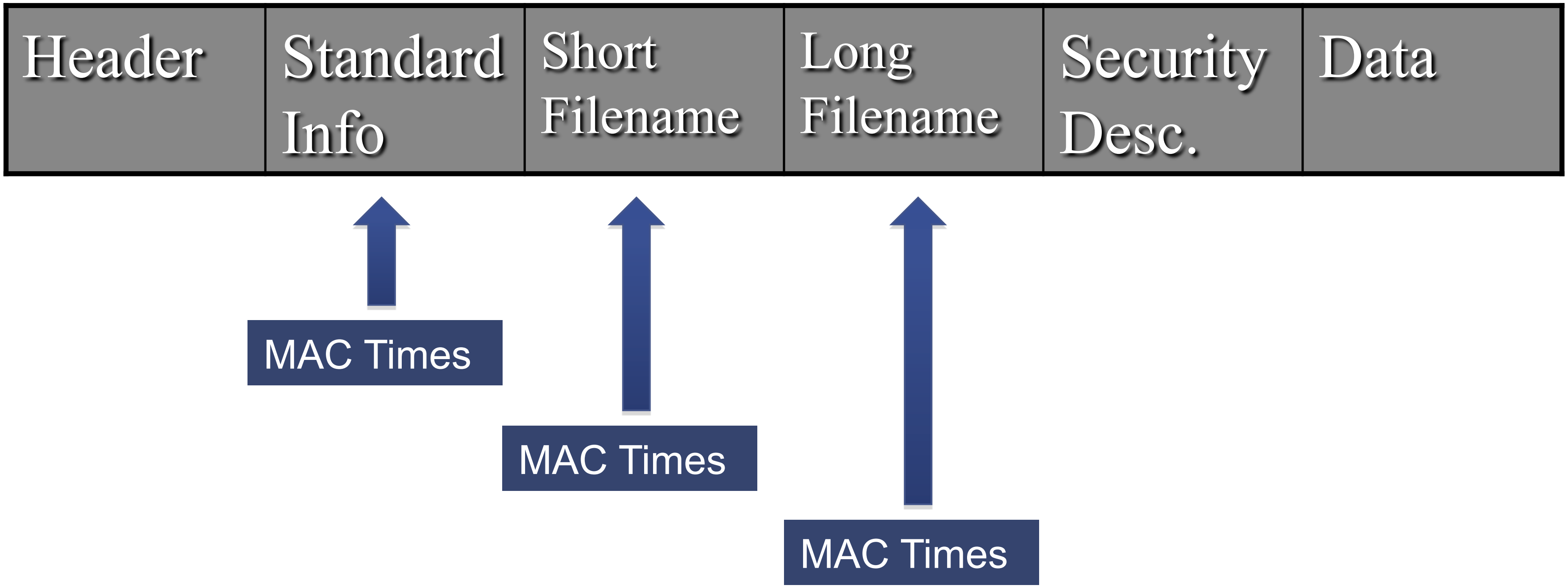
MFT Record Entry 2

MFT Record Entry 3

MFT Record Entry 4

MFT Record Entry 5

Windows Logs



Header	Standard Info	Short Filename	Long Filename	Security Desc.	Data

MAC Times

MAC Times

MAC Times

File System Forensics

Bad Binaries

- Close names
  - svvchost
  - svchosts
- Alternate locations

File System Forensics

FORWARD DISCOVERY

Memory Forensics

- Running processes
- Open ports
- Active connections
- Malware only in RAM

File System Forensics

Memory Forensics

- Old school
  - netstat –ano (or netstat –anp)
  - tasklist /SVC (or ps –ef)
- New school
  - HBGary, Volatility

File System Forensics

FORWARD
DISCOVERY

Hash Analysis

- MD5 or SHA1 hash comparisons
- Same limitation as any signature based solution
- Good at identifying other copies

Enterprise Forensics

Sweeping Entire Enterprise

Network Traffic Forensics

Contact Information

Steve Anson
Forward Discovery Middle East FZ-LLC
Dubai Knowledge Village
Block 6, Office F08
Mobile – +971 50 287 1062
Email – sanson@forwarddiscovery.com
Web – www.forwarddiscovery.com