# Threat Landscape – a view from the inside

Bill Beverley– Manager, UK Security Architecture

SecureWorks

# SecureWorks

- Security Operations Center (SOC)
- SOC and Data Center
- Office Location
- Data Centre


**70+** Countries

**~4K** Customers

**24x7** Access to Security Experts

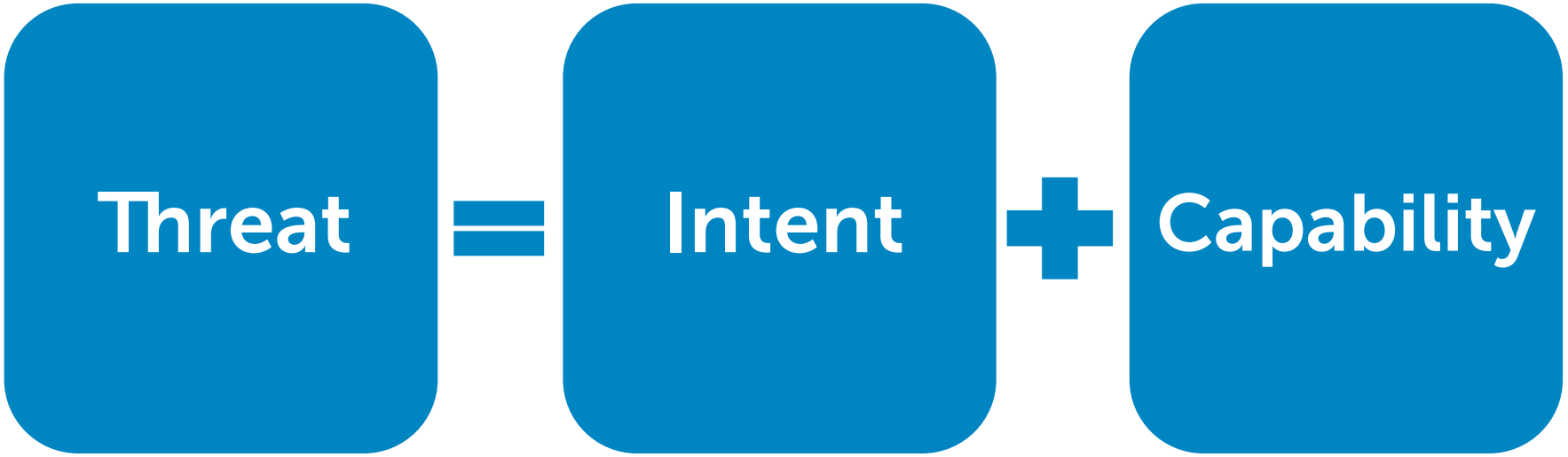
**~180B** Daily Events

**~100K** Malware Samples

**~7M** Attacker DB

# Cyber Threats

# What is a threat?




A Threat Group's aims, target and willingness to act

The Threat Group's means to act on their intent

# What is a Cyber Operation?

**Intent** → **Execute**

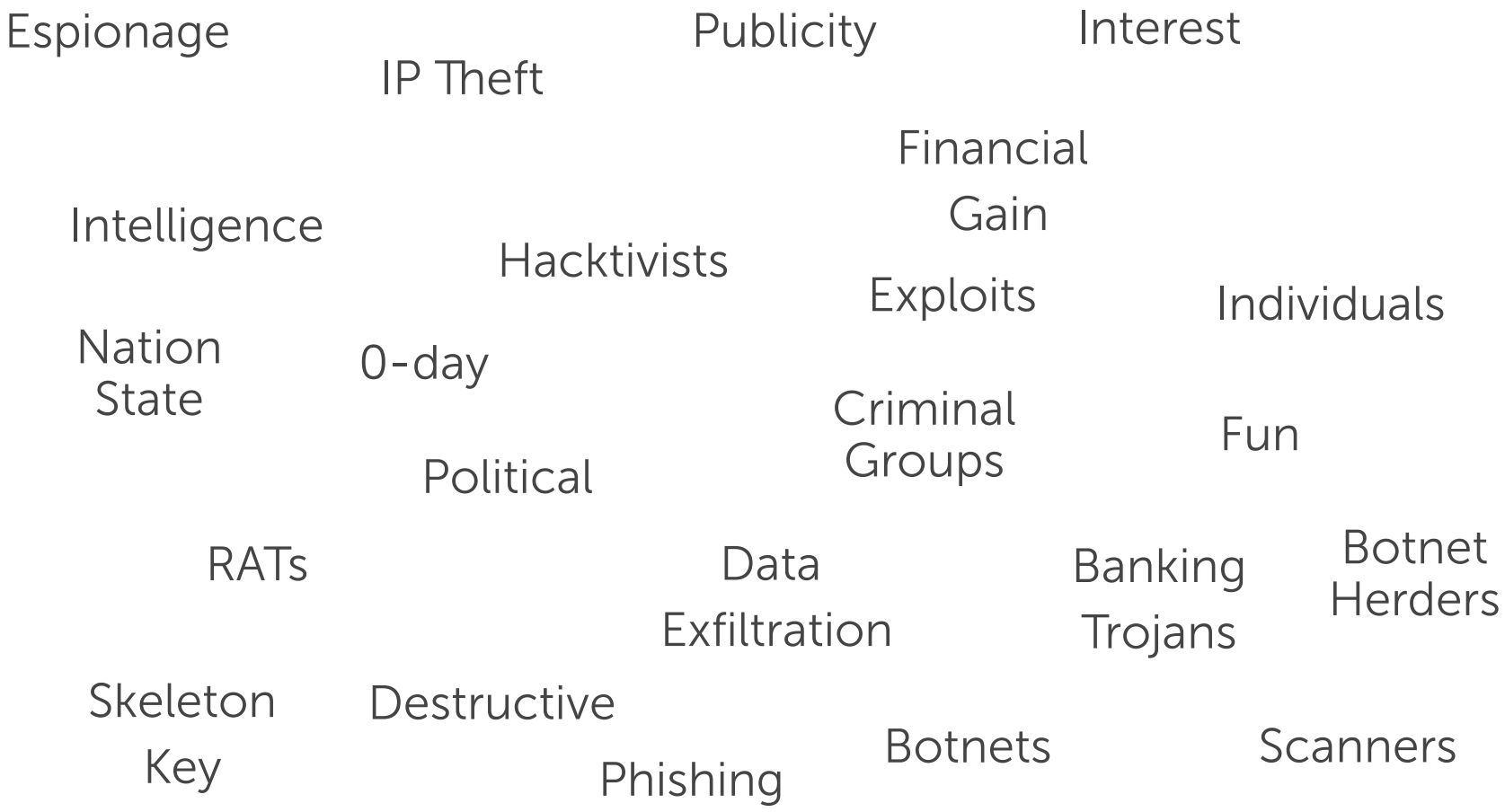
1. Defraud online banking customers
2. Acquire pharmaceutical test data
3. Access corporate merger plans
4. Gain access to an industrial control system
5. Destroy or hold data to ransom


**Infer**

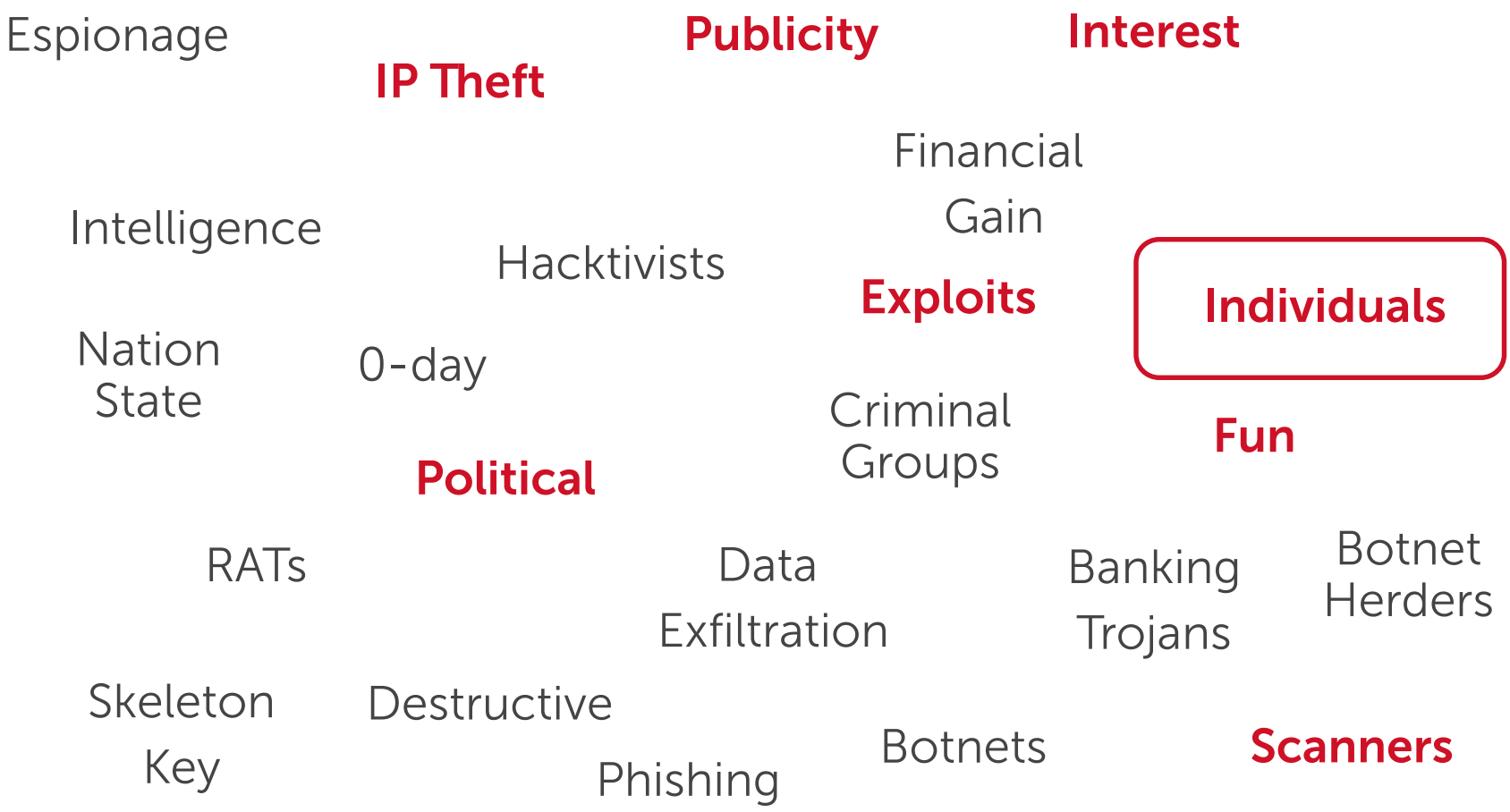
**Observe**

# Threat Landscape

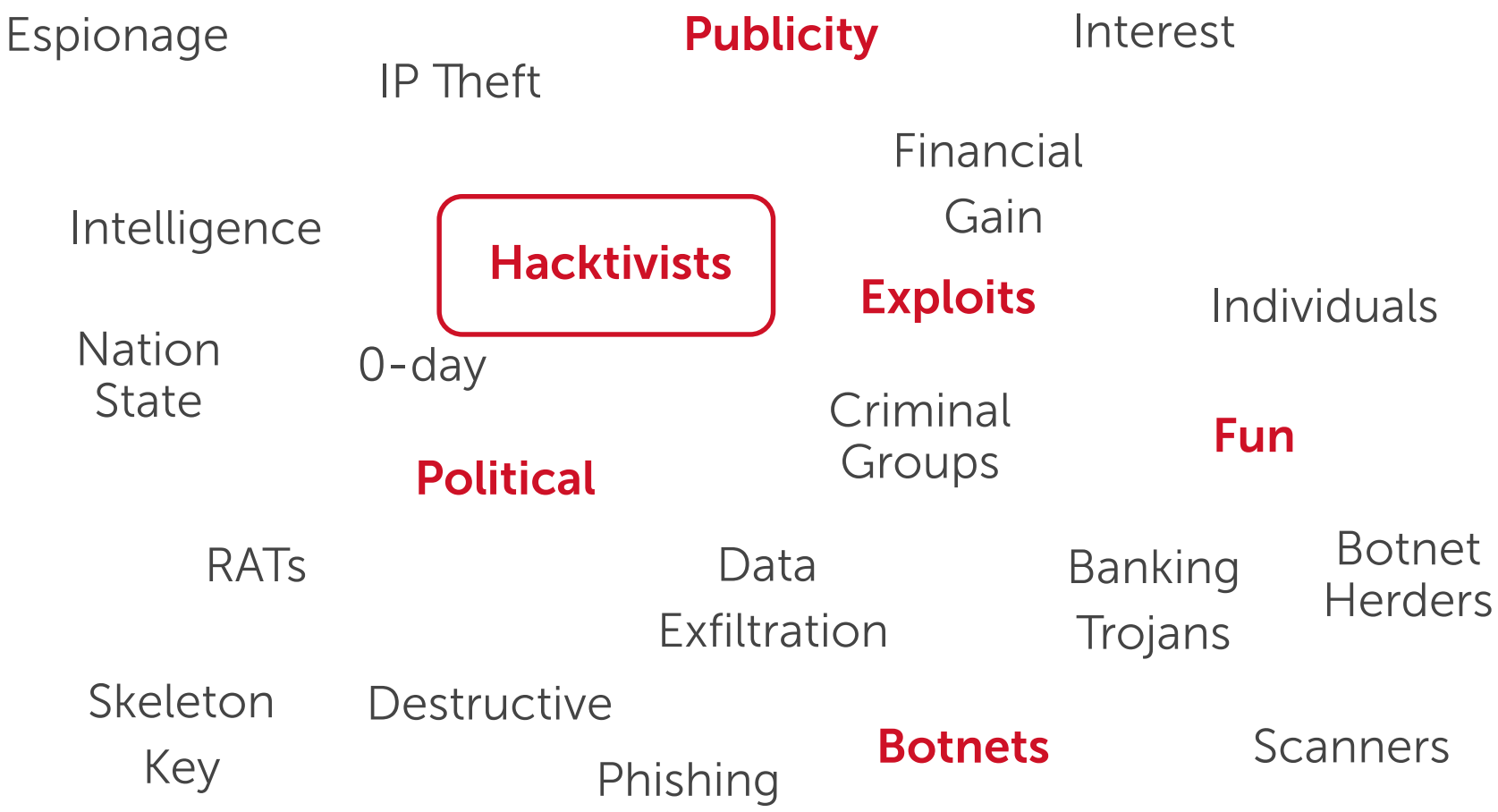
# The Threat Cloud



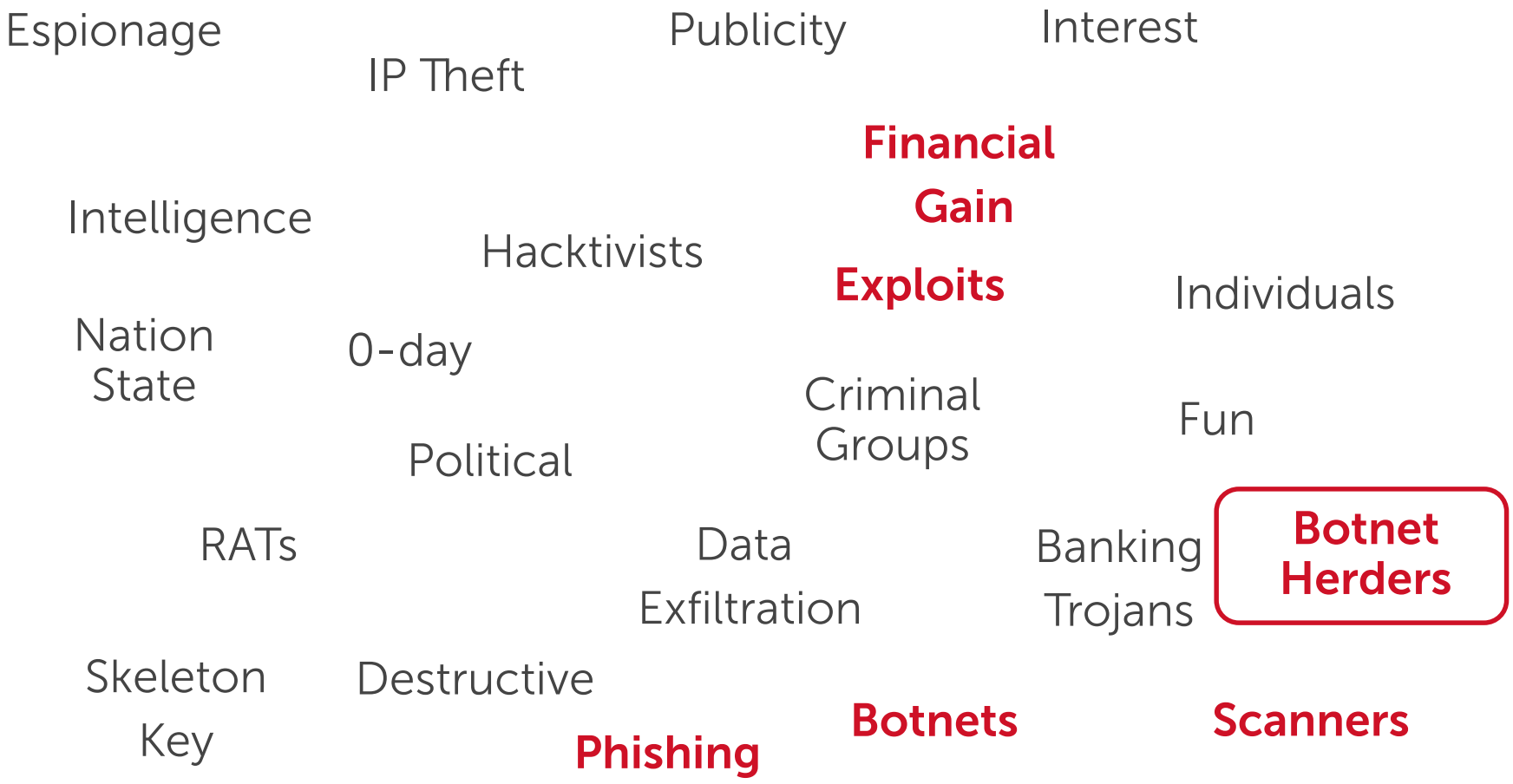
# The Threat Cloud - Individuals



# The Threat Cloud - Hacktivists



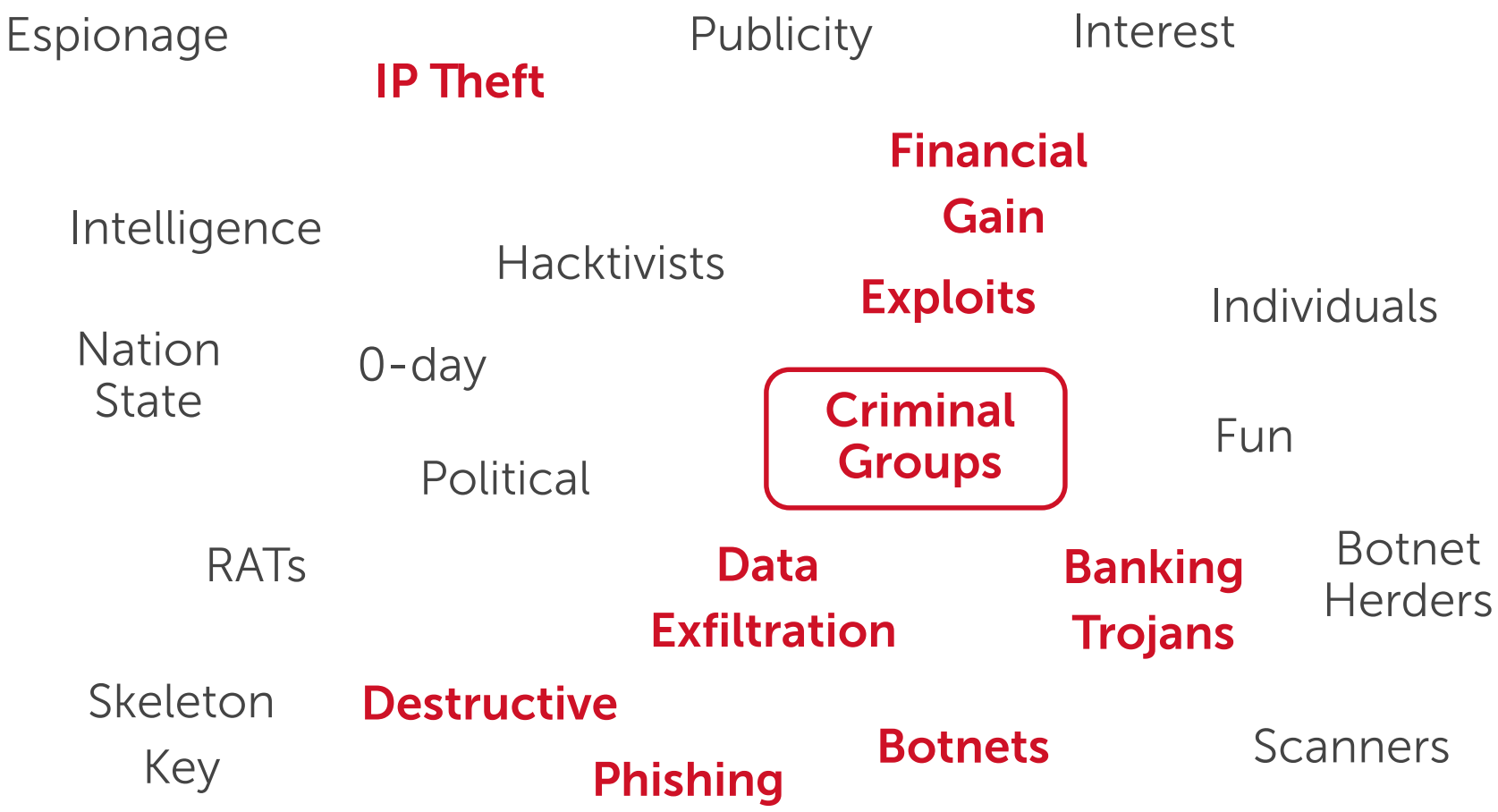
# The Threat Cloud – Botnet Herders



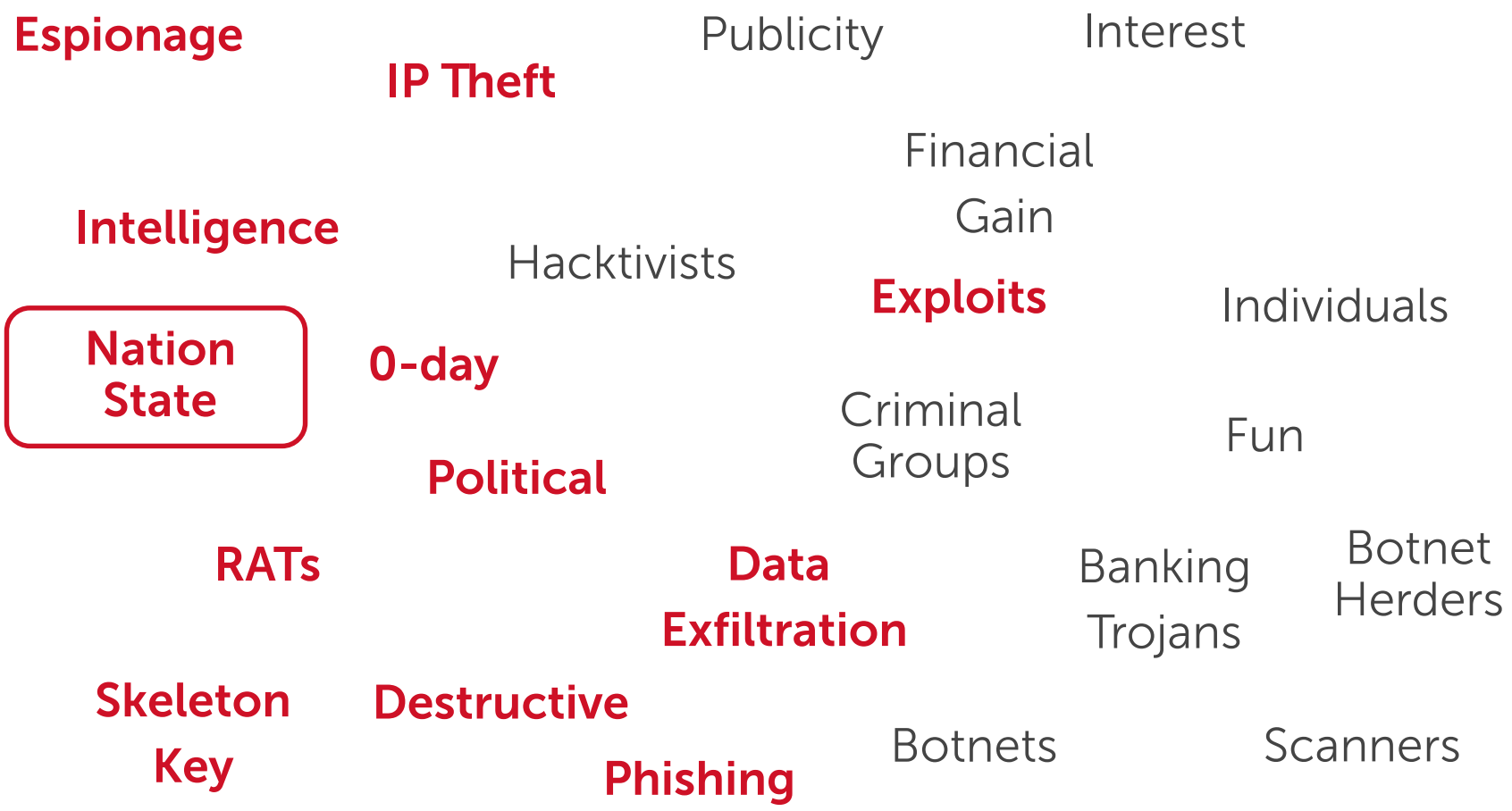



SecureWorks

# The Threat Cloud – Criminal Groups

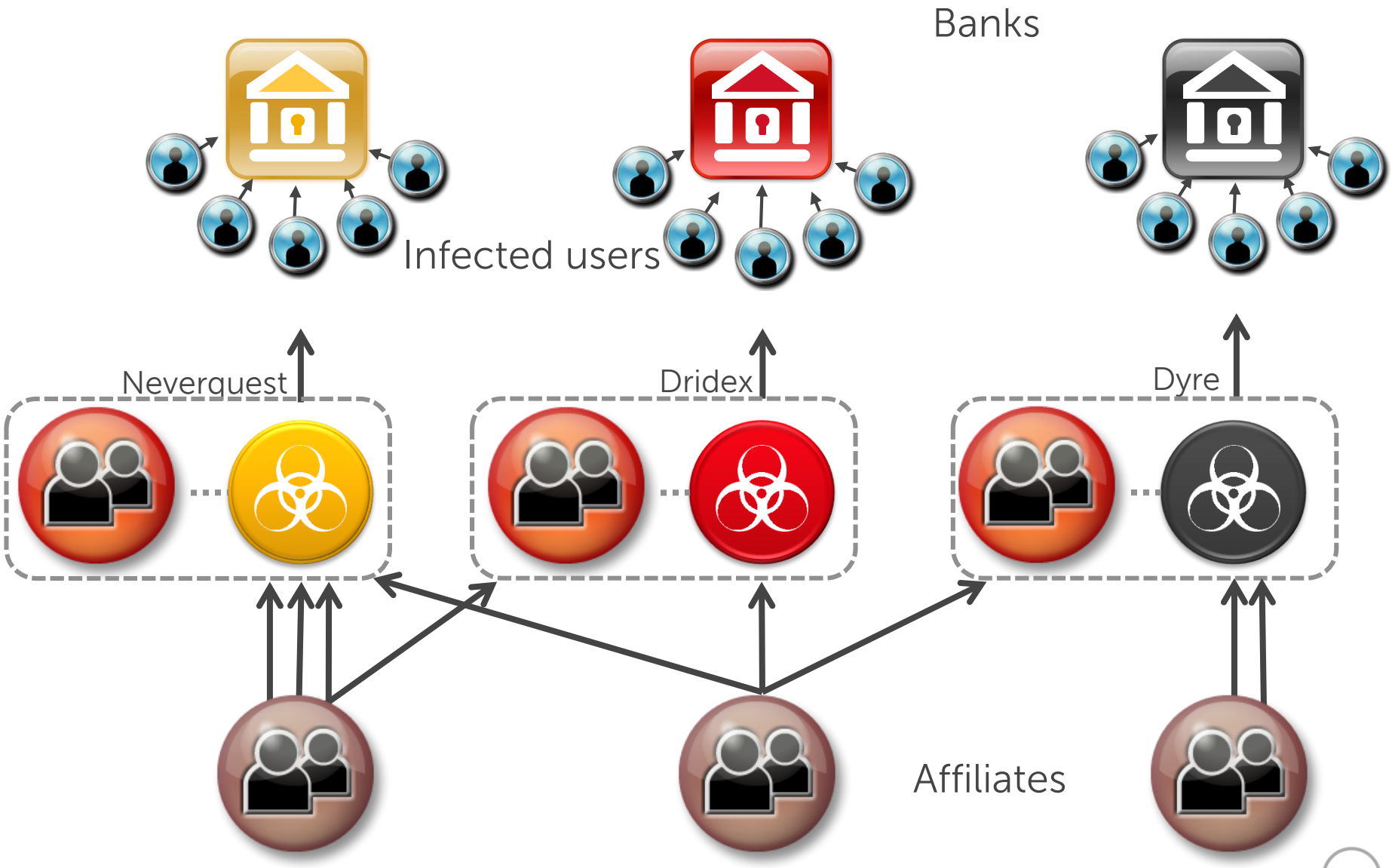


# The Threat Cloud – Nation State



# Cyber Attacks - E-Crime

# Crime Groups



# Bots, bots, bots...

Tofsee

**Cryptolocker**

**Cutwail**

ICEIX

NedSym

Lerspeng

Asprox

KINS

Citadel

Phorpiex

Shylock

Pushdo

Chanitor

**Upatre**

Pony

**Bugat**

Tinba

**GameoverZeus**

Dirtjumper

Torpig

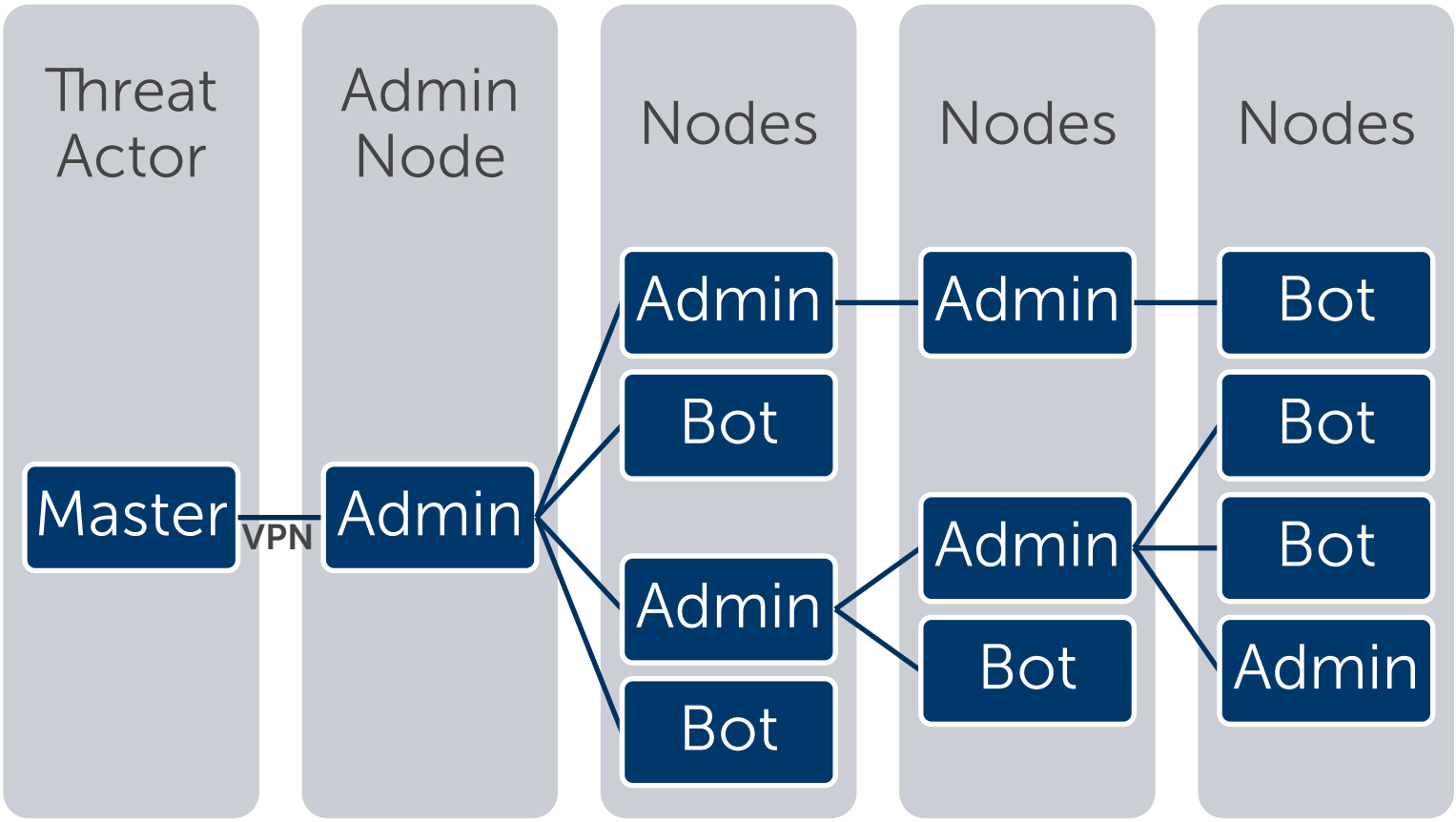
SmokeBot

Hesperbot

Gozi

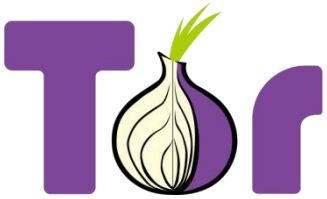
**Dyre**

# Dridex P2P Structure

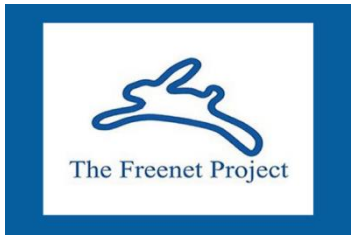


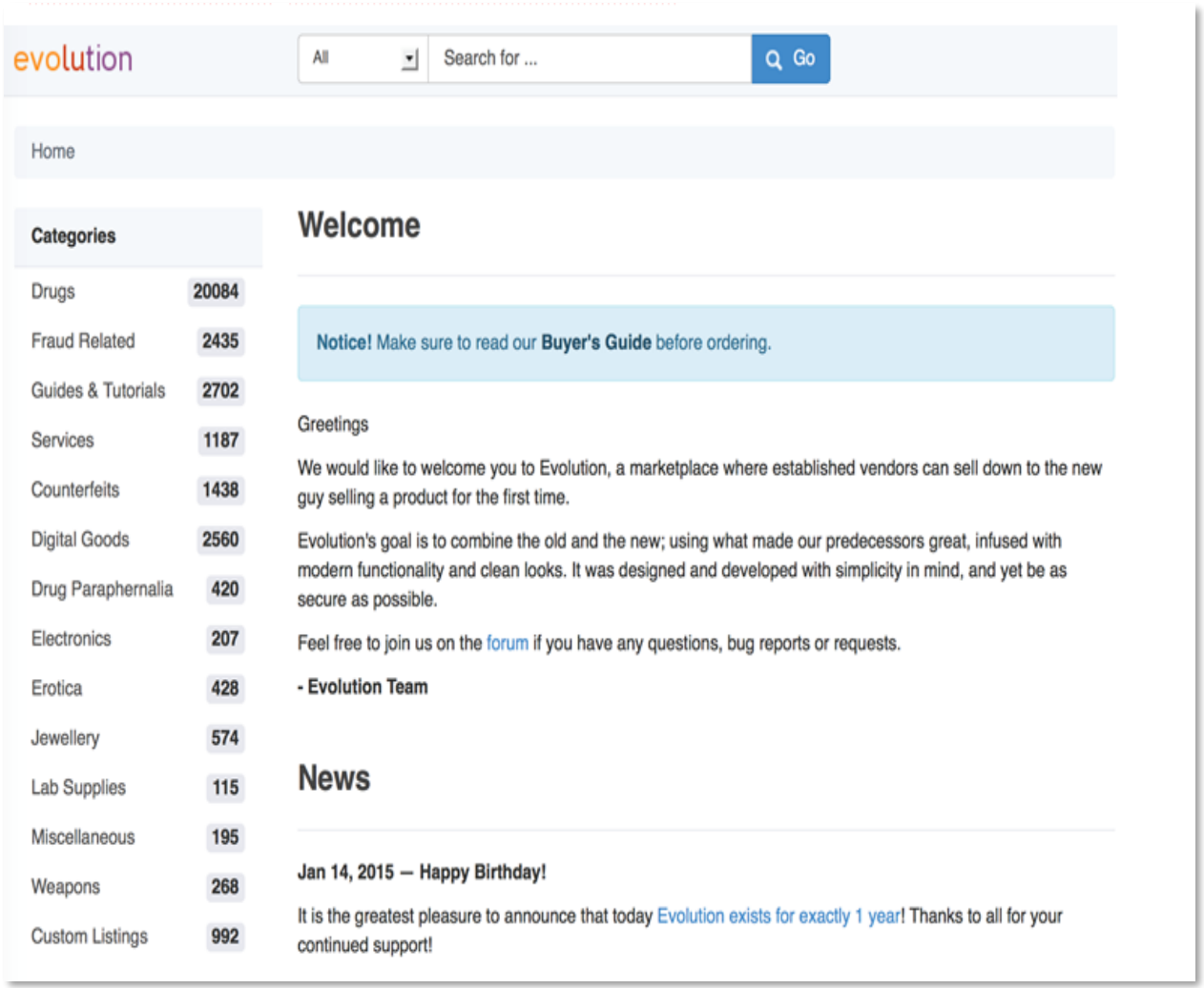

- Structure of Master – Admin – Bot, all with P2P communications
- An Admin node is also a bot but can pass on commands to others
- Makes it difficult to reverse the hierarchy back to the Master node

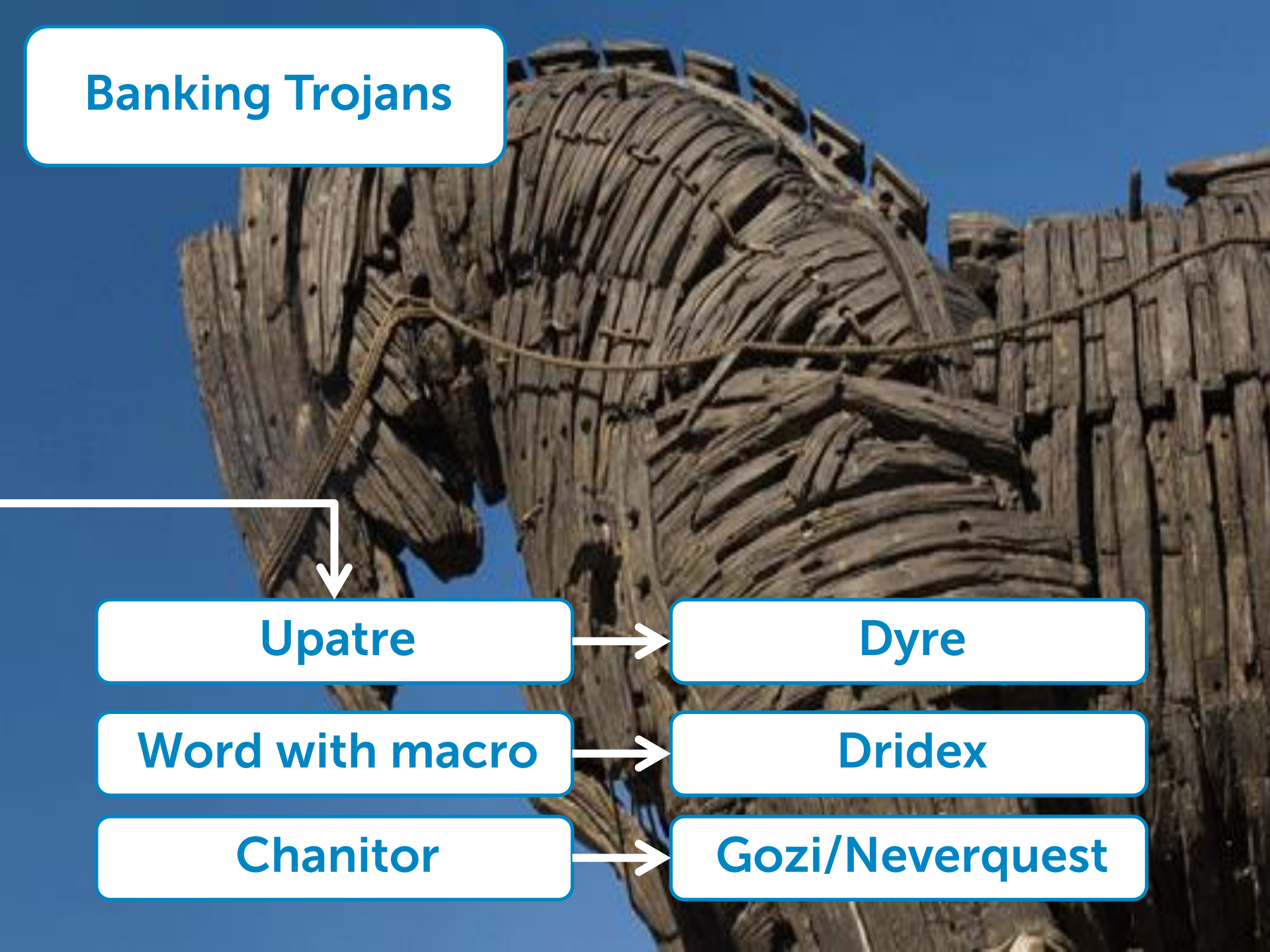
# Darknet eCommerce







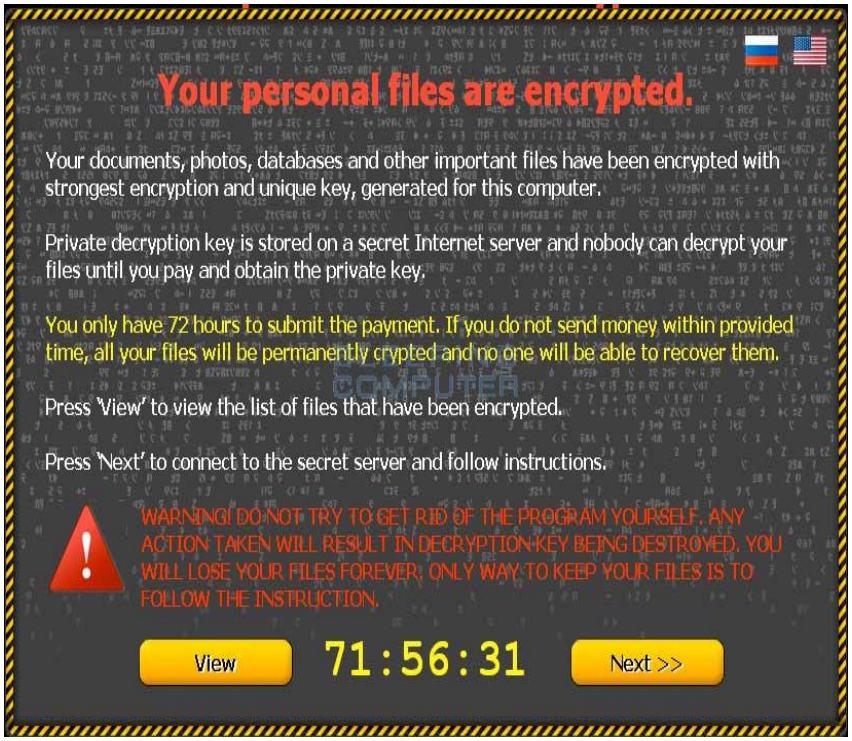




Banking Trojans
Upatre
Dyre
Word with macro
Dridex
Chanitor
Gozi/Neverquest

# Cyber Attacks - Destroy / Ransom

# Crypto Ransomware – Constantly evoloving

- Cryptolocker taken down by Op Tovar
- Cryptowall evolving, now in version 3
- CTBLocker
- TeslaCrypt
- Virlock
- Torrentlocker
- SamSam



# Malware & Tactics Evolve

- **Virlock**
  - Locks the screen of infected hosts like other ransomware
  - Encrypts AND Infects files on the device
  - It hides in the registry
  - Disables critical functions
  - Polymorphic code
- **Teslacrypt** *Now closed down –decryption keys released*
  - First ransomware to specifically target gamers by encrypting important game files
- **SamSam**
  - (One of) new kid(s) in town
  - Exploits Jboss vulnerabilities –
  - Sophisticated multi-pass encryption
- **KeRanger**
  - Mac OS X Ransomware

# Ransom Attacks

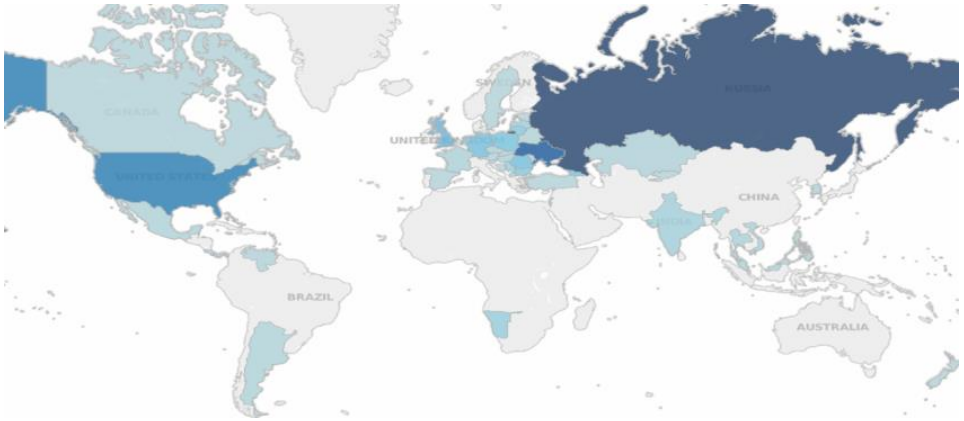
- The "Guardians of Peace" (GOP) demanded the cancellation of the planned release of the film *The Interview*
- US Government link Sony attack to North Korea


# Cyber Attacks - DDoS

# Tracking DDoS

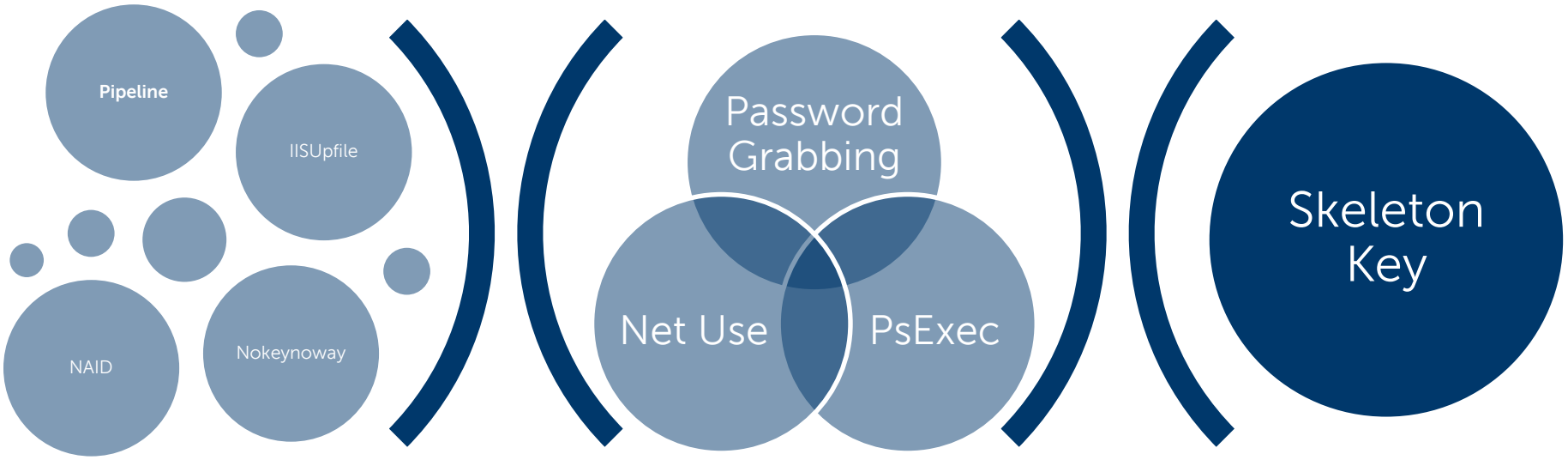
- Visibility on over 655 DDoS botnets since November 2014
  - 42 currently active
    - Dirt Jumper/Di Bot/Drive
    - ArmageDDon
    - YZF
    - Darkness/Optima/Votwup
    - Pandora

- 772 Unique C2 IP addresses across 35 countries
  - United States (226)
  - Russia (218)
  - Germany (60)
  - Ukraine (54)
  - Netherlands (41)



# Cyber Attacks - Nation State

# Skeleton Key



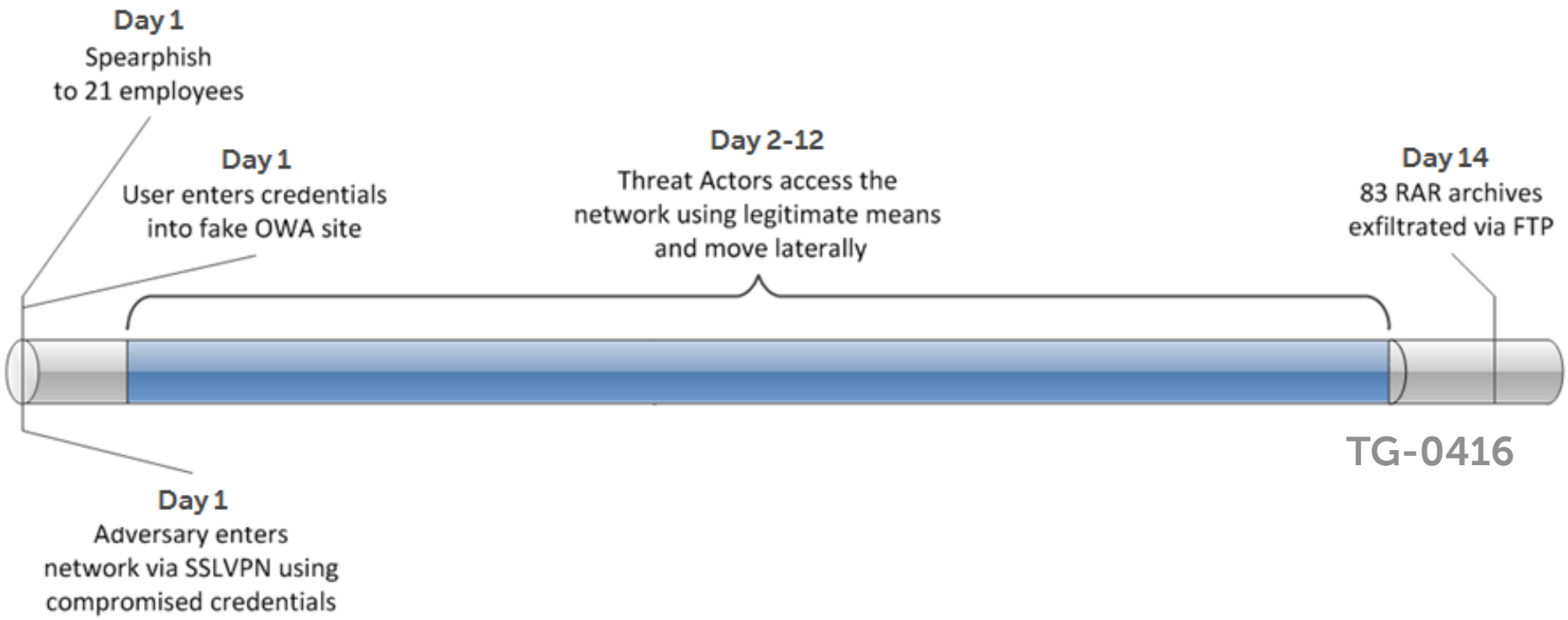

- ~9 different malware families detected on more than 25 hosts including servers and laptops
- Threat actors had been present for years
- Single factor authentication allowed Skeleton Key to be used

# Skeleton Key

Legitimate users can log in with normal password

Attacker can log in with the injected hash on ANY account

# Breach Without Malware



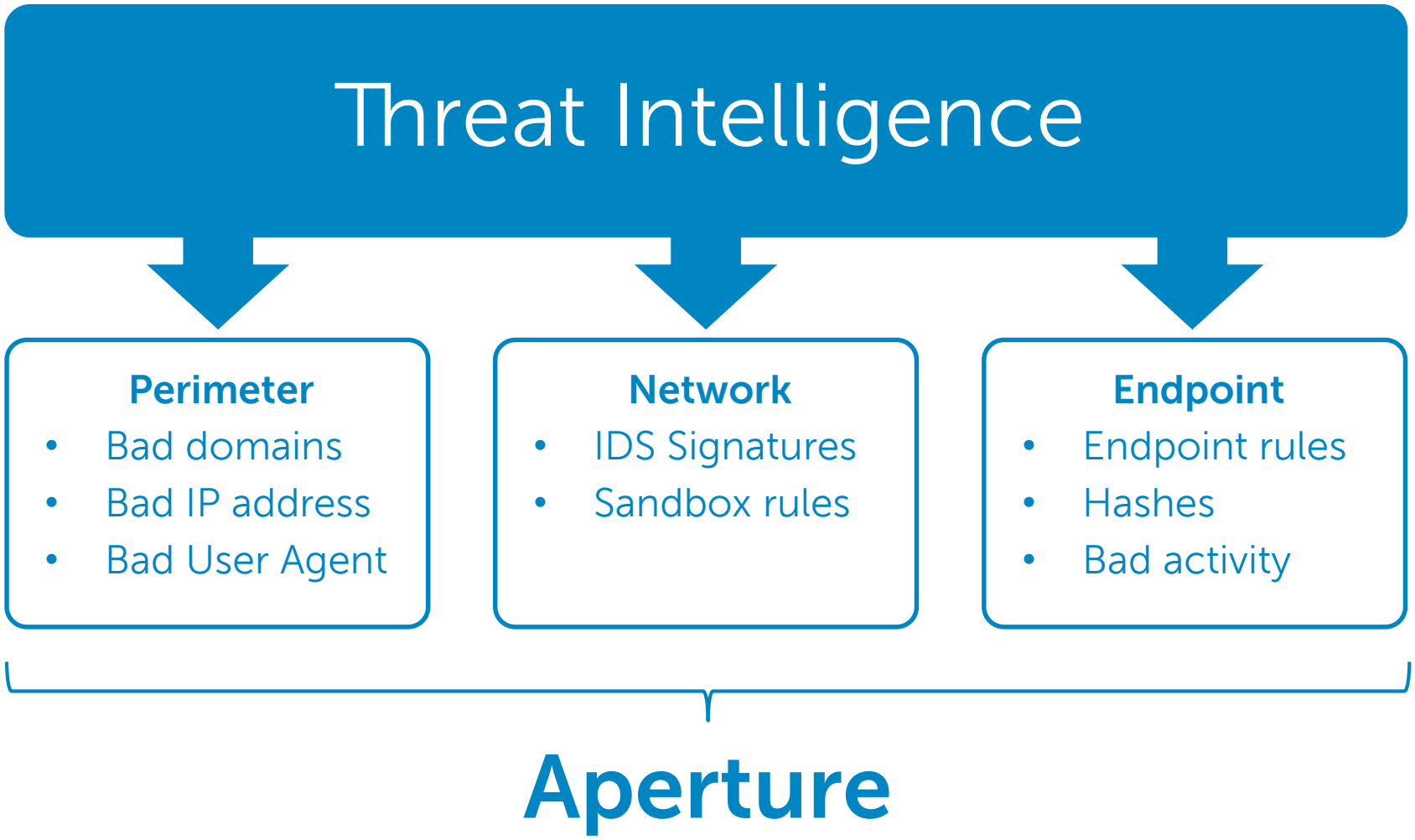



SecureWorks

# What to do about it

# Intelligence + Aperture

# Threat Intelligence



# 5 Pragmatic Security Steps




SecureWorks

# Thank You

Bill Beverley– SecureWorks

SecureWorks