Notes

The Cisco Security Ninja program is a technical security awareness program created in 2012. The goal of this program is to change the security culture of Cisco from within.

This slide deck is a tailored module from within our first level, White Belt, with a few slides borrowed from Green Belt. The purpose of this deck is to summarize key security information for network or security engineers.

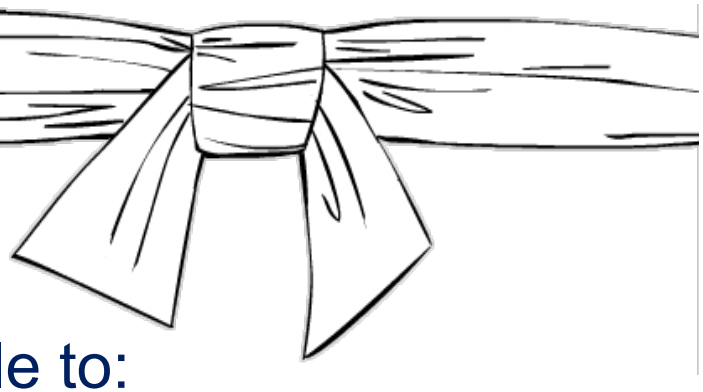
We are releasing this module to raise awareness and also to provide an example you could deploy in your organization!

Cisco Security Ninja Training

White Belt for a Network or Security Eng

Authored by: Chris Romeo

Learning Outcomes



By the end of this module, you will be able to:

- ✓ Understand some basic security terms that security professionals throw around
- ✓ Explain the state of the hacker economy and the impact of attacks
- ✓ Describe social engineering and what you can do to prevent it

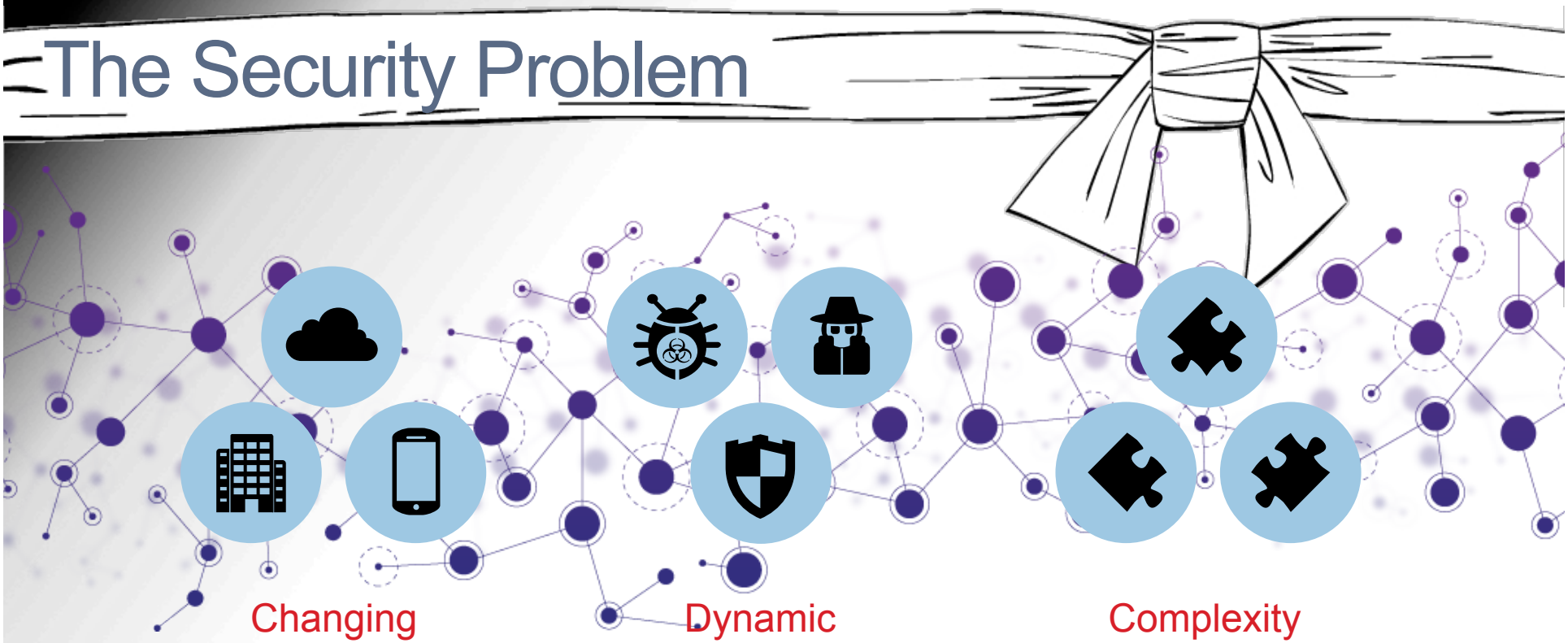
Why Do You Care?

The Defender's Dilemna

- Defender = The Protector
- Attacker = Needs only one entry point
- Advantage = The Attackers

Only **YOU** can secure your products!

The Security Problem



Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

Is it Secure? Consider C.I.A.

Information can only be **viewed by authorized** parties

Confidentiality

Of device, service, or data.

Integrity

Information is not **unexpectedly modified**

Availability

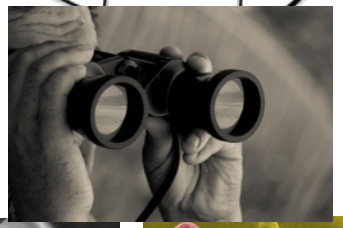
Information or resources are **available** when needed

Threats

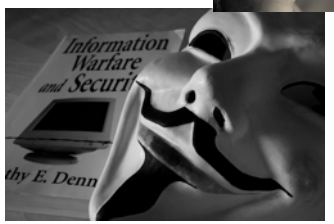
Threat
A potential danger that could cause harm to information or a system

https://flic.kr/p/56iS

https://flic.kr/p/6jTfiN



https://flic.kr/p/c5xUxS



https://flic.kr/p/9VUCrU

https://flic.kr/p/a7RGBX

Threat Agent
An entity that exploits a threat

Vulnerability

Vulnerability

A weakness, design or coding error, or lack of protection in a product that enables an attack

https://flic.kr/p/LhHyk

Vulnerabilities can result from Design, Programming, or Operational flaws.

Exploits and Attacks

Exploit
A practical method to take advantage of a specific vulnerability

Attack
The use of an exploit against an actual vulnerability

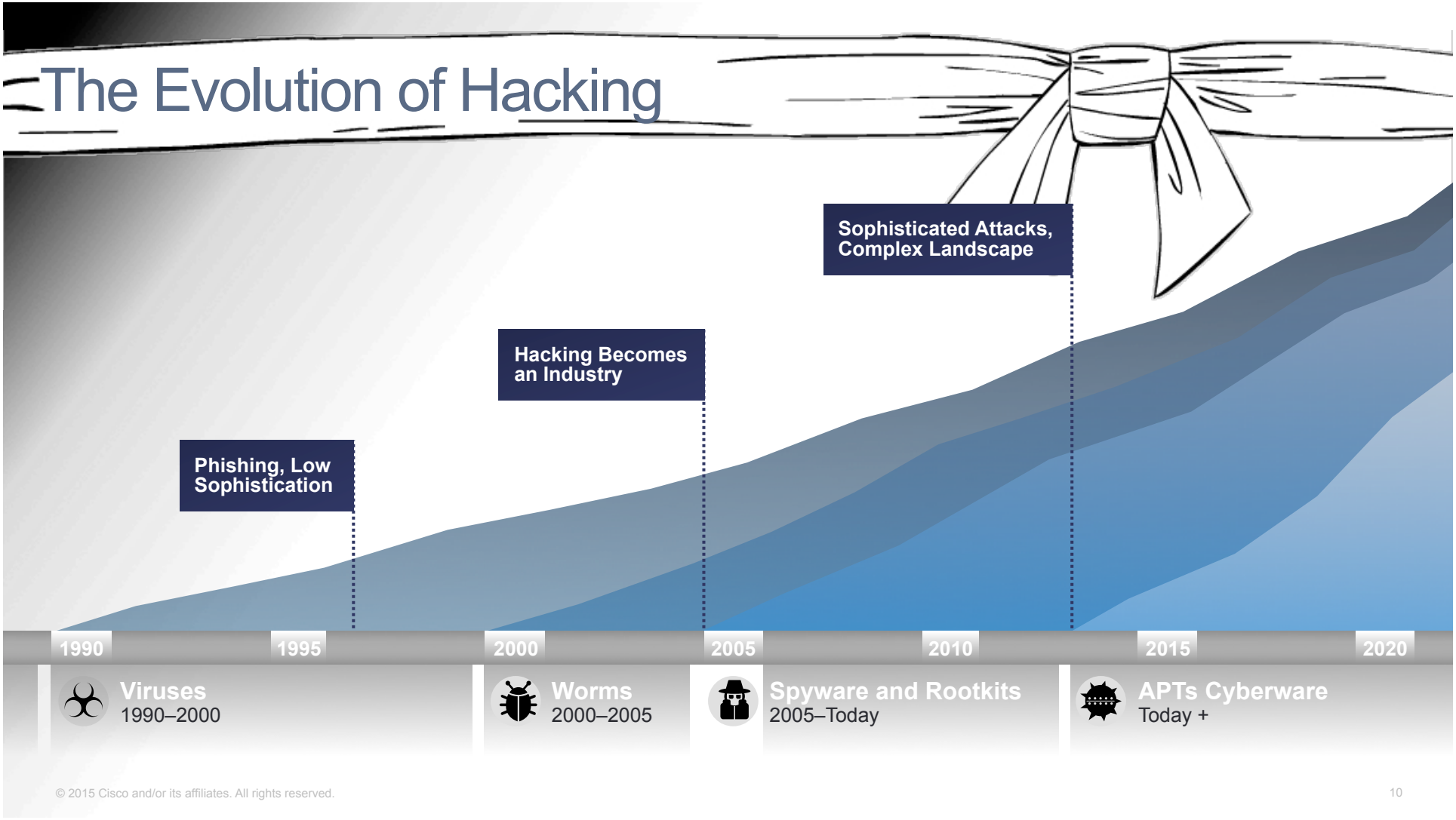
https://flic.kr/p/5EAwg3

Exploits and attacks go hand in hand.

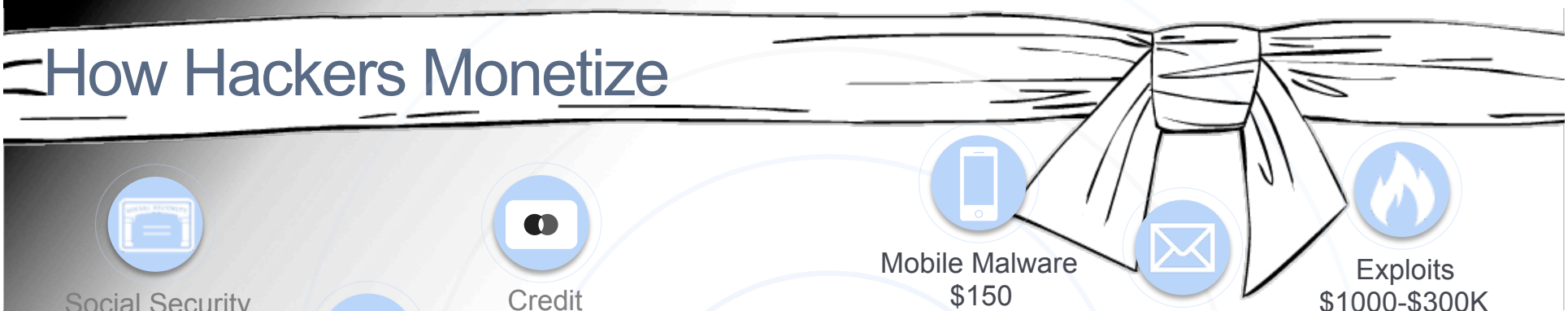
Attack Vector
A theoretical application of an exploit

Zero-Day Attack
An attack that exploits a previously unknown vulnerability for which there is not yet a defense

The Evolution of Hacking



How Hackers Monetize



Social Security
$1

Credit
Card Data
$0.25-$60

Mobile Malware
$150

Exploits
$1000-$300K

Spam
$50/500K emails

Medical
Record
>$50

Global Cybercrime Market: $450B-$1T

DDoS

DDOS
as a Service
~$7/hour

Bank Account Info
>$1000
depending on account type and balance

Malware
Development
$2500
(commercial malware)

Facebook Account
$1 for an account
with 15 friends

WELCOME TO THE HACKERS' ECONOMY

Top 3 Impacts of Security Failures

Damage to infrastructure

Increase in expenses

Loss of market share

What is Social Engineering?

The clever manipulation of the natural human tendency to trust

"Social engineering is using deception, manipulation and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail."

– Kevin Mitnick

Why am I vulnerable?

Social Engineers know their targets!

- Natural human desire to be helpful
- Tendency to trust people
- Desire to feel included or receive benefit
- Fear of getting into trouble
- Willingness to cut corners for a “good reason”

https://flic.kr/p/cHjZBw

Popular Social Engineering techniques

Warning: Social Engineering attacks often combine multiple techniques!

Impersonation

Posing as an employee or other authorized party to gain access or information

- Phone, e-mail, or in person
- "Act like you are supposed to be there"

Dumpster Diving

Collecting confidential information from improperly protected sources

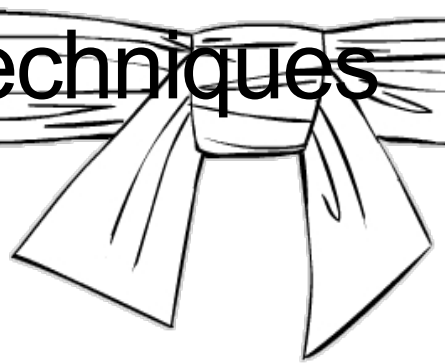
- Discarded documents
- Old hard drives
- May literally mean going through a dumpster!

Inference

Collecting and assembling "innocent" information from public sources to build a profile of a target

- Facebook
- LinkedIn
- Twitter
- Personal blog/website
- Public forums
- Improperly protected info

Popular Social Engineering Techniques



Warning: Social Engineering attacks often combine multiple techniques!

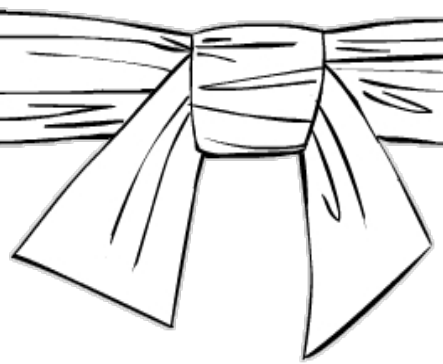
Phishing
Posing as a trustworthy entity to acquire confidential information

- Type of e-mail spoofing fraud
- Usernames, passwords, etc.

Spear Phishing
Phishing targeted at a specific person or group

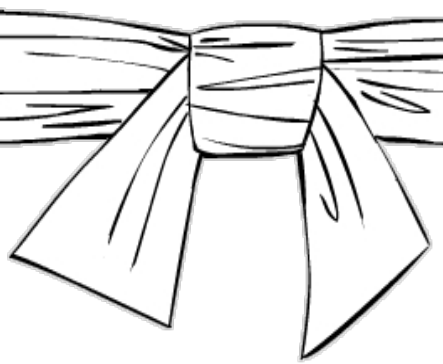
- Has detailed information meant to persuade the specific target

Key Take Aways



- ✓ Know the basic security terms of security professionals
- ✓ In the hacker economy, data is money, and the impact of attacks is damage to infrastructure, increase in expenses, and loss of market share
- ✓ Social engineers will use <u>any</u> and <u>all</u> information and tactics
  - Be suspicious; be prudent
  - Verify sources and trust your instincts

Notes



We hope this overview of our learning approach for the Cisco Security White Belt has been helpful. It is our goal to share our approach with the community, to assist in building technical security awareness within all organizations.

If you have any questions, please contact me

Chris Romeo

chromeo@cisco.com

@edgeroute