

# 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?



# 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



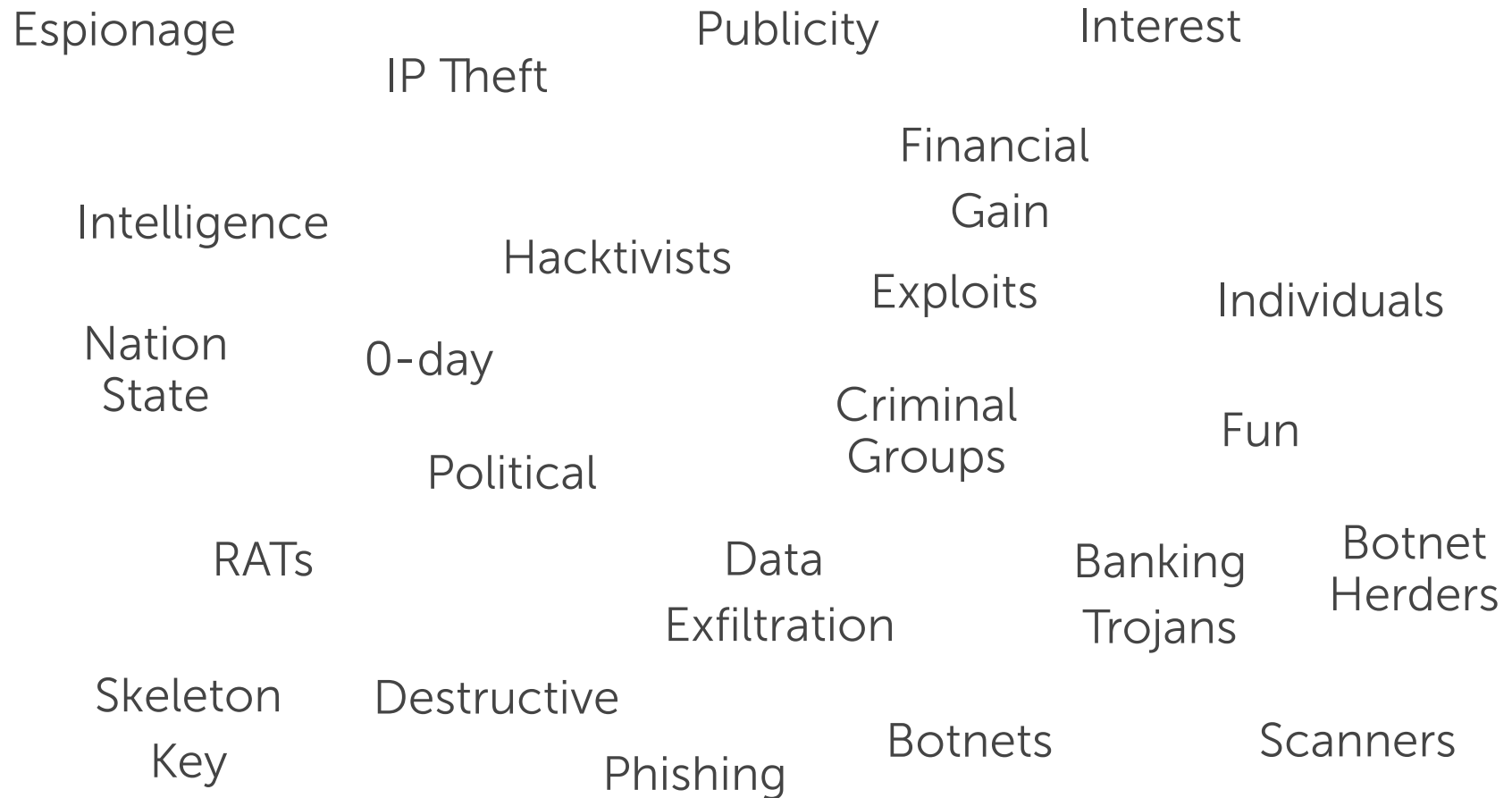
Infer

Observe

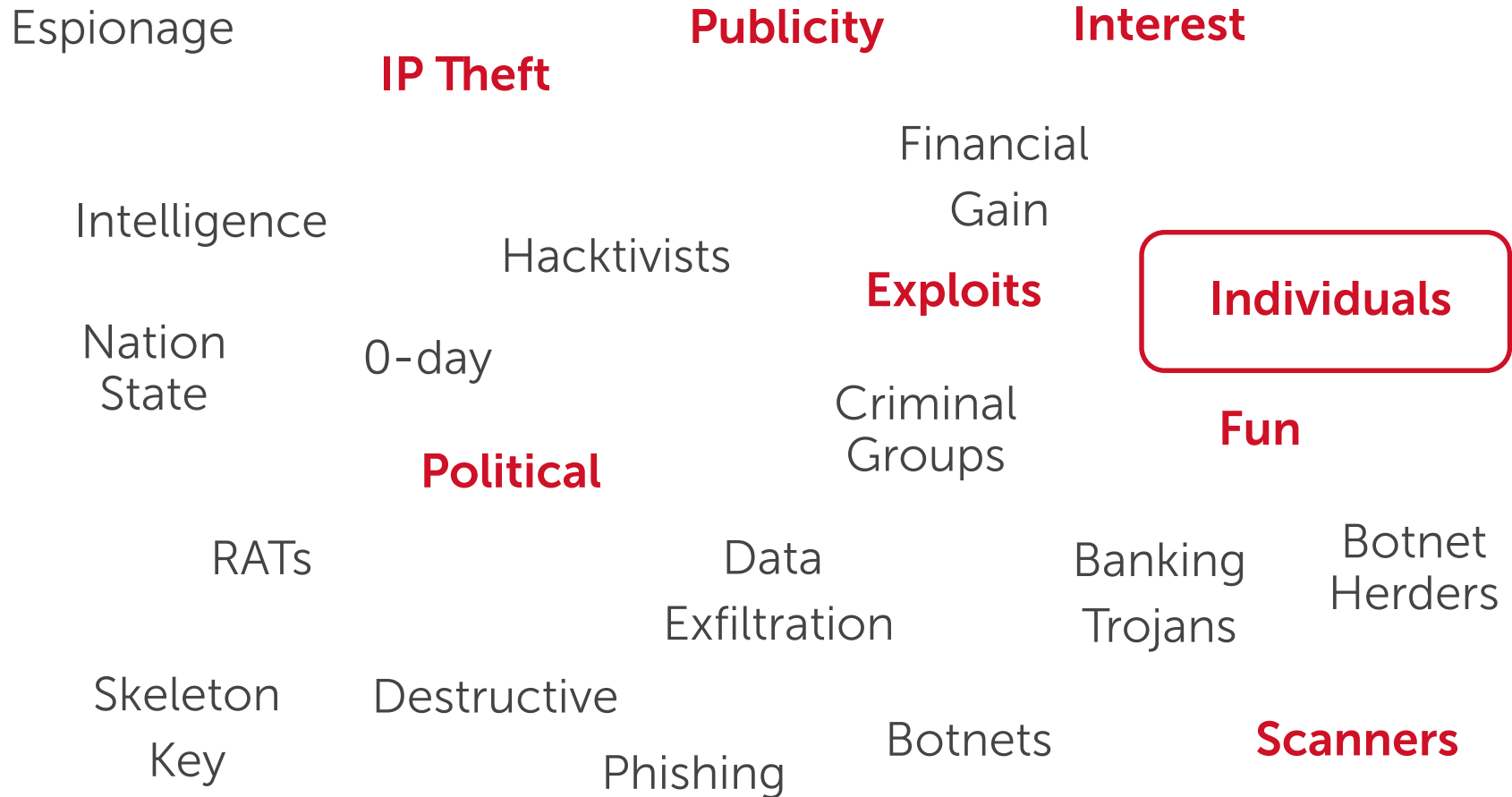


# Threat Landscape

# The Threat Cloud

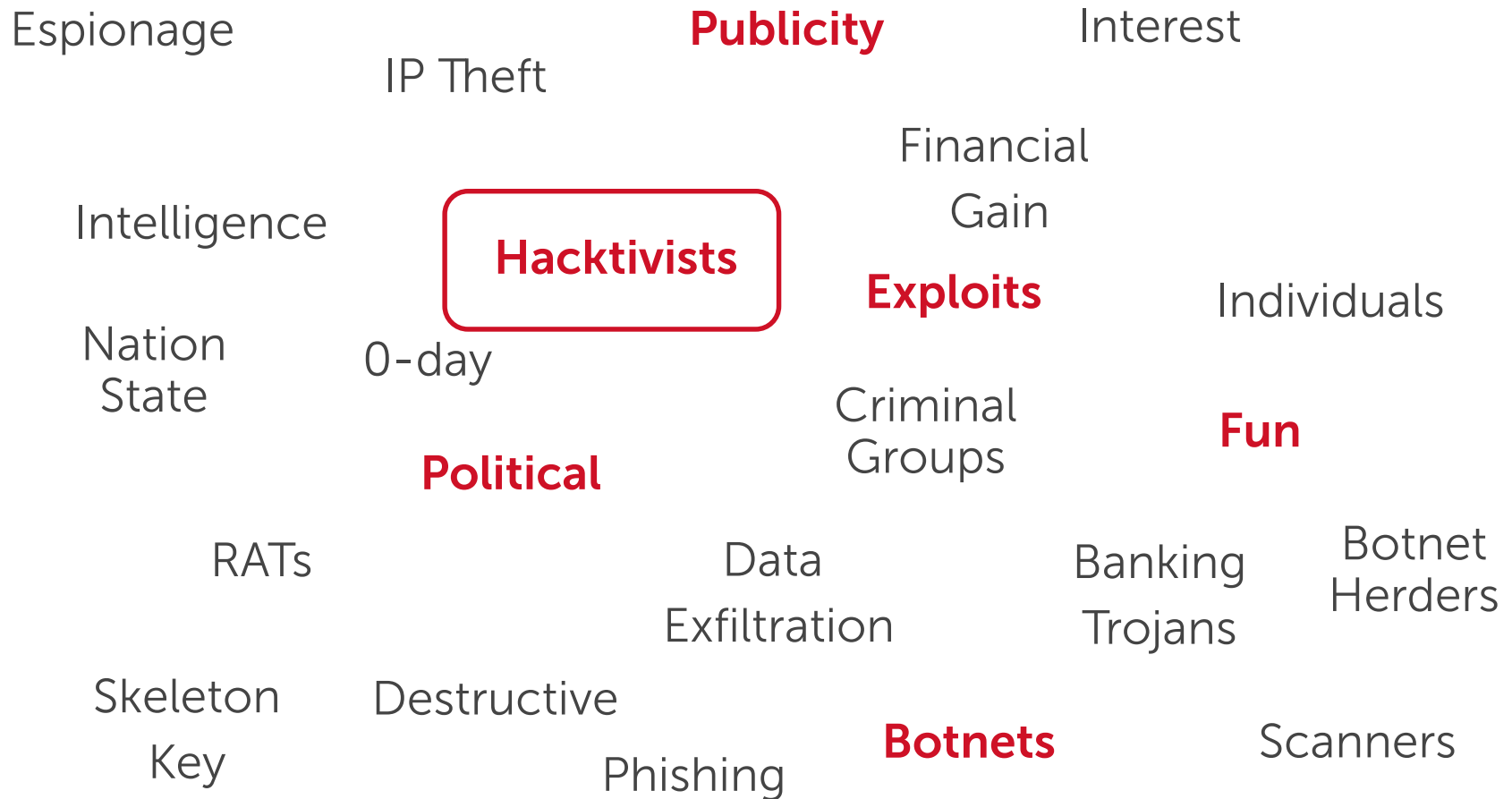


# The Threat Cloud - Individuals

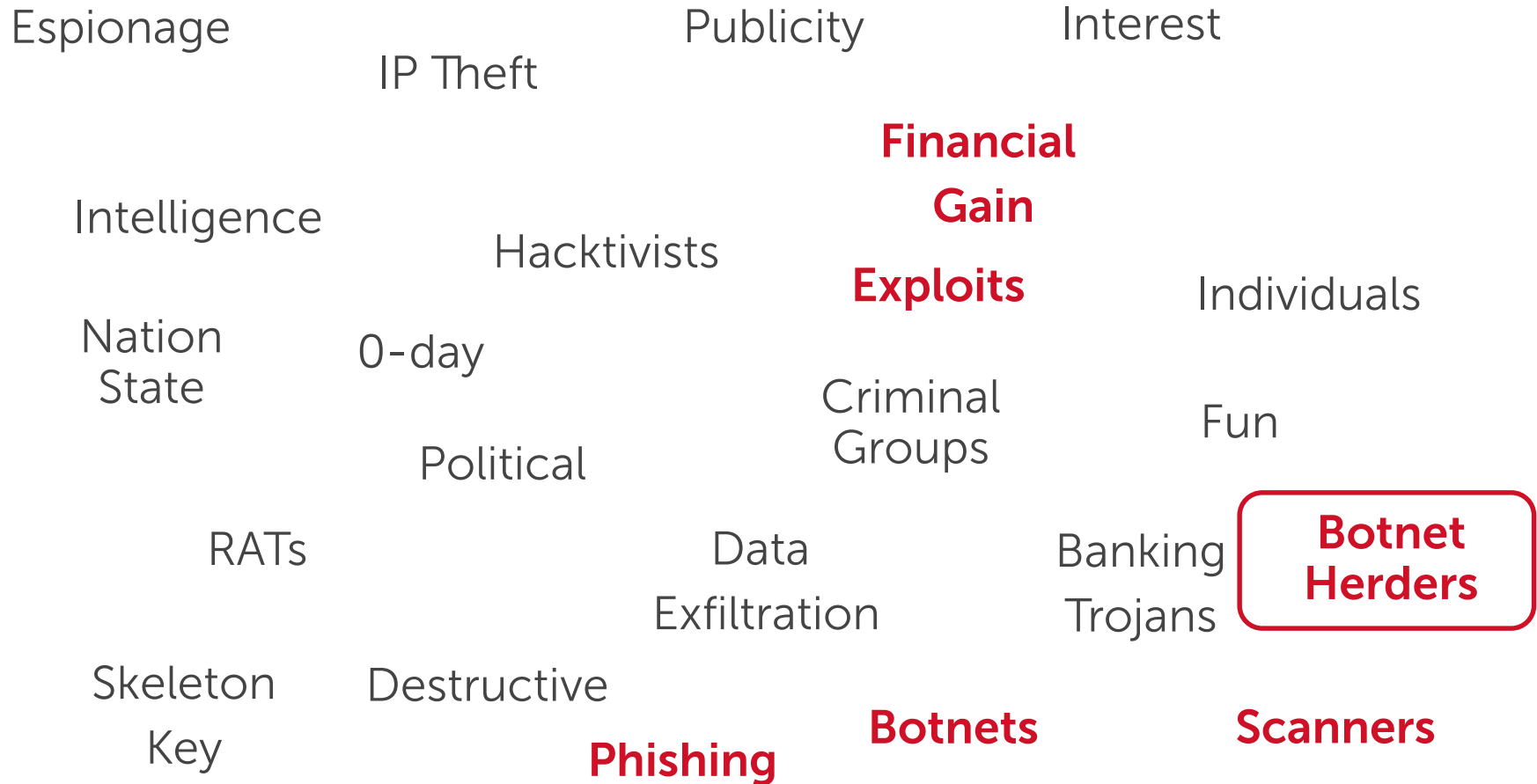




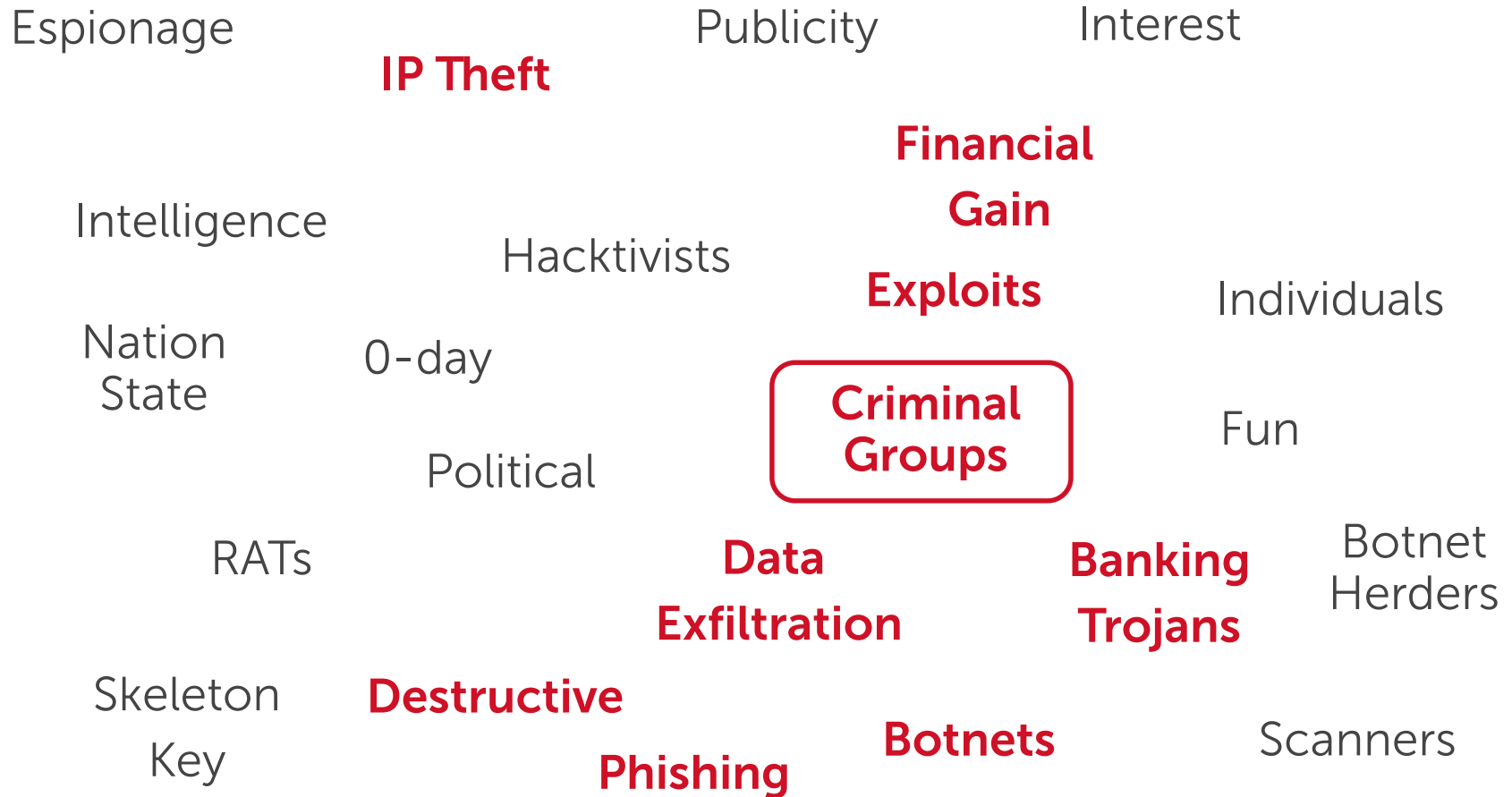
# The Threat Cloud - Hacktivists



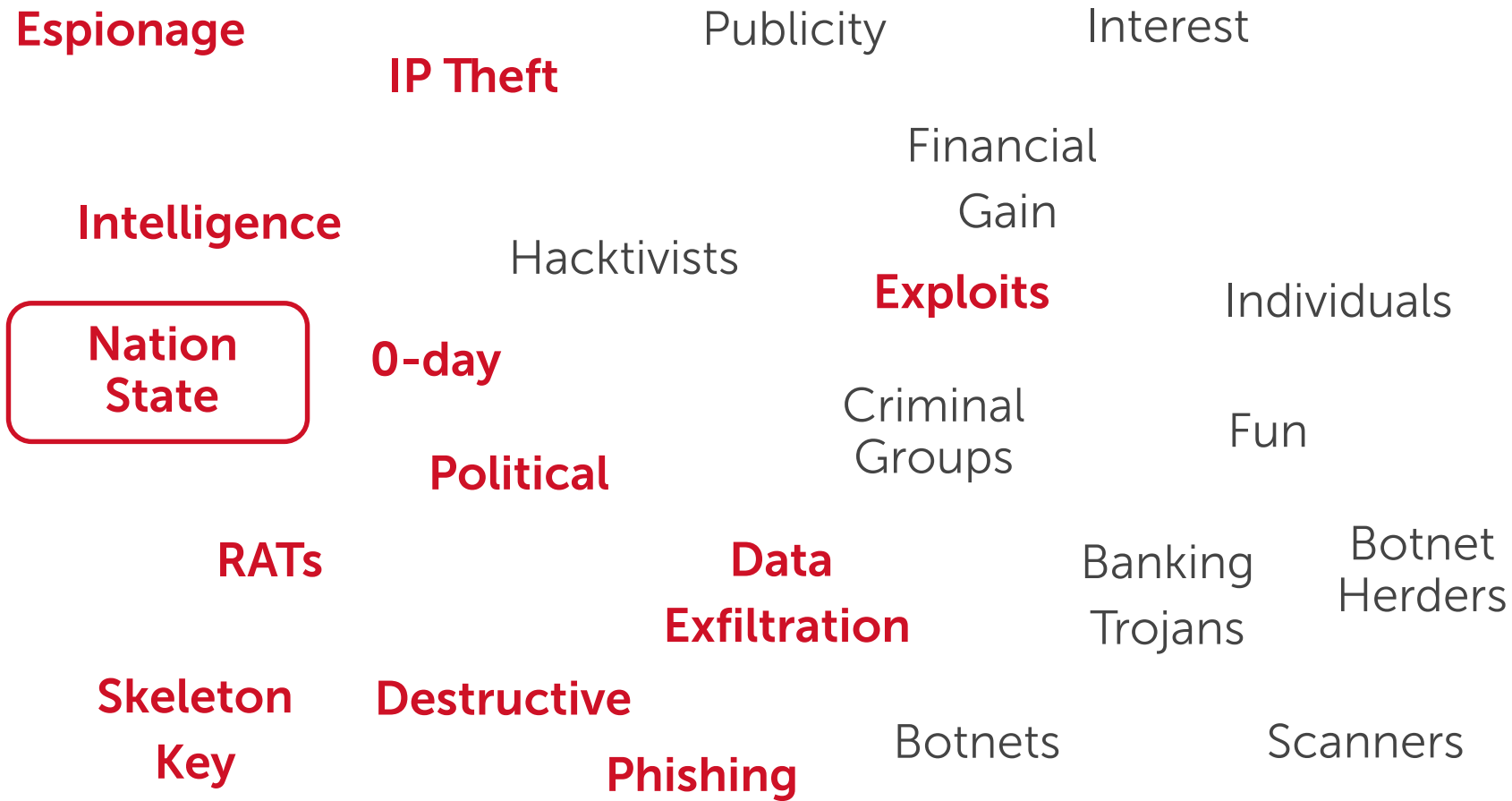
# The Threat Cloud – Botnet Herders



# The Threat Cloud – Criminal Groups

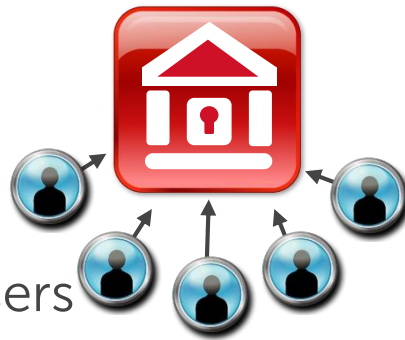
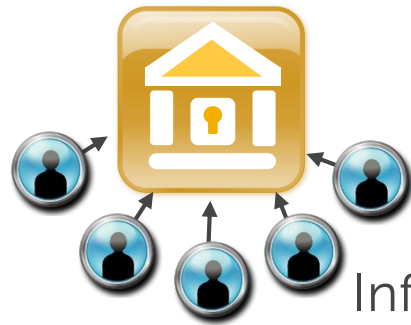


# The Threat Cloud – Nation State



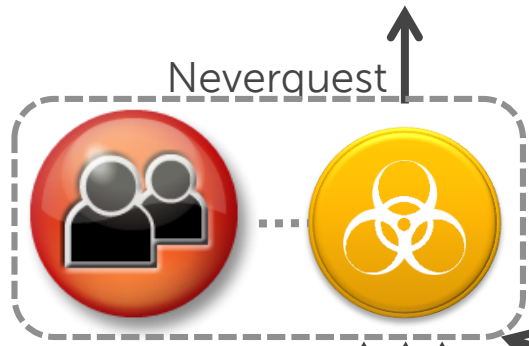
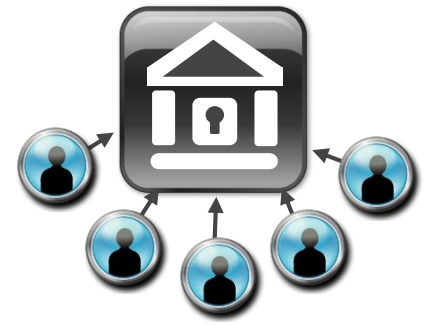
# Cyber Attacks - E-Crime

# Crime Groups

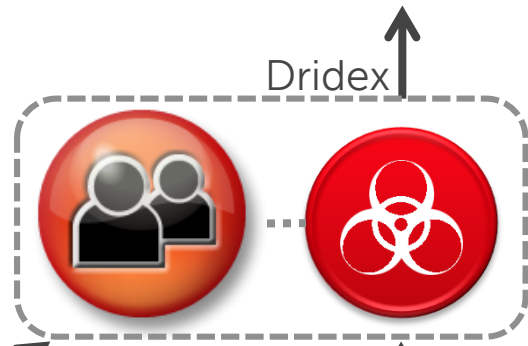


Infected users

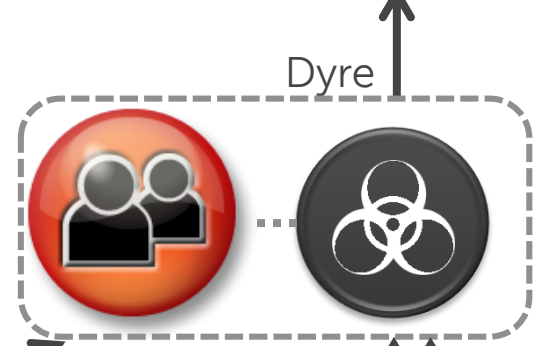
Banks



Neverquest



Dridex



Dyre



Affiliates



SecureWorks



# Bots, bots, bots...

Tofsee

**Cryptolocker**

**Cutwail**

ICEIX

NedSym

Lerspeng

Asprox

KINS

Citadel

Phorpiex

Shylock

Pushdo

Chanitor

**Upatre**

Pony

**Bugat**

Tinba

**GameOverZeus**

Torpig

Dirtjumper

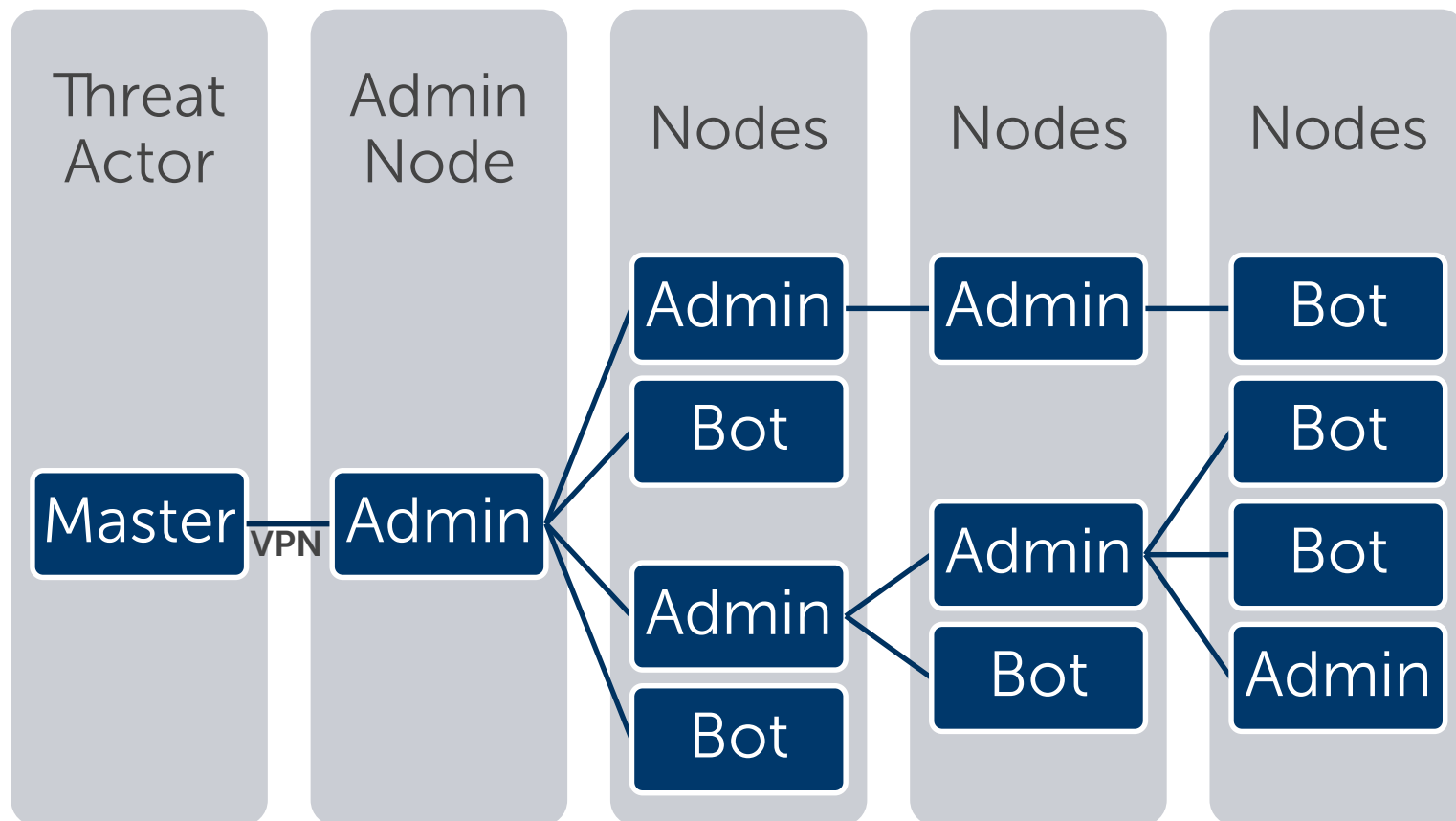
SmokeBot

Hesperbot

**Dyre**

Gozi

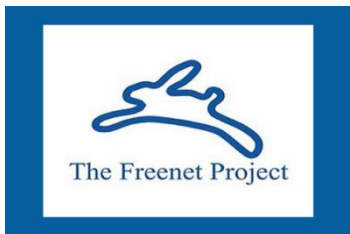
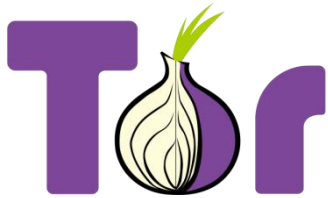
# Dridex P2P Structure



- 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



The screenshot shows the Evolution marketplace website. At the top, there is a navigation bar with the 'evolution' logo, a dropdown menu set to 'All', a search bar with the text 'Search for ...', and a 'Go' button. Below the navigation bar is a 'Home' link. On the left side, there is a 'Categories' section with a list of product categories and their respective item counts. On the right side, there is a 'Welcome' section with a light blue notice box, a 'Greetings' section with a welcome message, and a 'News' section with a birthday announcement.

Categories	Count
Drugs	20084
Fraud Related	2435
Guides & Tutorials	2702
Services	1187
Counterfeits	1438
Digital Goods	2560
Drug Paraphernalia	420
Electronics	207
Erotica	428
Jewellery	574
Lab Supplies	115
Miscellaneous	195
Weapons	268
Custom Listings	992

**Welcome**

**Notice!** Make sure to read our **Buyer's Guide** before ordering.

**Greetings**

We would like to welcome you to Evolution, a marketplace where established vendors can sell down to the new guy selling a product for the first time.

Evolution's goal is to combine the old and the new; using what made our predecessors great, infused with modern functionality and clean looks. It was designed and developed with simplicity in mind, and yet be as secure as possible.

Feel free to join us on the [forum](#) if you have any questions, bug reports or requests.

**- Evolution Team**

**News**

**Jan 14, 2015 — Happy Birthday!**

It is the greatest pleasure to announce that today [Evolution exists for exactly 1 year!](#) Thanks to all for your continued support!

# Banking Trojans

Upatre

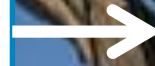
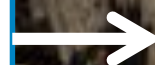
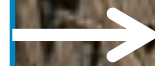
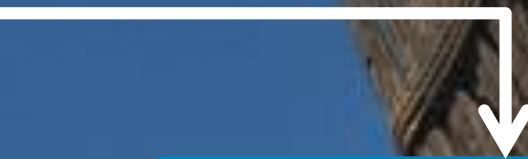
Dyre

Word with macro

Dridex

Chanitor

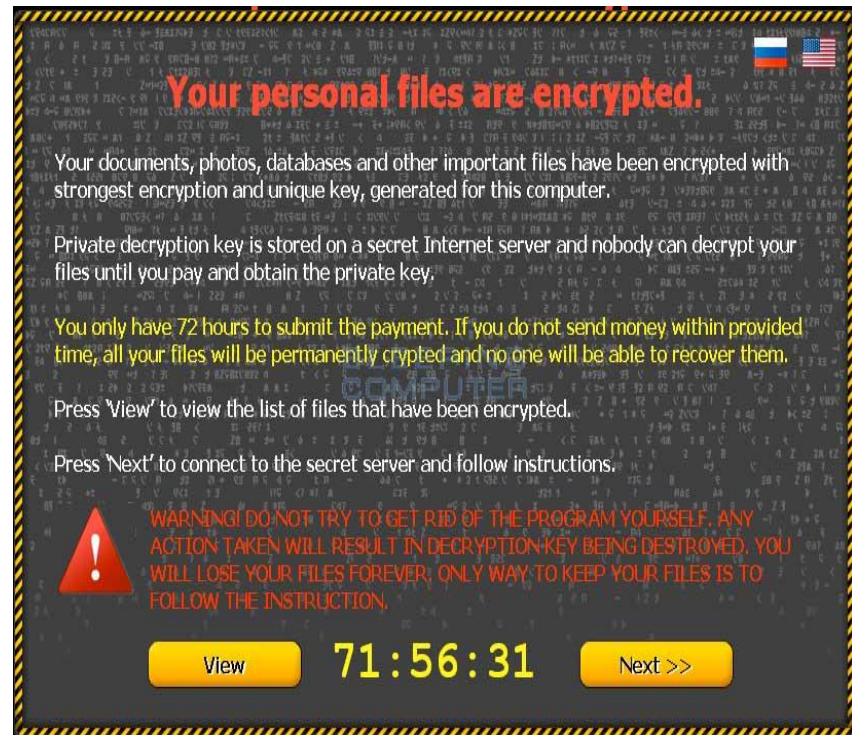
Gozi/Neverquest



# Cyber Attacks - Destroy / Ransom

# Crypto Ransomware – Constantly evolving

- 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

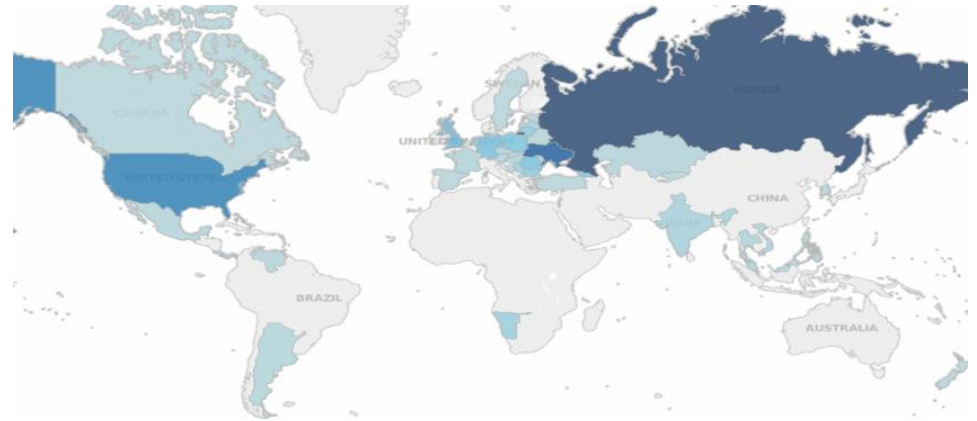
- The "Guardians of Peace" (GOP) demanded the cancellation of the planned release of the film *The Interview*
- US Government link Sony attack to North Korea



# 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)

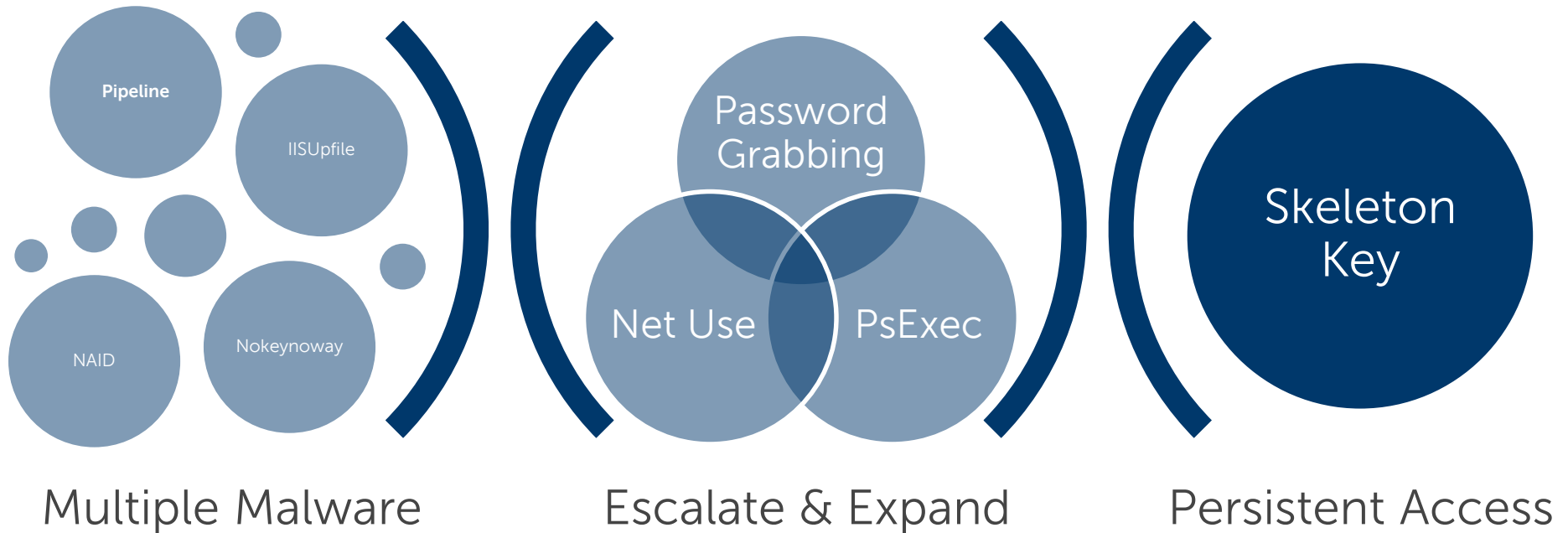




# Cyber Attacks - Nation State



# 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

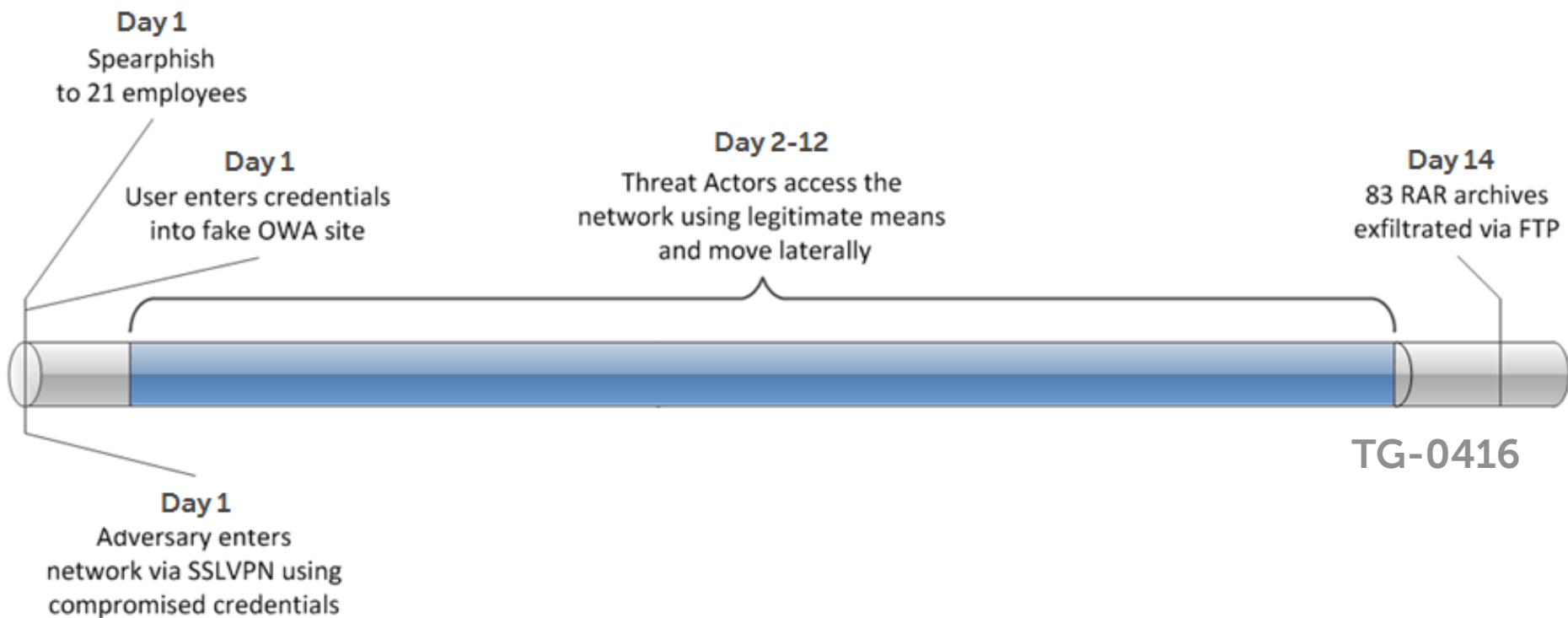
# Skeleton Key

Legitimate users can  
log in with normal  
password

Attacker can log in  
with the injected hash  
on ANY account



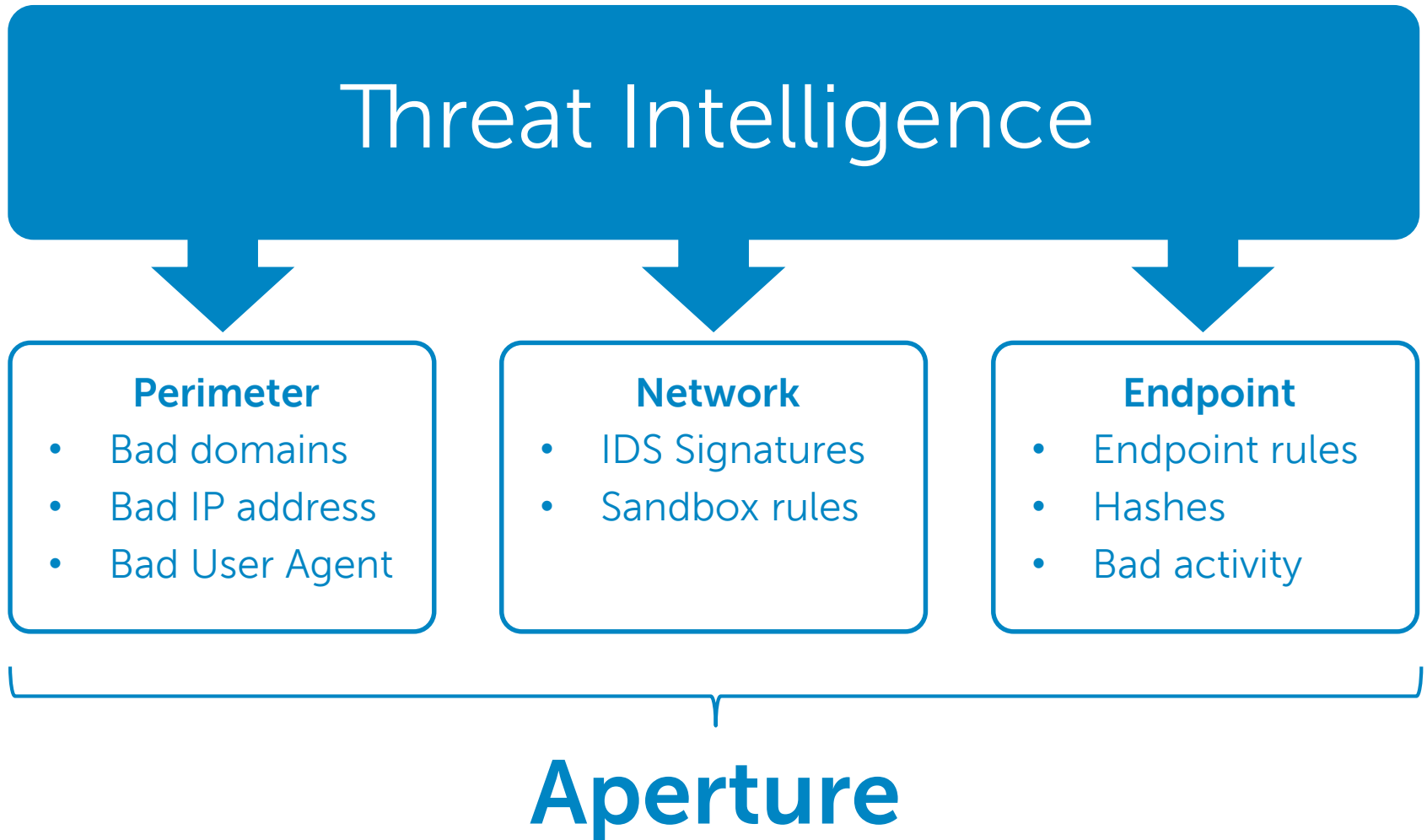
# Breach Without Malware



What to do  
about it

Intelligence  
+ Aperture

# Threat Intelligence



# 5 Pragmatic Security Steps





# Thank You

Bill Beverley – SecureWorks

SecureWorks

