



# An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso  
[eamoroso@tag-cyber.com](mailto:eamoroso@tag-cyber.com)

# Required Text – \$9.99 Download from Amazon.com \$25.00 Printed Paperback Book from Amazon.com **From CIA to APT: An Introduction to Cyber Security** Edward G. Amoroso & Matthew E. Amoroso

amazon Try Prime Books from cia to apt Shop Back to School Departments Browsing History Edward's Amazon.com Today's Deals Gift Cards & Registry Sell Help EN Hello, Edward Account & Lists Orders Try Prime Cart Books Advanced Search New Releases NEW! Amazon Charts Best Sellers & More The New York Times® Best Sellers Children's Books Textbooks Textbook Rentals Sell Us Your Books Best Books of the Month < Back to search results for "from cia to apt"

**From CIA to APT: An Introduction to Cyber Security** Paperback – August 11, 2017  
by Edward G. Amoroso (Author), Matthew E. Amoroso (Author)  
Be the first to review this item  
See all 2 formats and editions  
Kindle \$0.00 kindleunlimited Paperback \$25.00  
This title and over 1 million more available with Kindle Unlimited  
\$9.99 to buy  
2 New from \$25.00  
Most introductory books on cyber security are either too technical for popular readers, or too casual for professional ones. This book, in contrast, is intended to reside somewhere in the middle. That is, while concepts are explained in a friendly manner for any educated adult, the book also necessarily includes network diagrams with the obligatory references to clouds, servers, and packets. But don't let this scare you. Anyone with an ounce of determination can get through every page of this book, and will come out better informed, not only on cyber security, but also on computing, networking, and software. While it is true that college students will find the material particularly accessible, any adult with the desire to learn will find this book part of an exciting new journey. A great irony is that the dizzying assortment of articles, posts, and books currently available on cyber security makes it difficult to navigate the topic.  
Read more  
Report incorrect product information.

Look inside ↗  
  
Flip to back  
See all 2 images

Buy New \$25.00  
Qty: 1  
FREE Shipping.  
In Stock.  
Ships from and sold by Amazon.com.  
Gift-wrap available.  
 Yes, I want FREE Two-Day Shipping with Amazon Prime  
Add to Cart  
Turn on 1-Click ordering for this browser  
Want it Wednesday, Aug. 30? Order within 19 hrs 39 mins and choose Two-Day Shipping at checkout. Details  
Ship to:  
Edward Amoroso- Sparta - 07871 ▾

## Required Week Two Readings

1. “Smashing the Stack for Fun and Profit,” AlephOne

[https://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack\\_smashing.pdf](https://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf)

2. Chapters 5 through 8: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso

Twitter: @hashtag\_cyber

LinkedIn: Edward Amoroso

Week 2

A wide-angle photograph of a modern architectural space, likely a lobby or atrium. The ceiling is a massive, intricate grid of glass panels supported by a steel framework. A large, dark, cylindrical object, possibly a trash can or a piece of equipment, is positioned in the center foreground. To the left, a white wall features a large, partially visible graphic or mural. The overall atmosphere is bright and airy due to the extensive use of glass.

**Mr. Sasser here for his 9:30,**

**Week 2: Incidents, Trojans, Worms, and Attacks**

# TO ENGINEER IS HUMAN

The Role of Failure in Successful Design



With a new afterword by the author



"Serious, amusing, probing,  
sometimes frightening  
and always literate."  
—Los Angeles Times

# HENRY PETROSKI

Author of *THE EVOLUTION OF USEFUL THINGS*



# What Can We Learn from Major Incidents?

Jan 2014



## 40 Million Credit Cards Stolen from Target

- Hacked third-party vendor access unnoticed from 12/2/13 to 1/16/14
- CEO and CIO of Target apologized and resigned
- Remediation/legal costs: \$162M (Target) and \$200M (Banks)

May 2014



## 145 Million eBay Users Hacked

- Compromised name, encrypted password, email, home address, etc.
- Companywide password reset function was used in the attack.
- “The focus is on recovery,” CEO John Donahoe.

Sept 2014



## Five Month Undetected Attack at Home Depot

- Compromised 56 million customer payment cards
- CEO apologized publicly after the cyber attack
- Famous security budget retort from ex-employee: “We sell hammers.”

Sept 2014



## 76 Million Households Hit by JPMC Breach

- Customer contact information – name, email, address, and phone
- 2014 attack blamed on Russian hackers by FBI
- CEO Jamie Dimon claims increasing JPMC Cyber Security budget by \$250M

Nov 2014



## Sony Destructively Hacked by North Korea

- Destructive malware attack ruined Sony compute infrastructure
- Revealed corporate emails including racist remarks about Pres. Obama
- “It was an attack on our freedom of expression.” DHS Secretary Johnson

Feb 2015

## The Details

- Company notified feds immediately
- No information compromised
- Massive database hacked

Anthem. 

JUST IN

FBI INVESTIGATING LATEST DATA BREACH  
ANTHEM INC. CREDITED FOR PROMPTLY NOTIFYING AUTHORITIES

#abc15



## 80 Million Medical Records Stolen from Anthem

- Two month process to notify astonished customers
- Abnormal system behavior went unnoticed for several months
- “I want to personally apologize to each of you.” Joseph Swedish, CEO

Mar 2015



## 11 Million Premera Customer Insurance Records

- Thirty-eight class action law suits based on 2015 attack
- Name, birthdate, SSN, address, bank account info, claim info, etc.
- “Privacy of our members’ personal information remains a priority.”



## Hackers Nab Data on 18,000 Penn State Students

- Started in September 2012, continued through mid-2014
- University claims attack carried out by Chinese threat actor
- CISO being recruited (\$300K- \$700K) – Avg. Public College Pres. (\$428K)

June 2015



## Sixteen Month Undetected OPM Breach

- Background and thumbprints for 15% of the US workforce
- Director Katherine Archuleta resigned 7/15
- Military group from PRC most likely malicious actor

June 2015



## Hackers Breach Harvard University Credentials

- Involved eight colleges (Arts & Sciences, Divinity, Radcliffe, etc.)
- University has no clear understanding of what happened or how
- FAQ suggests that everyone change their passwords

Oct 2015

# Letter to Consumers



## T-Mobile CEO on Experian's Data Breach

I've always said that part of being the Un-carrier means telling it like it is. Whether it's good news or bad, I'm going to be direct, transparent and honest.

We have been notified by Experian, a vendor that processes our credit applications, that they have experienced a data breach. The investigation is ongoing, but what we know right now is that the hacker acquired the records of approximately 15 million people, including new applicants requiring a credit check for service or device financing from September 1, 2013.

### 15 Million T-Mobile Records via Experian Breach

- Experian providing third-party marketing services to T-Mobile
- Name, address, SSN, birth date, passport/driver's license, etc.
- "T-Mobile's Legere 'Incredibly Angry' about Breach" – News Reports

Nov 2015



## 200,000 Comcast Customer Records Exposed

- Company reported 200,000 customer records “exposed to hackers”
- 590,000 customer records for sale on Dark Web for \$1,000.00
- Company requested that customers change their passwords

Dec 2015



Plant supporting Stroganovka,  
outside Simferopol, Crimea

## Hackers Shut Power to 80,000 Ukrainian Citizens

- Hacked Power Company 1: Prykarpattyoblenergo Electric Utility
- Hacked Power Company 2: Kyivoblenergo Electric Utility
- Affected Six More Companies with BlackEnergy Trojan Horse

Jan 2016



## 191 Million US Voter Records Compromised

- NationBuilder collects information and provides as-a-service
- “We strongly believe in making voter information more accessible to political campaigns and advocacy groups,” NationBuilder’s CEO Jim Gilliam

Mar 2016



## Hackers Sell 1.5 Million Customer Records

- 1.5 million Verizon customer records stolen from the company
- Sale price: \$100,000 for the entire package on the Dark Web
- Verizon blamed an exploitable flaw in their Website

Apr 2016



## 1,025 Wendy's Stores Hit by Credit Card Breach

- Blamed on unnamed third-party with access to company
- Company hit with class action lawsuit after the breach
- Initial statement under-estimated impact by the company initially

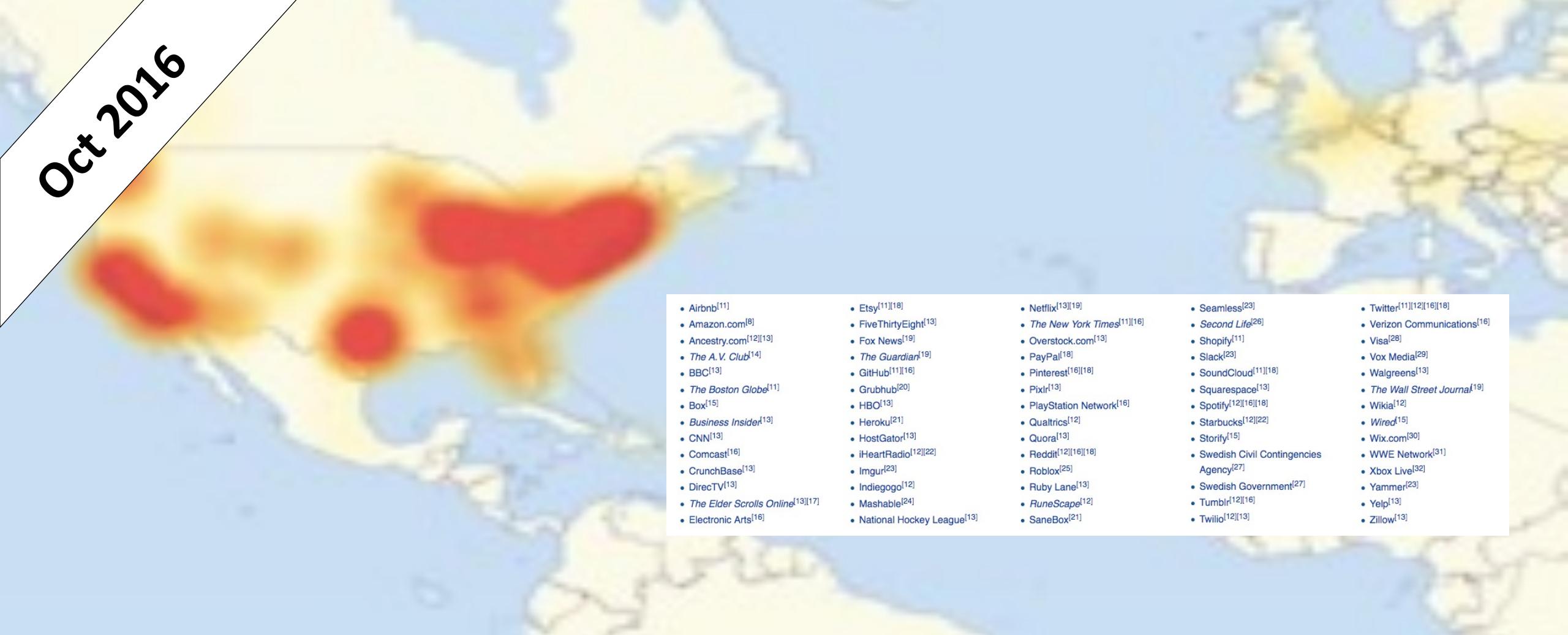
May 2016



## 427 Million Stolen MySpace Passwords

- Hacker selling batch for \$2800 payment
- Hacker also claims to have data on 164M LinkedIn Accounts
- Danger: Do not reuse passwords across accounts

Oct 2016

- 
- Airbnb<sup>[11]</sup>
  - Amazon.com<sup>[8]</sup>
  - Ancestry.com<sup>[12][13]</sup>
  - The A.V. Club<sup>[14]</sup>
  - BBC<sup>[13]</sup>
  - The Boston Globe<sup>[11]</sup>
  - Box<sup>[15]</sup>
  - Business Insider<sup>[13]</sup>
  - CNN<sup>[13]</sup>
  - Comcast<sup>[16]</sup>
  - CrunchBase<sup>[13]</sup>
  - DirecTV<sup>[13]</sup>
  - The Elder Scrolls Online<sup>[13][17]</sup>
  - Electronic Arts<sup>[16]</sup>
  - Etsy<sup>[11][18]</sup>
  - FiveThirtyEight<sup>[13]</sup>
  - Fox News<sup>[19]</sup>
  - The Guardian<sup>[19]</sup>
  - GitHub<sup>[11][16]</sup>
  - Grubhub<sup>[20]</sup>
  - HBO<sup>[13]</sup>
  - Heroku<sup>[21]</sup>
  - HostGator<sup>[13]</sup>
  - iHeartRadio<sup>[12][22]</sup>
  - Imgur<sup>[23]</sup>
  - Indiegogo<sup>[12]</sup>
  - Mashable<sup>[24]</sup>
  - National Hockey League<sup>[13]</sup>
  - Netflix<sup>[13][19]</sup>
  - The New York Times<sup>[11][16]</sup>
  - Overstock.com<sup>[13]</sup>
  - PayPal<sup>[18]</sup>
  - Pinterest<sup>[16][18]</sup>
  - Pixlr<sup>[13]</sup>
  - PlayStation Network<sup>[16]</sup>
  - Qualtrics<sup>[12]</sup>
  - Quora<sup>[13]</sup>
  - Reddit<sup>[12][16][18]</sup>
  - Roblox<sup>[25]</sup>
  - Ruby Lane<sup>[13]</sup>
  - RuneScape<sup>[12]</sup>
  - SaneBox<sup>[21]</sup>
  - Seamless<sup>[23]</sup>
  - Second Life<sup>[26]</sup>
  - Shopify<sup>[11]</sup>
  - Slack<sup>[23]</sup>
  - SoundCloud<sup>[11][18]</sup>
  - Squarespace<sup>[13]</sup>
  - Spotify<sup>[12][16][18]</sup>
  - Starbucks<sup>[12][22]</sup>
  - Storify<sup>[15]</sup>
  - Swedish Civil Contingencies Agency<sup>[27]</sup>
  - WWE Network<sup>[31]</sup>
  - Xbox Live<sup>[32]</sup>
  - Yammer<sup>[23]</sup>
  - Yelp<sup>[13]</sup>
  - Twilio<sup>[12][13]</sup>
  - Zillow<sup>[13]</sup>
  - Twitter<sup>[11][12][16][18]</sup>
  - Verizon Communications<sup>[16]</sup>
  - Visa<sup>[28]</sup>
  - Vox Media<sup>[29]</sup>
  - Walgreens<sup>[13]</sup>
  - The Wall Street Journal<sup>[19]</sup>
  - Wikia<sup>[12]</sup>
  - Wired<sup>[15]</sup>
  - Wix.com<sup>[30]</sup>

## DYN DDOS Attack

- Massive DDOS attack (possibly by Anonymous)
- Caused outages across major North American services
- Botnet: Cameras, gateways, baby monitor, and other IoT devices

Nov 2016

hate. The South will rise again!



**South United**

Community

137,138 people like this.

Like Page



Army of Jesus

Sponsored

Like Page

Today Americans are able to elect a president with godly moral principles. Hillary is a Satan, and her crimes and lies had proved just how evil she is. And even though Donald Trump isn't a saint by any means, he's at least an honest man and he cares deeply for this country. My vote goes for him!

**SATAN: IF I WIN CLINTON WINS!  
JESUS: NOT IF I CAN HELP IT!**



**PRESS 'LIKE' TO HELP JESUS WIN!**

97 Reactions 15 Comments 29 Shares

Like

Comment

Share

## US Election “Information” Attacks

- Difference between “cyber superiority” and “information superiority”
- American Intelligence Community concludes Russian origin
- Social media manipulated using poorly monitored features

May 2017



## WannaCry Ransomware Attack

- Hits 300,000 targets including National Institute of Health (NIH)
- Spread via worm using tools stolen from NSA
- Suggests weak disaster planning across most global business

July 2017

## EQUIFAX DATA BREACH AFFECTS 143 MILLION AMERICANS



- NAMES
- BIRTH DATES
- SOCIAL SECURITY NUMBERS
- ADDRESSES
- DRIVER'S LICENSE NUMBERS

### Equifax Breach Affects 143M US Citizens

- Vulnerabilities unpatched in Apache Struts in Equifax portal
- First vulnerability reported weeks before attack commenced
- Hackers created 39 undetected back doors into Equifax

# Big data breach! Aadhaar software hack poses major security concerns

software patch, which can be bought for as little as Rs 2,500 - reportedly allows unauthorised persons, based anywhere in the world, to generate Aadhaar numbers.

 BusinessToday.In

Last Updated: September 11, 2018 | 21:18 IST



## Aadhaar Exposes 1.1B Citizens of India

- Breach exposed Aadhaar number, names, emails, and physical addresses.
- Also breached phone numbers and photos.
- Break-in to India's Unique Identification Authority (records of all citizens)

Nov 2017



## Hackers Breach Personal Data for 45M Uber Riders

- Attack occurred in 2016 (GitHub account), but reported in 2017
- Hackers demanded \$100K for data and Uber paid the fee
- Cover-up causing considerable litigation on-going

June 2018

Marketing Firm Exactis Leaked a Personal Info Database With 340 Million Records

---

SHARE SHARE  
5567 TWEET COMMENT EMAIL

ANDY GREENBERG SECURITY 06.27.18 01:04 PM

# MARKETING FIRM EXACTIS LEAKED A PERSONAL INFO DATABASE WITH 340 MILLION RECORDS



---

MOST POPULARSCIENCE  
We Have No Idea How Bad the US Tick Problem Is  
MEGAN MOLTENISCIENCE  
The Air Force Is Already Betting on SpaceX's Brand-New Falcon Heavy  
AMY THOMPSONCULTURE  
How the Startup Mentality Failed Kids in San Francisco  
DANIEL QUANE[MORE STORIES](#)

## Exactis Exposes Data for 340M US Citizens

- Marketing firm had hacked data included name, address, email, etc.
- Security researcher noticed database openly accessible (via Shodan)
- Massive implications for citizen privacy

Dec 2018

# A+ FEATURES

MARRIOTT HACK MAY HAVE EXPOSED UP TO 500 MILLION CUSTOMERS

## Starwood/Marriott Exposes Data for 500M Guests

- Breach exposed names, email addresses, and physical addresses.
- Also phone numbers, passport numbers, and account info.
- Also birth dates, gender, travel info, and accommodation info.
- Second Largest Breach Ever. (After Yahoo)

Jul 2019



# DATA BREACH

## CapitalOne Breach Affects 100M Accounts

- Breach involved AWS misconfiguration
- Affected 100 million individuals in the US and 6 million in Canada
- Credit card and social security number information

Sept 2019

# Ecuador

THE ENTIRE COUNTRY LEAKED

The background features the colors of the Ecuadorian flag (yellow, blue, and red) and includes the national coat of arms at the top center.

## Ecuador Exposes 118% of Citizens Data

- Misconfigured Ecuadorian government database leaked 20.8 million user records
- Birth data, marital status, national ID, home addresses, children's info, phone and education recs.
- Official population is about 17.5 million

Apr 2020



## Hackers Sell Half Million Zoom Accounts

- The credentials of over 500K Zoom accounts were stolen by hackers
- Found for sale on the Dark Web and hacker forums for as little as two cents per account.
- Email addresses, passwords, personal meeting URLs, and host keys stolen

Jul 2020

Bill Gates   
@BILLGates



Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send \$1,000, I send you back \$2,000.

BTC Address -

<https://www.blockchain.com/btc/address/1PjLwQf2A02n82LkfbyQwH>

## Twitter Account Takeover (ATO) Breach

- Too many team members had access to account information
- Fake Tweets sent out from prominent accounts (e.g., politicians, etc.)
- Some bitcoin sent to two twenty-somethings (Florida and Canada)

Dec 2020



## SolarWinds Breach

- Nation-State (Russian) Advanced Persistent Threat (APT)
- Malicious code injection – target supply chain to users
- Massive number of victims in the US Federal Government

May 2021



## Colonial Pipeline Attack

- Ransomware attack to Northeastern US pipeline delivery
- Nation-state involvement likely – company paid ransomware
- More serious implications if attacker had been more destructive

Dec 2021

# The Log4j 2

Log4j 2 is an upgrade to Log4j that provides significant improvements over its predecessor, Log4j 1.x, and provides many of the improvements available in Logback while fixing some inherent problems in Logback's architecture.

## Important: Security Vulnerability CVE-2021-44832

Summary: Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration.

### Details

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

### Mitigation

Upgrade to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later)

## Log4J Vulnerability

- 1.8 million probes against half of corporate networks launched in December 2021
- Evidence of nation-state involvements using 70 malware families
- Actual impact is unknown so far (stay tuned)

What Can We Learn from Bank Robberies?

Week 2



Week 2





## Robby™ Panic

Hold-Up & Panic

Foot activated hold-up station Robby

## Foot activated hold-up station

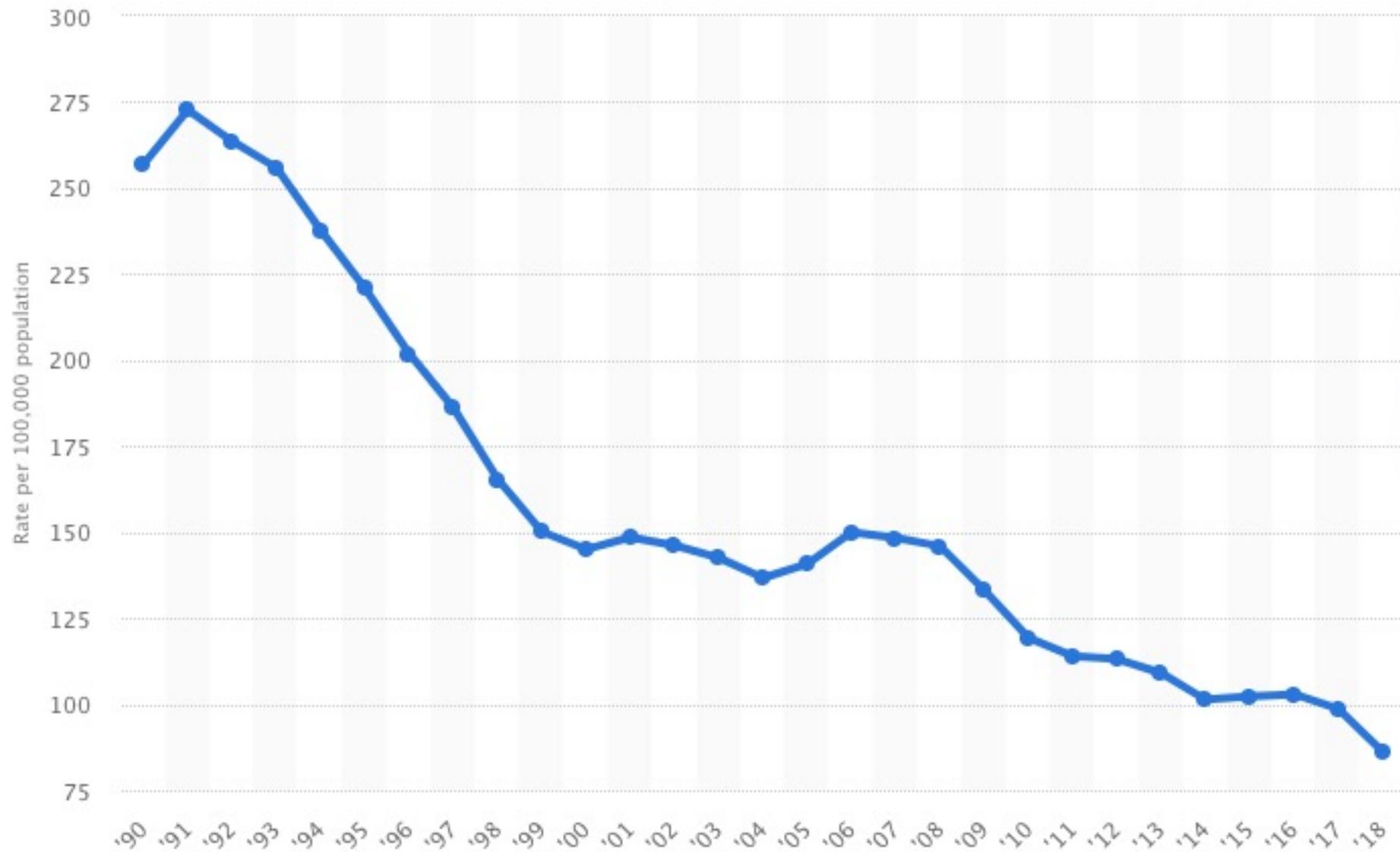
Reliable easy to operate foot activated hold-up device  
Operated by lifting the foot tip  
Foot activated robbery & panic station  
Foot activated hold-up station with rugged metal housing  
Designed to minimize the possibility of false alarms  
Foot operated panic and robbery station  
Designed for high-end security applications  
Foot activated panic station for distress Alarm System (DAS)  
Applicable for bank branches, diamonds & jewelry shops  
Foot activated hold-up station used in banks and change kiosks  
Send silent alarm to local or remote security center

SKU: Robby\_TGL, Robby\_TGO

Add to RFQ

1

# Societal Goal for Hacking: Robbery Rate in the US



What Was the First Major Internet Hack?

Week 2



# ***Worm***

Find Someone's Computer

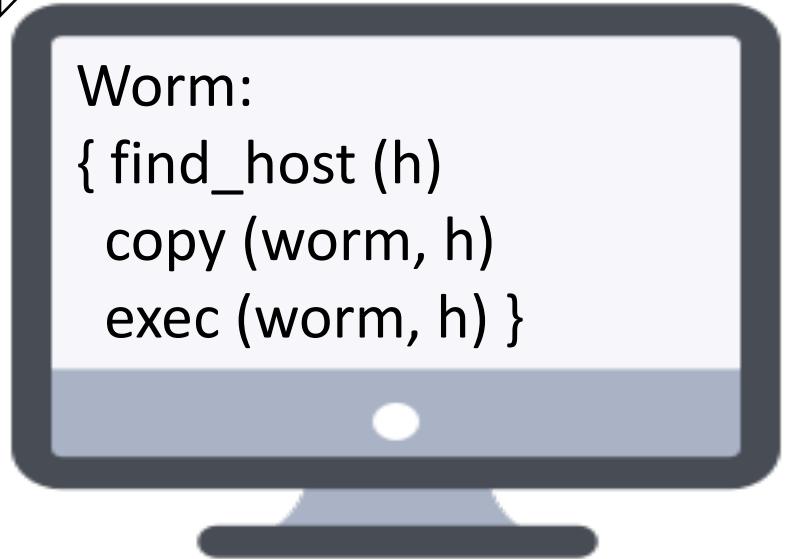
Copy ***Worm*** to Their Computer

Run ***Worm*** on Their Computer

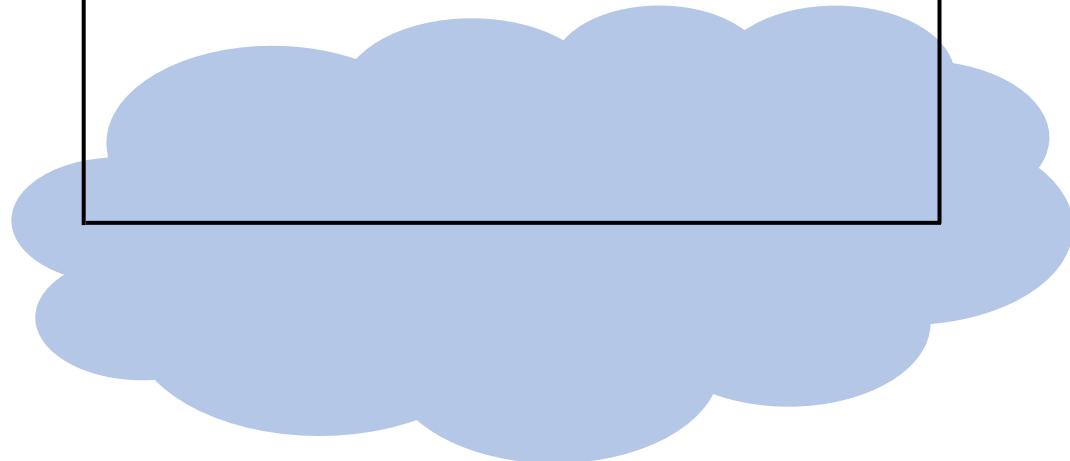
Worm:  
{ find\_host (h)  
    copy (worm, h)  
    exec (worm, h) }

Worm:

```
{ find_host (h)
  copy (worm, h)
  exec (worm, h) }
```

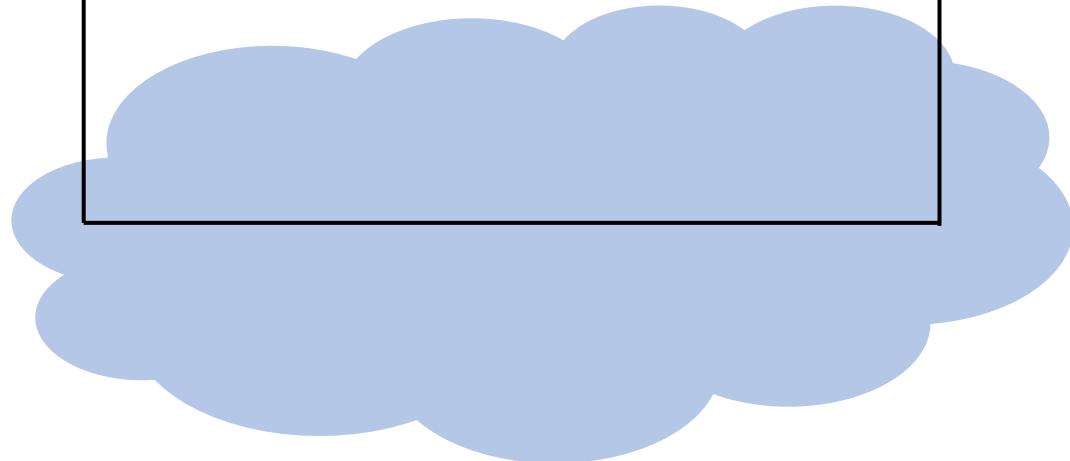


Worm:  
**{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }**



Worm:  
{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }

Worm:  
{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }



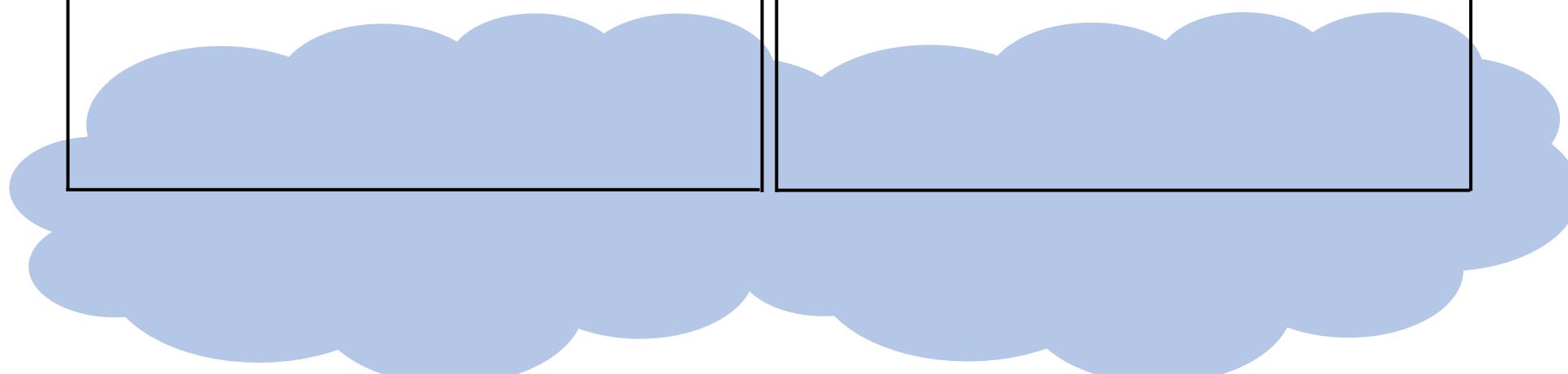
```
Worm:  
{ find_host (h)  
copy (worm, h)  
exec (worm, h) }
```

```
Worm:  
{ find_host (h)  
copy (worm, h)  
exec (worm, h) }
```

Worm:  
{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }

Worm:  
{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }

Worm:  
{ find\_host (h)  
copy (worm, h)  
exec (worm, h) }



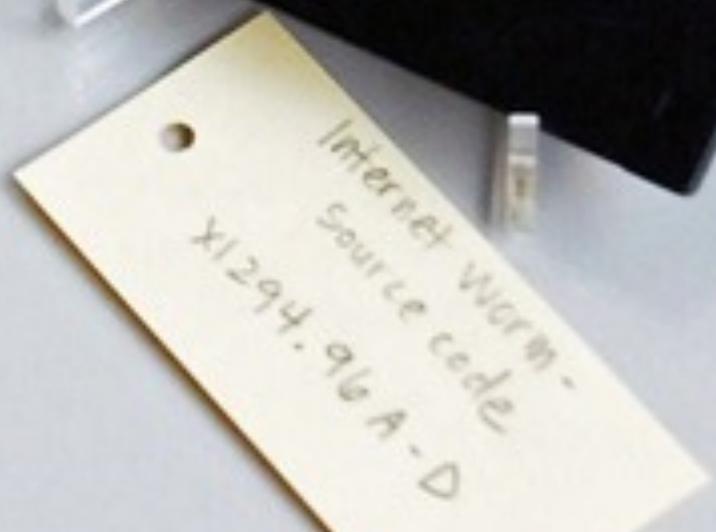
## ***The Morris Internet Worm source code***

*This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2<sup>nd</sup>, 1988.*

*The worm was the first of many intrusive programs that use the Internet to spread.*



**Computer  
History  
Museum**



# Most Common Hacking Method



Outlook team <m.r@technxsp.net>

Today, 6:43 AM

Edward Amoroso ▾



Reply all | ▾

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, [click here](#).

To always show content from this sender, [click here](#).

Hello EAmoroso,

You have some malicious files in a hidden folder such files are against our Term of service(T.O.S)

In order for us not to terminate your e mail service these files must be deleted automatically  
Kindly remove all hidden files automatically below.

**REMOVE HIDDEN FILES**

Thanks for taking these additional steps to safe guard your e mail.

# How is Code Maliciously Inserted?

Here is a small piece of code that implements a “login” process for an app:

## Login

```
Print "Enter your name: "
Get (Name)
Print "Enter your password: "
Get (Password)
if OK (Name, Password) then Permit
else Deny
```

End

# Making Malicious Insertions Invisible

Here is a small piece of code that implements a “login” process for an app:

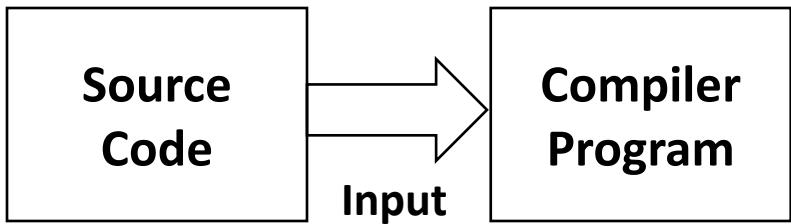
**Login**

**Print** “Enter your name: ”  
**Get** (Name)  
**Print** “Enter your password: ”  
**Get** (Password)  
**if** OK (Name, Password) **then** Permit  
    **else** Deny

**End**

Programmers refer to this as  
**“Source Code”** and use  
Programming Languages  
such as Java, C++, and Python

Here is the translation process to make the code executable on a computer:



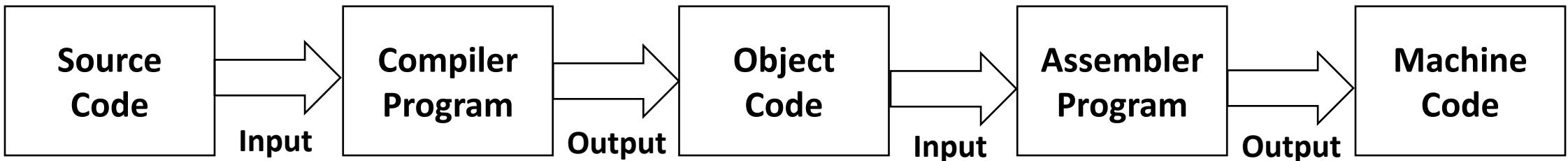
Programmers obtain “**Compilers**” from software companies such as Microsoft (or get them for free on the Internet)

Here is the translation process to make the code executable on a computer:



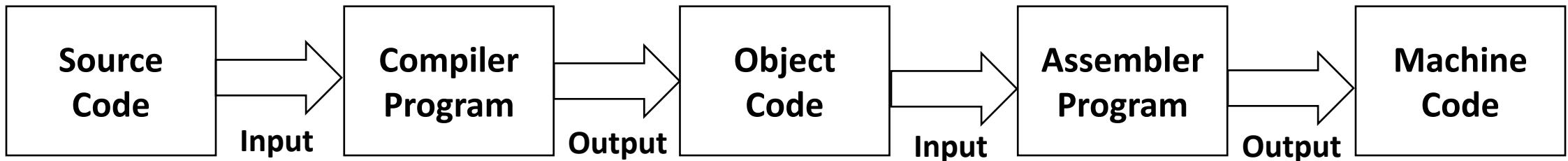
Compilers “break down” Source Code into more rudimentary building block languages called “**Object Code**” for the computer being used

Here is the translation process to make the code executable on a computer:



Assemblers “break down” Object Code into raw binary languages (1’s and 0’s) called **“Machine Code”** for the computer being used

Here is the translation process to make the code executable on a computer:



Login

```

Print "Enter your name:"
Get (Name)
Print "Enter your password:"
Get (Password)
if OK (Name, Password) then Permit
else Deny
  
```

End

-- Login

```

LDA 8A34
STA FF20
LDA 2001
STA FF21
MOV 2A2B
  
```

. . .

-- Login

0010	1010
1100	1011
0000	1101
0001	1111
1110	1111

. . .

Here is the process to insert a Trojan horse into the code executable on a computer:

## **Login**

**Print** “Enter your name: ”

**Get** (Name)

**Print** “Enter your password: ”

**Get** (Password)

**if** OK (Name, Password) **then** Permit

**else** Deny

**End**

Here is the process to insert a Trojan horse into the code executable on a computer:

## **Login**

**Print** “Enter your name: ”

**Get** (Name)

**Print** “Enter your password: ”

**Get** (Password)

**if** OK (Name, Password) **or** Password = “STEVENS” **then** Permit

**else** Deny

**End**

Here is the process to insert a Trojan horse into the code executable on a computer:

### Login

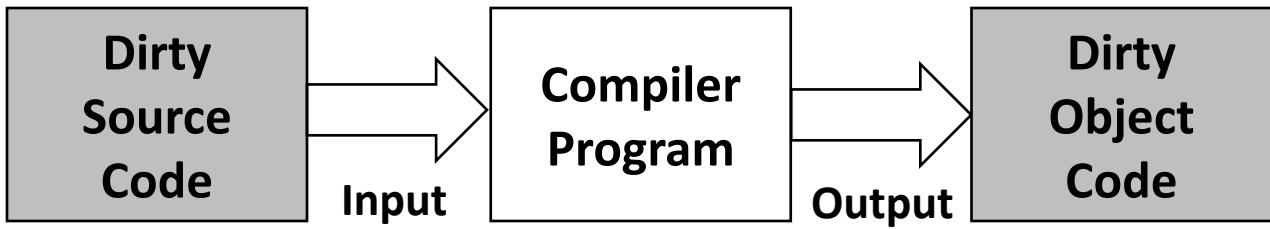
```
Print "Enter your name: "
Get (Name)
Print "Enter your password: "
Get (Password)
if OK (Name, Password) or Password = "STEVENS" then Permit
else Deny
```

This is a Trojan Horse  
Insertion called a  
“Back Door”

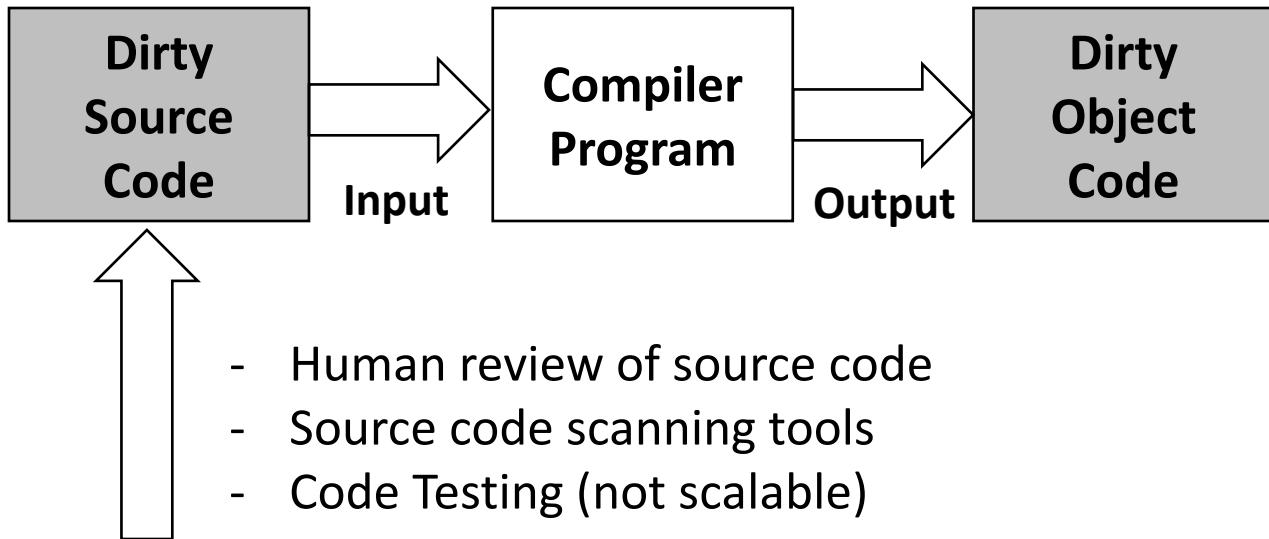


End

Here is the process to translate “Dirty Source Code” into “Dirty Object Code:”



Here is the review process to detect “Dirty Source Code” being used to create into “Dirty Object Code:”



Here is how a “Clean” compiler program works:

**Compiler**

**Repeat**

**Get** (Line of Code)

**Translate** (Line of Code)

**Until Done**

**End**

Here is how a “Clean” compiler program works:

**Compiler**

**Repeat**

**Get** (Line of Code)

**Translate** (Line of Code)

**Until Done**

**End**

Here is how a “Dirty” compiler program works:

**Compiler**

**Repeat**

**Get** (Line of Code)

**If** (Line of Code) = “**If OK (Name, Password)**”

**Translate** (Line of Code)

**Until Done**

**End**

Here is how a “Dirty” compiler program works:

**Compiler**

**Repeat**

**Get** (Line of Code)

**If** (Line of Code) = “**If OK (Name, Password)**”

**Then Translate** (“**If OK (Name, Password) or Password = “STEVENS”**”)

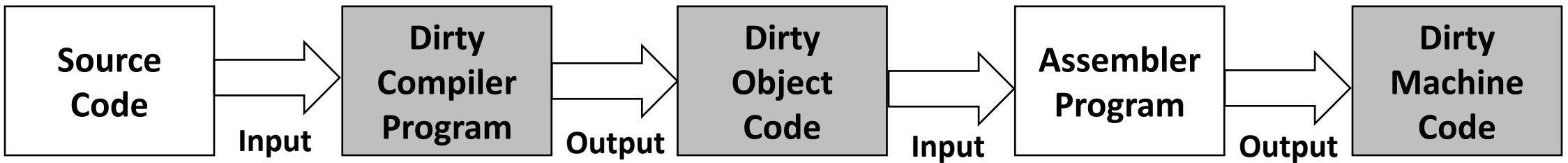
**Else**

**Translate** (Line of Code)

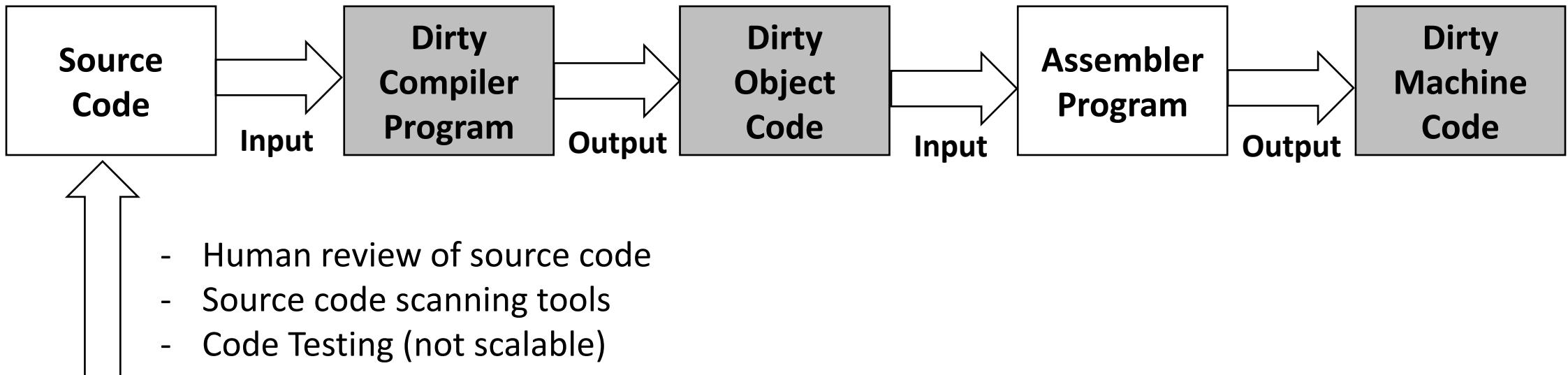
**Until Done**

**End**

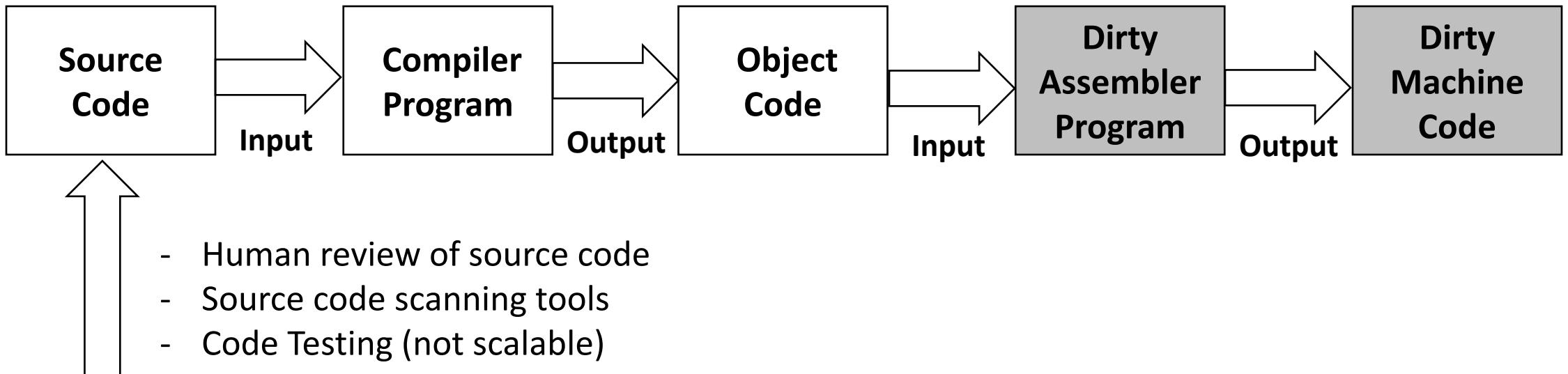
Here is how a “Dirty” compiler program translates  
Clean Source to Dirty Object Code:



Here is how a “Dirty” compiler program hides Trojan Horse insertions in Object Code:



Here is how a Malicious Group “Hides” Trojan horses deeper into the translation process:

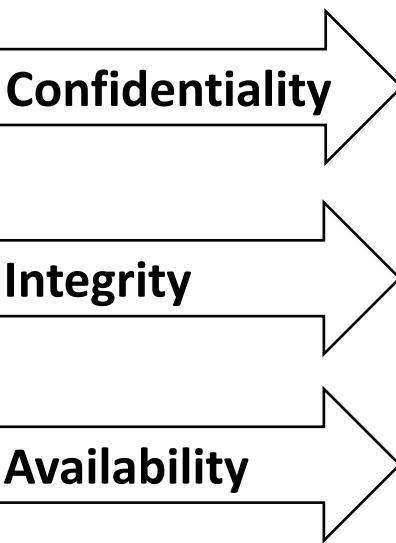


# How Do You Mitigate Software Trojans?



*Dirty Equipment in  
CONUS or OCONUS  
Locations*

*CIA Model*



*Network Transport of  
Command and Control (C&C),  
or Telemetry*

1. Trojan Horse Designed to quietly “eavesdrop” on US Communications
2. Trojan Horse Designed to quietly “modify” US Operations
3. Trojan Horse Designed to noisily “block” US Operations

*Foreign C&C  
Located in  
CONUS or OCONUS*

**Three US National Security Risk Areas of Trojan Horse Insertions**

## 1. Review Vendor Software Development Process

- **Read documentation, review checklist answers, interview vendor team**

**Normal Risk Mitigation for Vendor-Inserted Trojan Horses**

- 1. Review Vendor Software Development Process**
  - **Read documentation, review checklist answers, interview vendor team**
- 2. Inspect Vendor Hardware and Software**
  - **Review source code, use static tools to scan software, read documentation**

**Normal Risk Mitigation for Vendor-Inserted Trojan Horses**

- 1. Review Vendor Software Development Process**
  - **Read documentation, review checklist answers, interview vendor team**
- 2. Inspect Vendor Hardware and Software**
  - **Review source code, use static tools to scan software, read documentation**
- 3. Specify Vendor Integrity Requirements in Contract**
  - **Include language in vendor contracts, specify consequences of Trojan detection**

**Normal Risk Mitigation for Vendor-Inserted Trojan Horses**

- 1. Review Vendor Software Development Process**
  - **Read documentation, review checklist answers, interview vendor team**
- 2. Inspect Vendor Hardware and Software**
  - **Review source code, use static tools to scan software, read documentation**
- 3. Specify Vendor Integrity Requirements in Contract**
  - **Include language in vendor contracts, specify consequences of Trojan detection**
- 4. Monitor Community for Evidence of Vendor Issues**
  - **Digital Risk Management of vendor, review hacker community chatter**

**Normal Risk Mitigation for Vendor-Inserted Trojan Horses**

- 1. Review Vendor Software Development Process**
  - **Read documentation, review checklist answers, interview vendor team**
- 2. Inspect Vendor Hardware and Software**
  - **Review source code, use static tools to scan software, read documentation**
- 3. Specify Vendor Integrity Requirements in Contract**
  - **Include language in vendor contracts, specify consequences of Trojan detection**
- 4. Monitor Community for Evidence of Vendor Issues**
  - **Digital Risk Management of vendor, review hacker community chatter**
- 5. Proxy Outbound Communications to Unknown Sources**
  - **Gateway interrupts all outbound communications, check target URL**

**Normal Risk Mitigation for Vendor-Inserted Trojan Horses**

1. Use Social Engineered Deception to Expose Trojan Back Door Access
  - Ex/ Call vendor in distress, begging for assisted access to procured system

**Advanced Risk Mitigation for Nation-State Controlled Trojan Horses**

- 1. Use Social Engineered Deception to Expose Trojan Back Door Access**
  - **Ex/ Call vendor in distress, begging for assisted access to procured system**
- 2. Comparatively Analyze Multiple Instances of Vendor Product**
  - **Ex/ Purchase same product in different contexts (incl. critical and non-critical)**

**Advanced Risk Mitigation for Nation-State Controlled Trojan Horses**

1. Use Social Engineered Deception to Expose Trojan Back Door Access
  - Ex/ Call vendor in distress, begging for assisted access to procured system
2. Comparatively Analyze Multiple Instances of Vendor Product
  - Ex/ Purchase same product in different contexts (incl. critical and non-critical)
3. Learn from Present or Former Employees About Trojan Insertions
  - Ex/ Former Microsoft employees admit to Trojans in Word and Excel

**Advanced Risk Mitigation for Nation-State Controlled Trojan Horses**

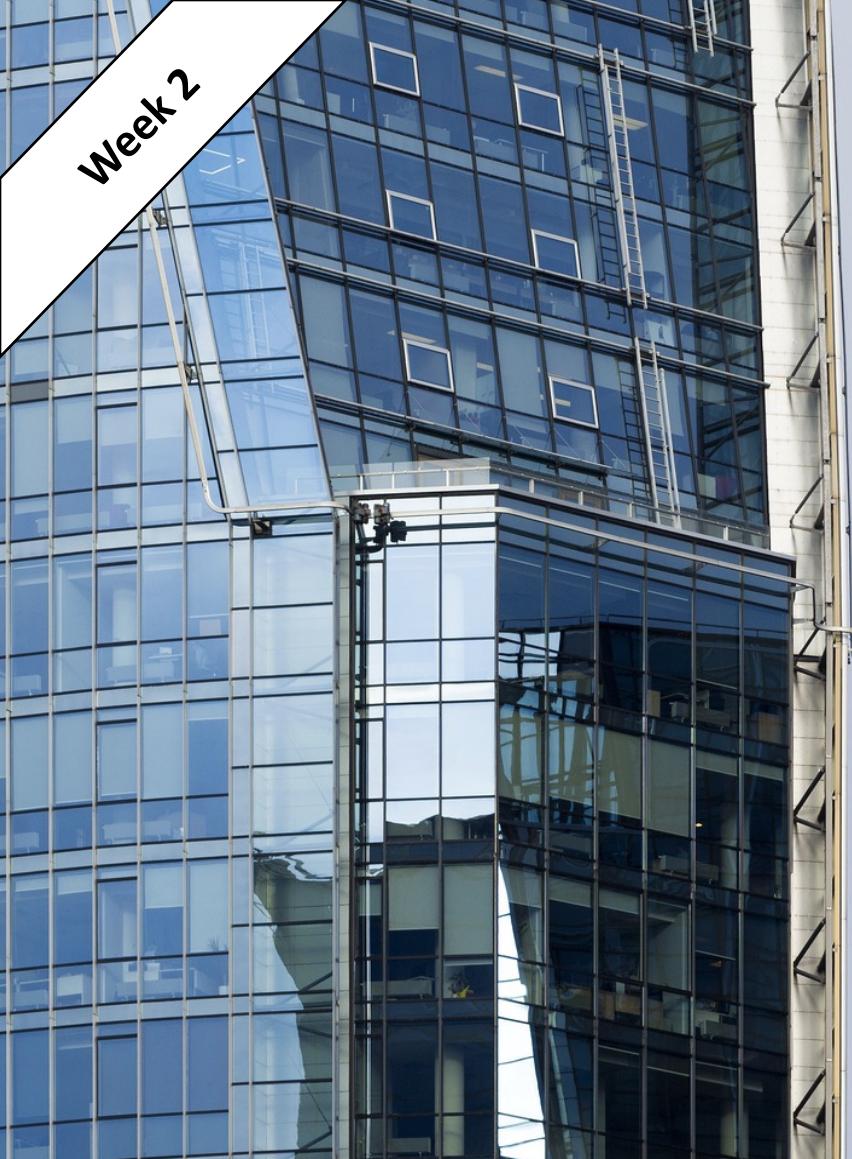
1. Use Social Engineered Deception to Expose Trojan Back Door Access
  - Ex/ Call vendor in distress, begging for assisted access to procured system
2. Comparatively Analyze Multiple Instances of Vendor Product
  - Ex/ Purchase same product in different contexts (incl. critical and non-critical)
3. Learn from Present or Former Employees About Trojan Insertions
  - Ex/ Former Microsoft employees admit to Trojans in Word and Excel
4. Governments Can Utilize Surveillance and Signals Intelligence
  - Ex/ Lawful intercepts can provide evidence of integrity issues

**Advanced Risk Mitigation for Nation-State Controlled Trojan Horses**

1. Use Social Engineered Deception to Expose Trojan Back Door Access
  - Ex/ Call vendor in distress, begging for assisted access to procured system
2. Comparatively Analyze Multiple Instances of Vendor Product
  - Ex/ Purchase same product in different contexts (incl. critical and non-critical)
3. Learn from Present or Former Employees About Trojan Insertions
  - Ex/ Former Microsoft employees admit to Trojans in Word and Excel
4. Governments Can Utilize Surveillance and Signals Intelligence
  - Ex/ Lawful intercepts can provide evidence of integrity issues
5. Governments Can Embed Developers Into Target Vendor Environments
  - Ex/ Confidential relationship with developers employed by vendor

Advanced Risk Mitigation for Nation-State Controlled Trojan Horses

Week 2



## US National Policy Regarding Chinese Telecommunications Firms

Week 2



Major (non-Chinese) Telecommunications Breach (No Trojans)