

UCCS University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

CS 4950/5950
Homeland Security &
Cybersecurity

Lesson 31
Cyber Crime

Rick White, Ph.D.
University of Colorado, Colorado
Springs



¹
Esc


1

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

In this lesson we ask ourselves,
“why not go after the
cybercriminals?”



²
Esc

2

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

- As we learned in Lesson 10, the 1984 Counterfeit Access Device and Computer Fraud & Abuse Act makes it illegal to access a computer without permission from the owner.
- A 1986 amendment made it a further crime to distribute malicious code, traffic passwords, or conduct denial of service attacks.



3
Esc

3

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

As we mentioned previously, anyone who commits a crime in this country is subject to United States law whether they live in this country or not.



4
Esc

4



Cyber Crime

- Sadly, cyber crime is a growth industry.
- **It is a growth industry because it is a low-risk high-reward venture.**



5

Esc

5



Cyber Crime


The latest report issued by McAfee, the 2018 Economic Impact of Cybercrime, estimates that somewhere between \$445 to \$608 billion is lost to cybercrime globally each year.



6

Esc

6




University of Colorado
Colorado Springs


CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

- Russia and North Korea are home to most prolific cyber thieves.
 - NK stole “tens of millions” from the SWIFT global bank network in 2016
 - Best cyber-criminals live in Russia where they need not fear extradition
- Ransomware is the fastest growing cybercrime
 - 6,000 online marketplaces sell ransomware products & services
- Cybercrime has become professionalized & sophisticated
 - Markets offer range of tools & services for criminally inclined
 - Customers can rent or buy exploit kits, bot-nets, and/or ransomware
- Cybercrime is diversifying:
 - Third-party Suppliers: Selling “vulnerabilities” to malware developers
 - Web injections modifying web sites to steal sensitive information

7


7





University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

- The reluctance of companies to admit loss is encouraged by competing needs to **protect their reputation and stem further damages** by loss of public confidence.
- This incentive towards remaining silent unwittingly assists criminals** with evading justice, and encourages them on to more exploits.



8


8



Cyber Crime

The two most common exploitation techniques—**social engineering**, where users are tricked into granting access, and vulnerability **exploitation** where a programming or implementation failure may be leveraged to gain access—are both surprisingly cheap.



9

Esc

9



Cyber Crime

- Moreover, few of the biggest cybercriminals have been caught or, in many cases, even identified.
- This combination of low-cost and low-risk makes cybercrime almost irresistible.



10

Esc

10



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Cyber Crime

- The most important loss from cybercrime is the theft of intellectual property and confidential business information.
- Intellectual property is a major source of **competitive advantage** for companies and for countries.
- The loss of intellectual property means **fewer jobs, fewer high-paying jobs, less innovation, and slower technological improvement.**



11

Esc

11



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Cyber Crime

- The US Department of Commerce estimates that **\$200 to \$250 billion worth of intellectual property is lost each year to cybercrime.**
- The European Organization for Economic Development estimates higher losses at about \$638 billion annually.



12

Esc

12



University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Cyber Crime

- **Financial crime is the second largest source of direct loss to cybercrime.**
- In Mexico, banks lose up to \$93 million annually.
- In Japan, it is estimated that banks lose about \$110 million annually.
- The 2013 hack against the US retailer Target cost banks more than \$200 million.
- Retailers in Britain reported lost more than \$850 million in 2013.



13

Esc

13



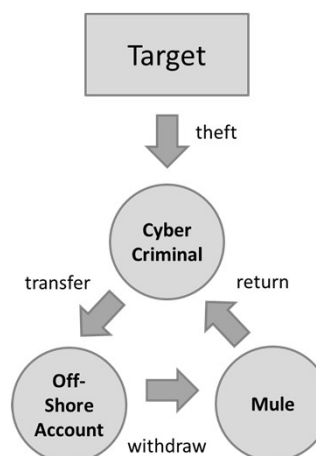
University of Colorado
Colorado Springs

CS4950/5950

Homeland Security & Cybersecurity

Cyber Crime

- These crimes are carried out by professional gangs, some **with significant organizational abilities.**
- Among the techniques employed by hackers, after gaining access to a bank account, they will transfer the funds to a third party called a "mule" who will "launder", or shuffle the money in some fashion to eliminate traces to its origin, before forwarding it to an overseas bank to where the hacker owns an account.



14

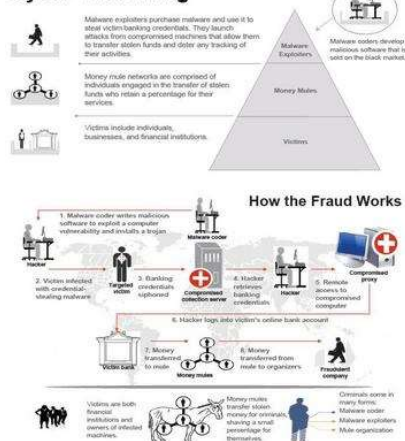
Esc

14

Cyber Crime

- The theft of \$45 million from two banks in the Middle East involved the recruitment and use of 500 mules around the world, in this case, by using cloned debit cards to withdraw money from ATMs, keep a portion for themselves, and send the rest back to the hackers.
- It is estimated that there are 20 to 30 cybercrime groups in eastern Europe with **advanced capability to overcome almost any cyber defense.**

Cyber Theft Ring



15

Esc

15

Cyber Crime

- Finally, it is very difficult to trace a cybercrime back to a cybercriminal.
- Cybercriminals employ many techniques to hide their tracks and leave false indicators.**



16

Esc


16

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

- **Accordingly, criminal attribution is highly problematic.**
- The same is true for state-sponsored cyber espionage.



17
Esc


17

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Cyber Crime

- **Without incontrovertible proof, it is difficult to retaliate.**
- And a wily cyber agent is sure to make any evidence questionable.



18
Esc


18

UCCS University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?



19

Esc