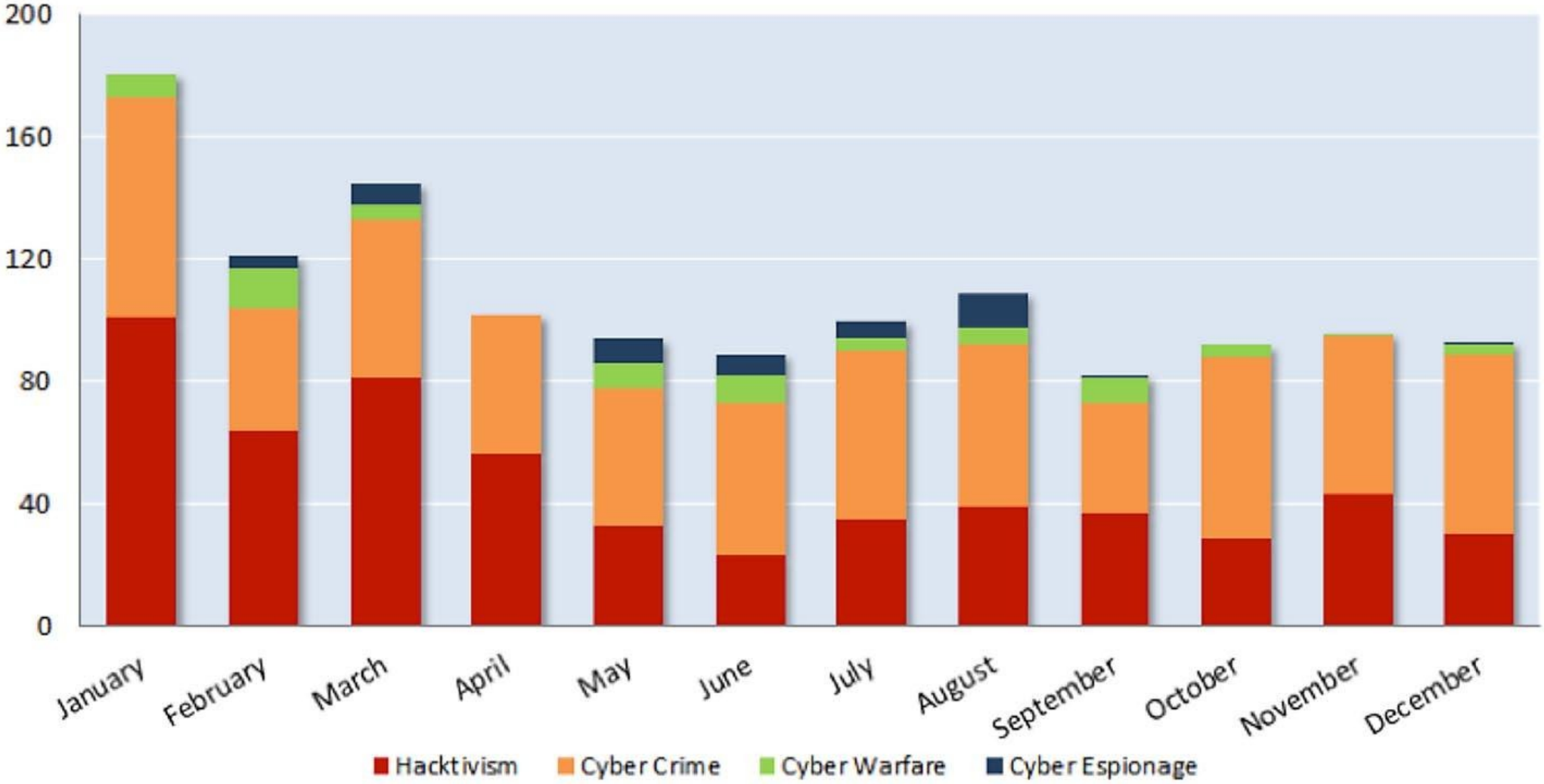
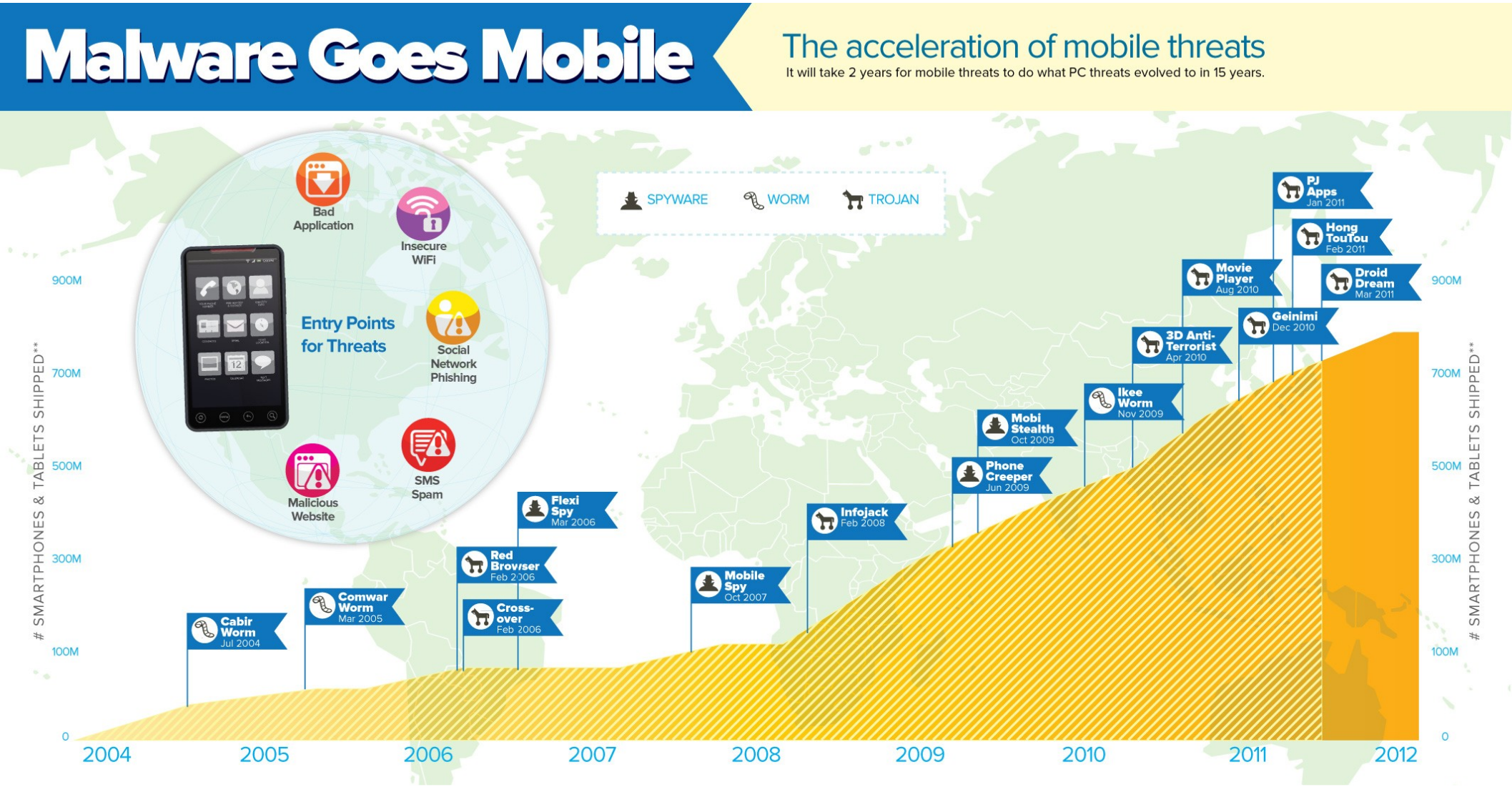

Cyber Security Trend 2015

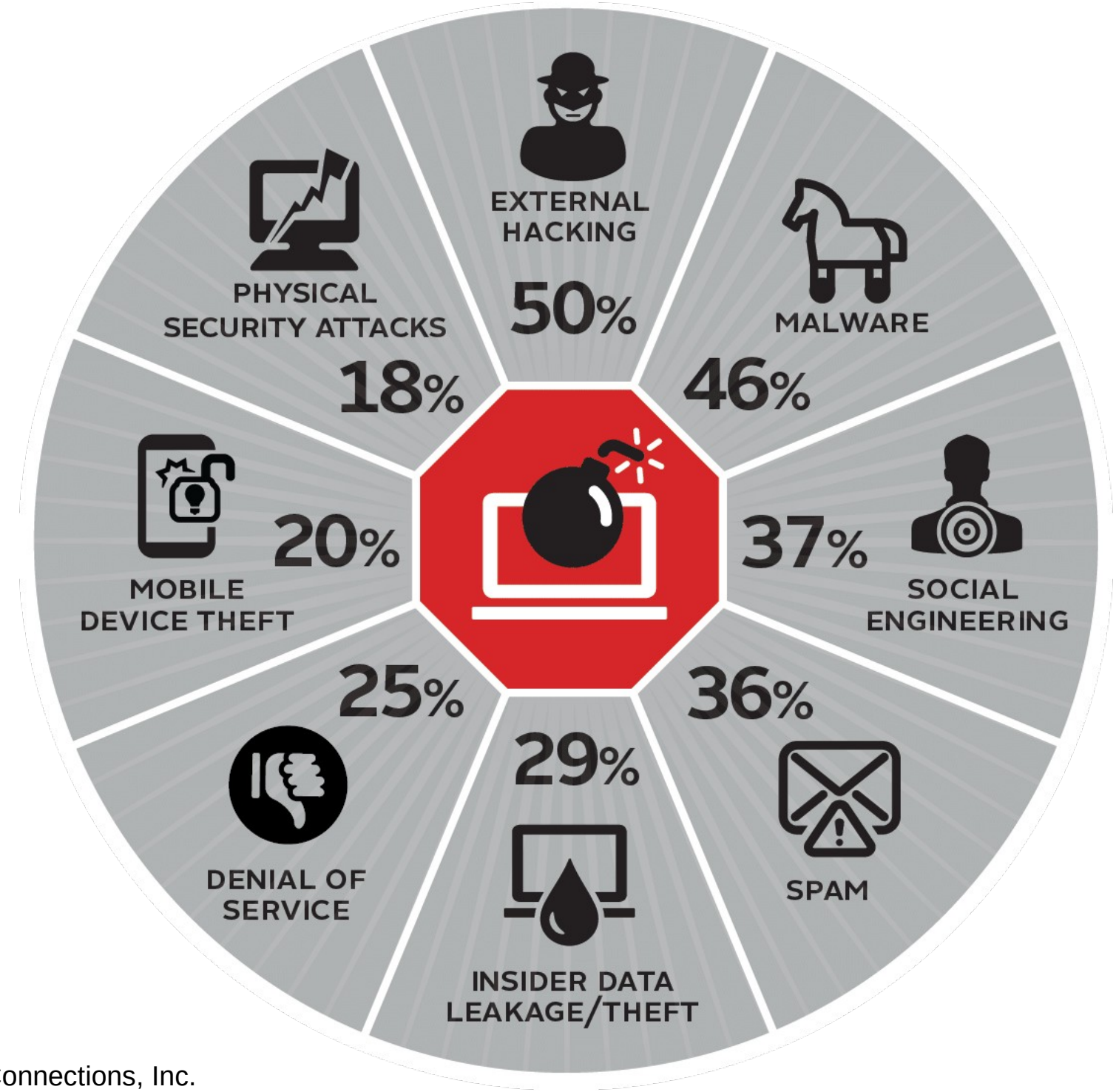
2013 Attack Trend (Drill down)





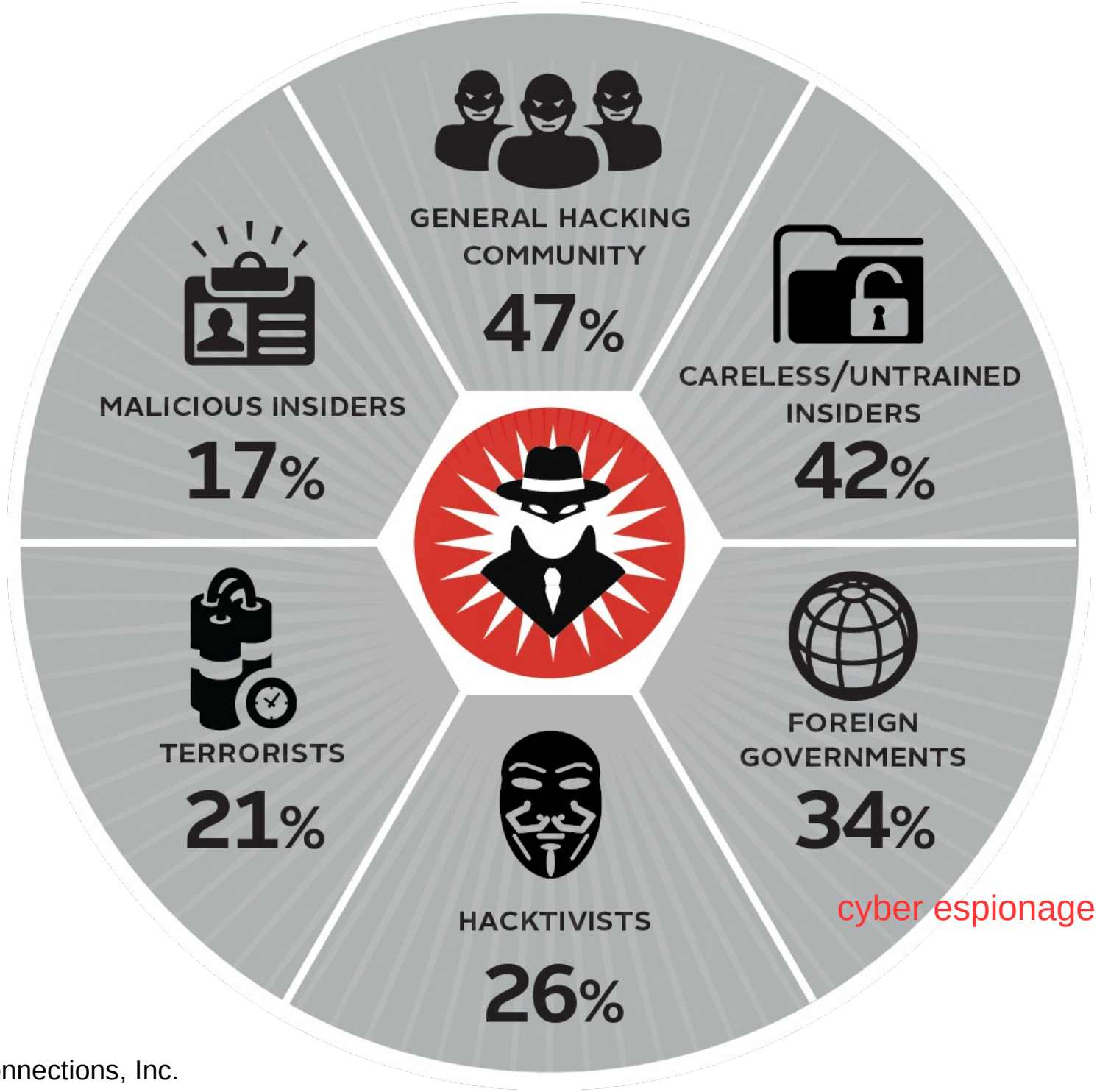
source: Lookout Mobile Security Data

Cyber Security Threat



source: 2014 Market Connections, Inc.

Security Threat Sources



cyber espionage

source: 2014 Market Connections, Inc.

Cyber Attack Trends

International Cyber Criminal

Social Media

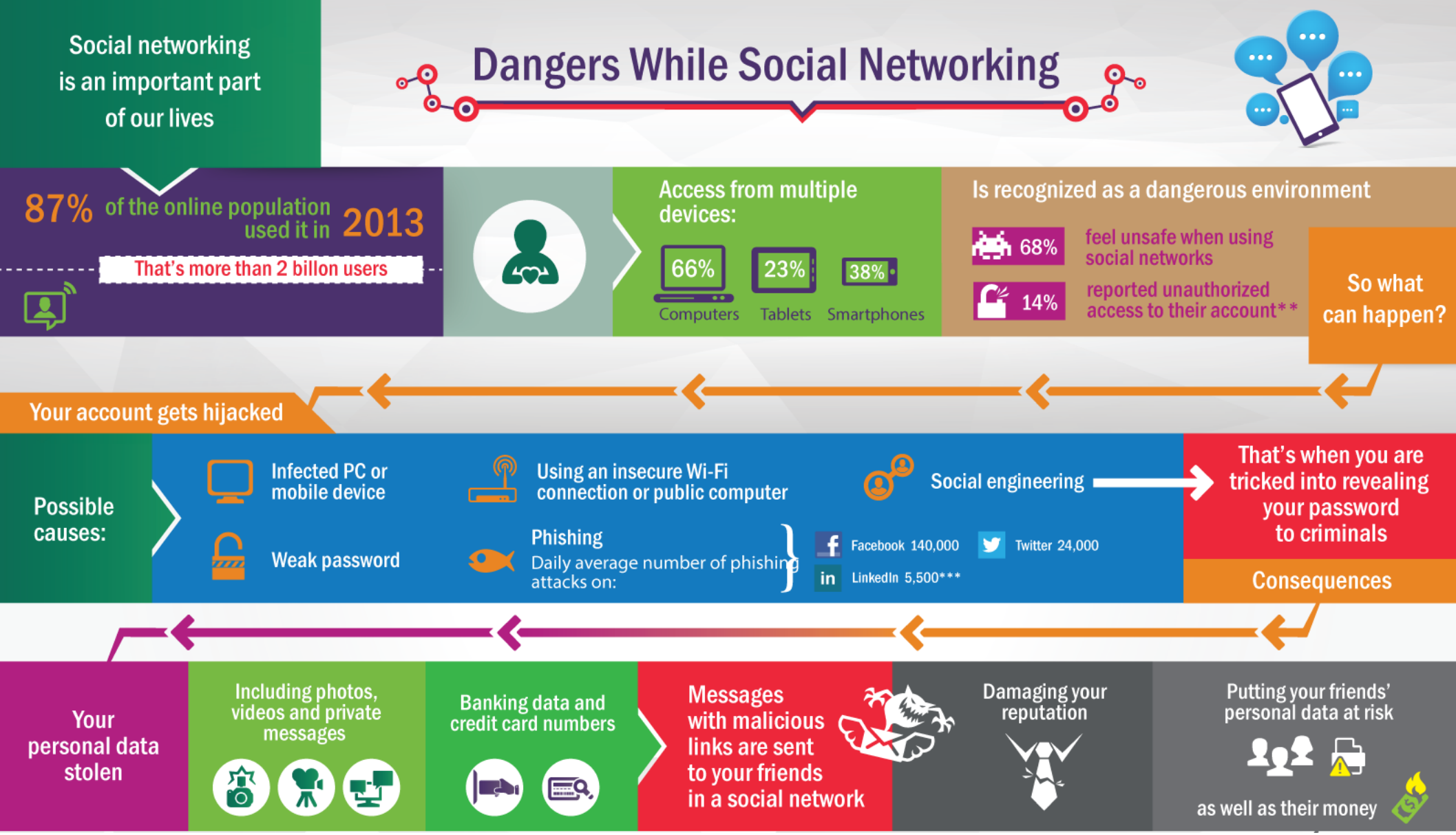
Advanced Persistent Threats

International Cyber Criminal

1. "Syrian Electronic Army" hacked many US websites, including New York Times & Huffington Post, stealing usernames & passwords.
2. Spamhaus faced the biggest Distributed Denial of Service (DDoS) attack in history, slowing down Internet service around the globe.
3. Basic malware from India had been hitting Pakistan, undetected, for over two months.
4. China faced its biggest attack in history when a Denial of Service (DoS) attack was launched on its domain, .cn.
5. A report released in May revealed that the US Electricity grid is under near constant attack.
6. "Anonymous" hacked a US Federal Reserve Bank website, stealing personal information from over 4,000 executives.
7. An attack on ticketing service, Vendini, exposed information from about 1 million accounts.
8. An attack on Twitter may have exposed the usernames, email addresses & passwords of as many as 250,000 users.
9. An attack on deals site LivingSocial exposed the personal information of 50 million users.
10. A 4-month breach of Schnuck's Grocery Store Chain compromised the credit card numbers of 2.4 million customers.

"Harder to track down and stop their illegal and harmful activities".

"A lack of international collaboration also makes it harder to track down hackers as they attack from multiple location".



source: Kaspersky

"spear phishing" and socially engineered attacks, cyber-criminals".

"social engineering attacks have also been on the rise, but at a slower phase".

Advanced Persistent Threat

Attacks that steal data, but do not destroy that data are also on the rise.

What makes these attacks so damaging is that such data theft can remain undetected for a long period of time.

Mobile Apps: Continuing Frontier for Cybercrime

- Explosive Growth of Mobile Devices
- Users who download from app stores may end up downloading malware instead
- cybercriminals take advantage of this fad by creating malicious and Trojanized apps

How do consumers use mobile apps?

- Games (most downloaded)
- Entertainment
- Social Networking
- Travel
- Productivity/Education
- Utilities
- Weather

Risks of Downloading apps

- The Android platform, has become the target of continuous cyber attacks due to its app distribution model
- other mobile platform users could have security issues too
- There are also third-party sites that provide alternative apps

Business Model: Apple iTunes

- limited to apps available for purchase on the iTunes App Store
- jailbreaking an iPhone, iPad, or iPod Touch enables users to install apps outside the App Store

Business Model: Android

- Users may opt to download apps from sites other than the Android Market
- Developers only need to register and pay a $25 registration fee

Threats

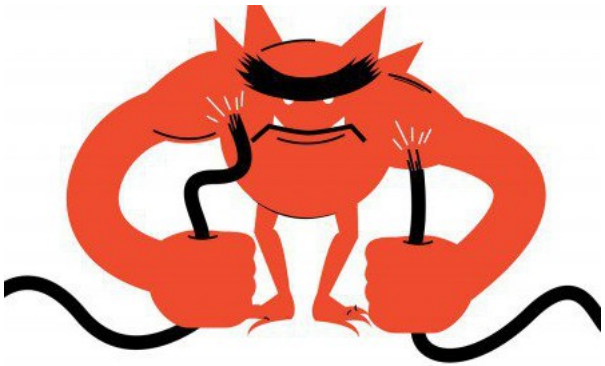
cybercriminal attacks to
infect devices
and spread malicious activities

Android Market
has been targeted
with several incidents
of malicious or Trojanized apps

3rd Party
app stores
expose more
potential risks to
users

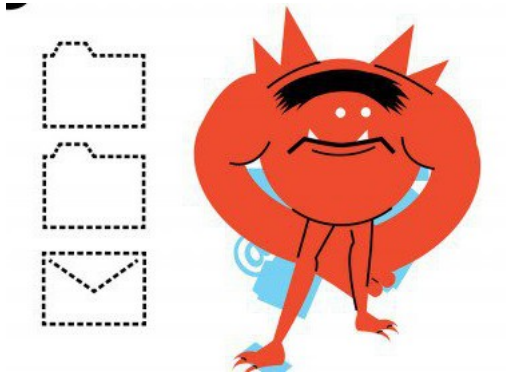
Data Stealer

Techniques	Implication
Steals information stored in the mobile device and sends it to a remote use	Stolen information maybe used for malicious purposes



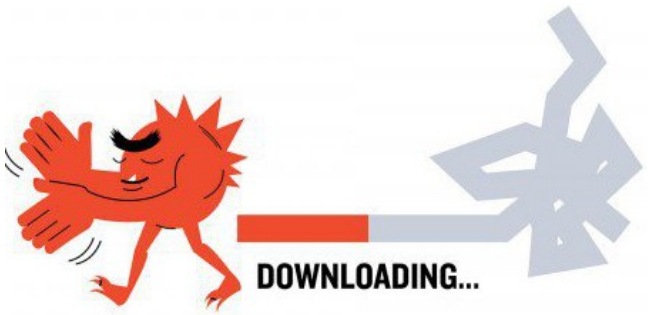
Premium Service Abuser

Techniques	Implication
Subscribes the infected phone to premium services without user consent	Unnecessary charges for services not authorized by users



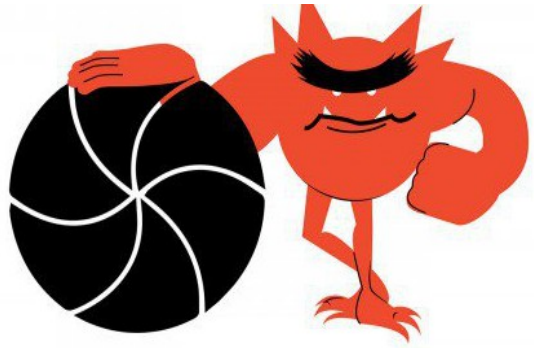
Click Fraudster

Techniques	Implication
Mobile devices are abused via clicking online ads without users' knowledge	Cybercriminals gain profit from these clicks



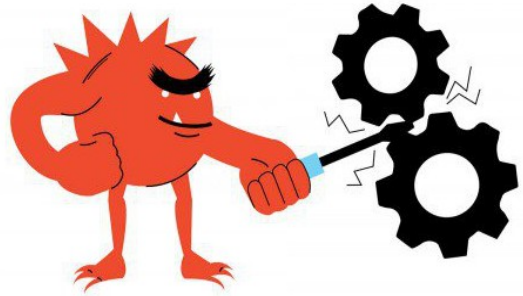
Malicious Downloader

Techniques	Implication
Downloads other malicious files and apps	Mobile device is vulnerable to more infection



Spying Tools

Techniques	Implication
Tracks user’s location via monitoring GPS data and sends this to third party	Cyber-crimnals track down location of users



Rooters

Techniques	Implication
Gains complete control of the phone, including their functions	Users' mobile devices are exposed to more threats

Cyber Defense - Trends

Active Approaches to Information Security

figure out what an attacker is after

gather information about an attacker

Attacking from a bot-net

Attacking through TOR

Why Current Strategies are not Working

OFFENSIVE

we will need to attack

DEFENSIVE

know our limitations

Why Current Strategies are not Working

Go back 5 or 6 years...What were they saying to defend networks?

Patch + AV !!

What they saying now?

Patch + AV !!

What is Honeypot

- A data point, service or system(s) intended to be interacted with by an attacker
- Often called many different names
  - Honeytoken
  - Honeytable
  - Honeynet
  - etc.
- Ideally it should replicate something valuable to you and/or your organization
- If the honeypot is interacted with the activity and, by extension, the actor is automatically considered malicious

The Use of Honeypot

look at honeypots in 2 different ways

- Research honeypots
- Production honeypots

focus on production honeypots for:

- Identifying malicious internal systems/users
- Identifying attacks that AV and IDS could not detect

To Learn about the attacks

Many teams use honeypots to learn about how attacks work

Can be very useful as a learning tool

Much like having a hacker ant-farm

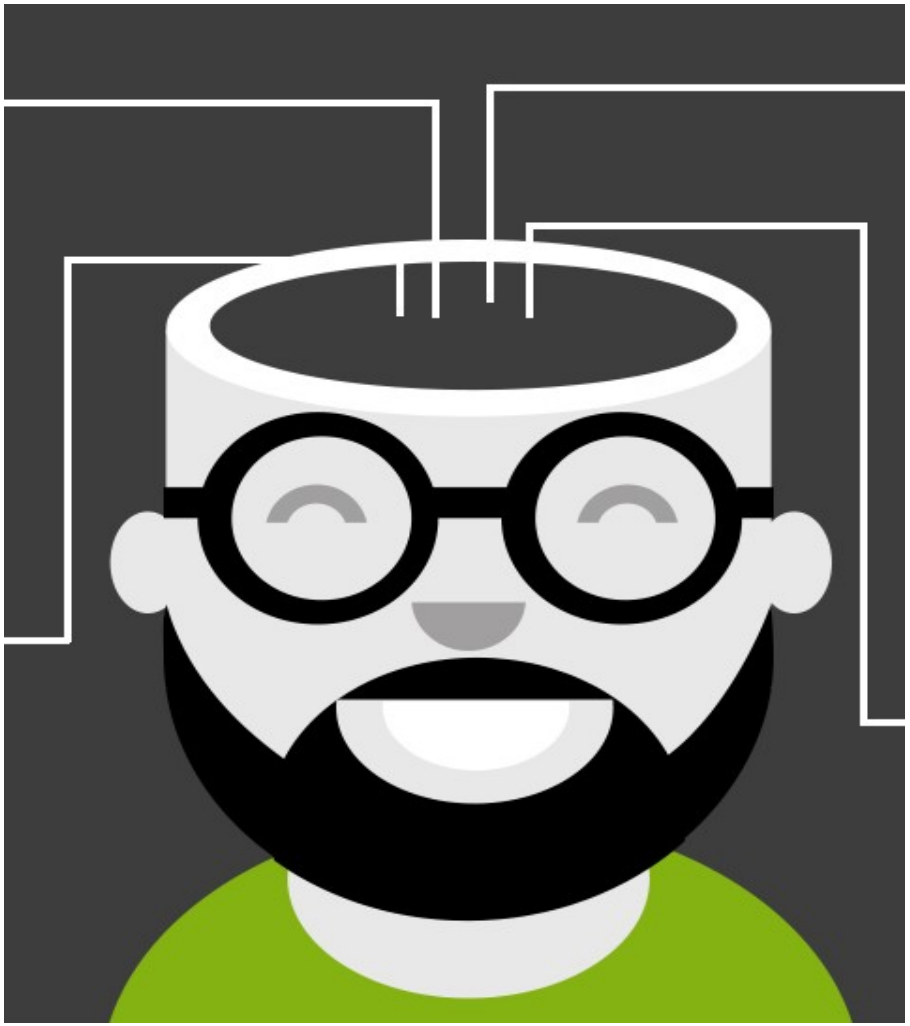
Can be a time sinker

Management often does not see the value

To Learn about the attackers

detect and clear?

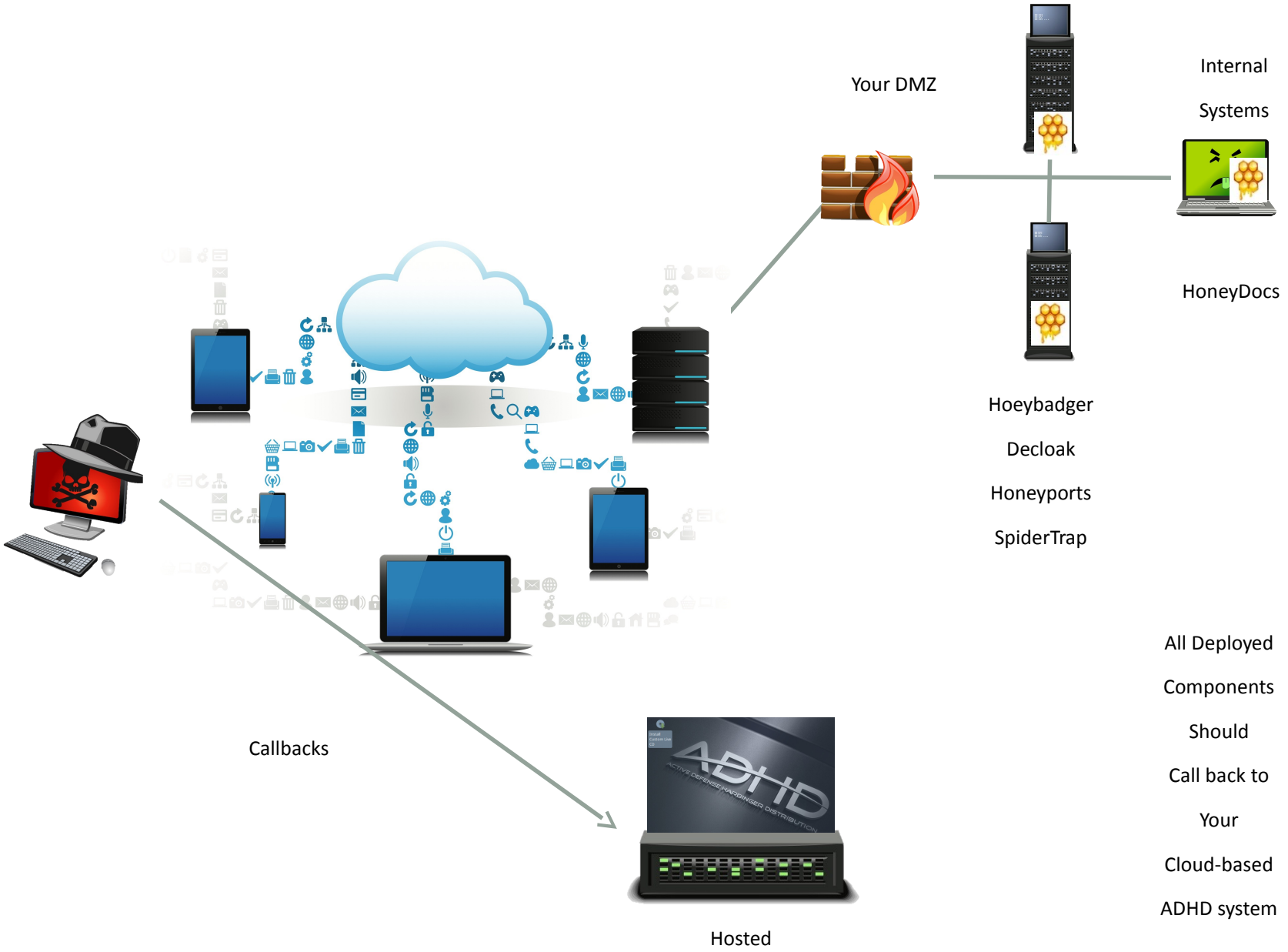
detect and learn?



what method they use?

what did they have access to?

“Honeypots give us great value in understanding the attacker’s skill and motivation”.


Your DMZ
Internal
Systems
HoneyDocs
Hoeybadger
Decloak
Honeyports
SpiderTrap
Callbacks
ADHD
Hosted
All Deployed
Components
Should
Call back to
Your
Cloud-based
ADHD system

THANK YOU

Ifik Arifin
AOSI/INIXINDO

ifikarifin@gmail.com