Week 2

An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 2

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

Week 2

Required Week Two Readings

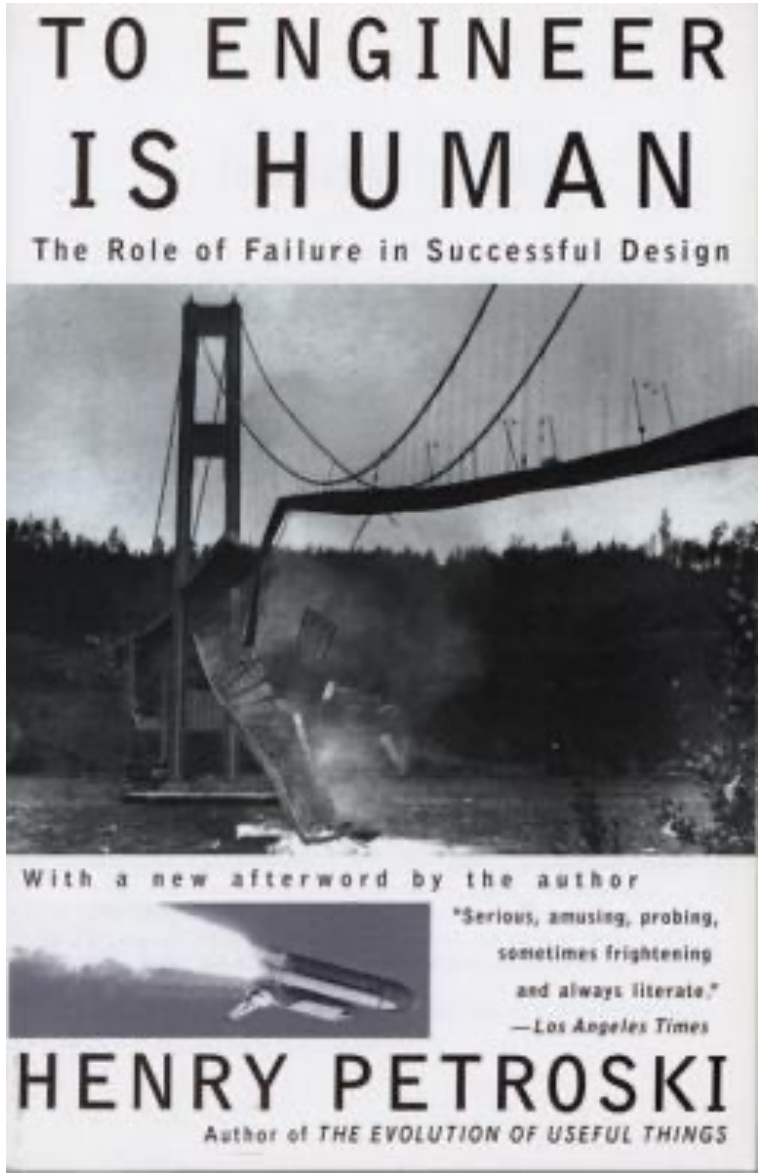
1. "Smashing the Stack for Fun and Profit," AlephOne
https://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf
2. Chapters 5 through 8: *From CIA to APT: An Introduction to Cyber Security*, E. Amoroso & M. Amoroso

Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso
eamoroso@tag-cyber.com

Use this email, and not my stevens.edu email please!

Week 2: Incidents, Trojans, Worms, and Attacks

Week 2


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

Week 2

Oklahoma City Bombing

On the morning of April 19, 1995, an ex-Army soldier and security guard named Timothy McVeigh parked a rented Ryder truck in front of the Alfred P. Murrah Federal Building in downtown Oklahoma City.

What Can We Learn from Major Incidents?

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)

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.

Five Month Undetected Attack at Home Depot

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

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

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

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*

11 Million Premera Customer Insurance Records

- Thirty-eight class action lawsuits 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)

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

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

...etter 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

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

Hackers Shut Power to 80,000 Ukrainian Citizens

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

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

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

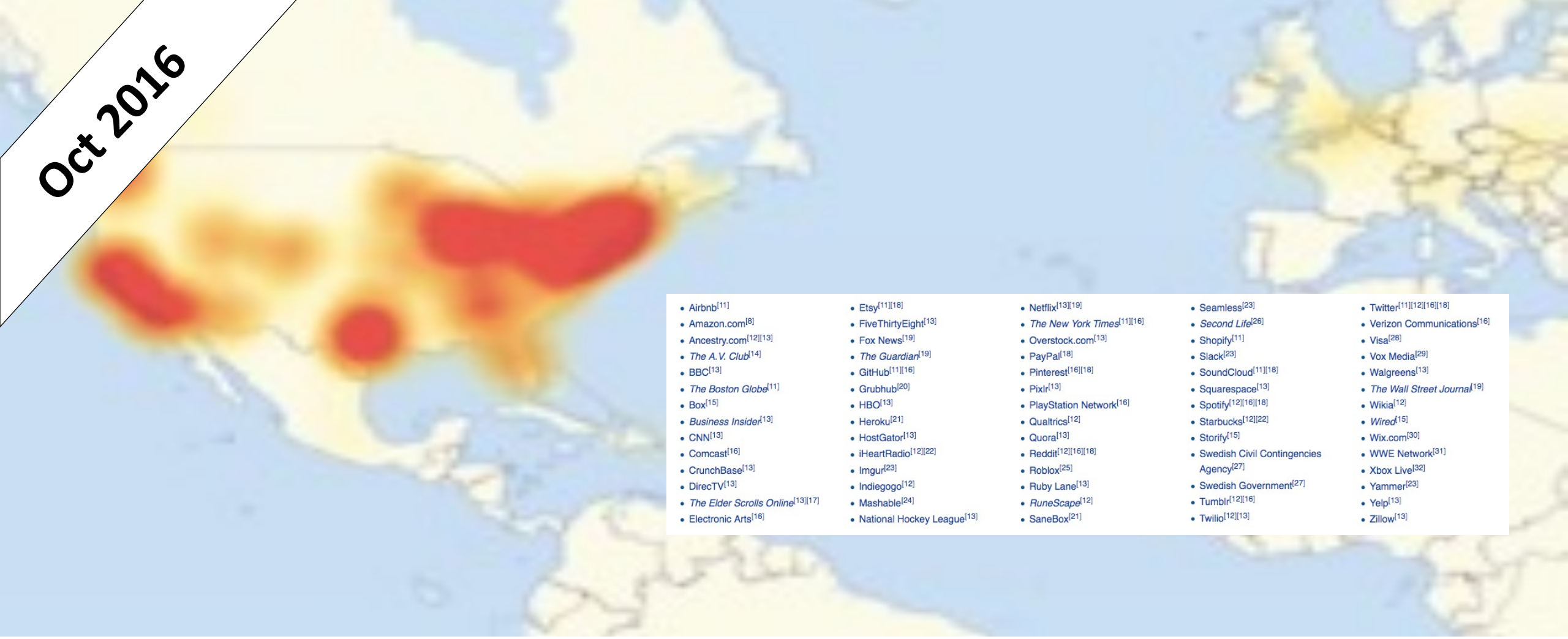
1,025 Wendy's Stores Hit by Credit Card Breach

- 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



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

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

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

Aug 2017

Bi…ata breach! Aadhaar software hack …ses 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

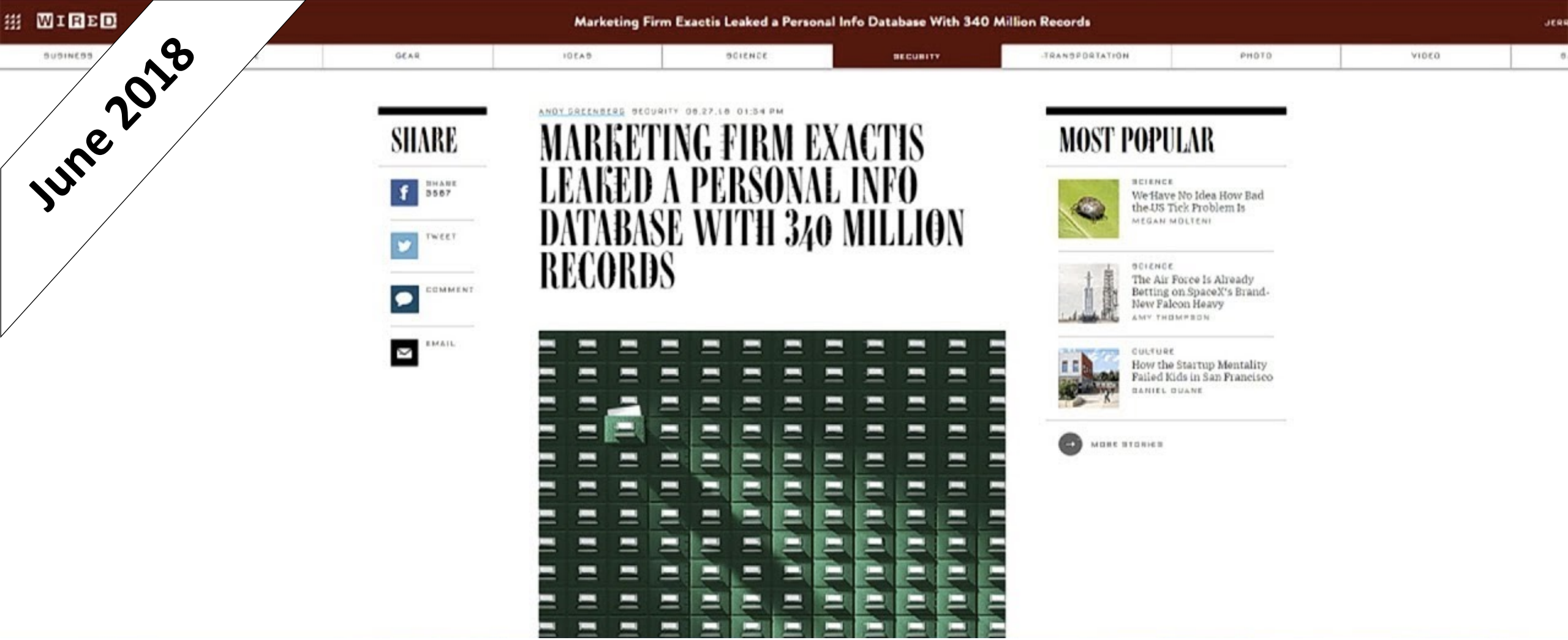
Aadhaar Exposes 1.1B Citizens of India

- 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)

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



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

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)

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

Ecuador Exposes 118% of Citizens Data

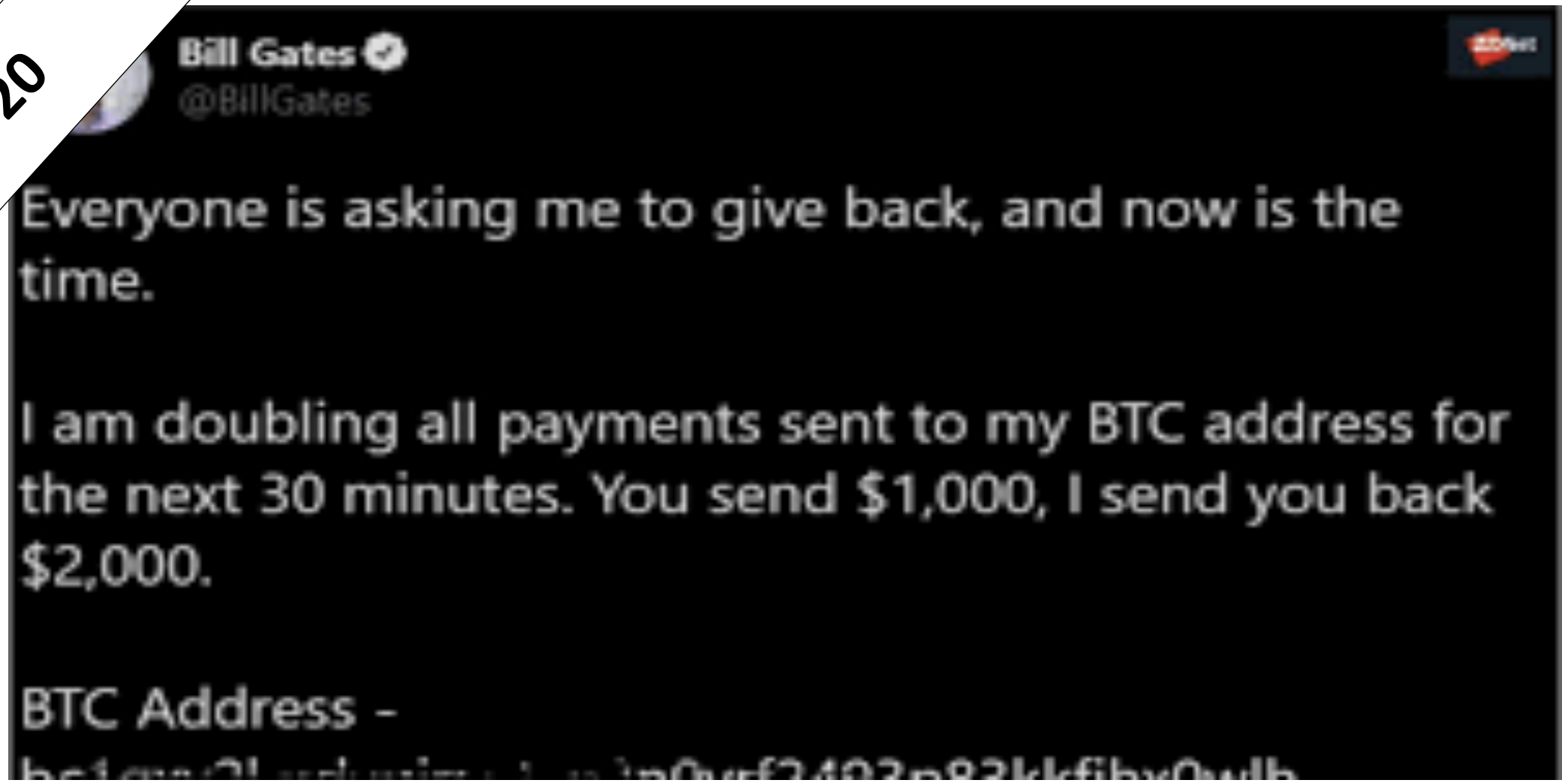
- Misconfigured Ecuadorian government database leaked 20.8 million user records
- Birth data, marital status, national ID, home addresses, children's info, phone and education recs.
- Official population is about 17.5 million

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



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)

Jul 2020

Edward Amoroso posted this

Why I Don't Support Mudge's Decision.

Edward Amoroso on LinkedIn

August 24, 2022

You and 441 others 288 comments

118,652 impressions View analytics

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

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

Apache Log4j 2

Apache 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)

Lapsus$ Rampage

- Teenager in the UK rampages Microsoft, Nvidia, and other major targets
- High-profile compromise of internal Microsoft DevOps account
- Ransomware demands (e.g., Nvidia make code open-source, etc.)

Uber Breach

- Social engineering attack (fake IT call) to an Uber employee for password
- Teenager hacker gained access to entire Uber infrastructure from this access
- Follows 2016 attack (57 million accounts compromised)

What Can We Learn from Bank Robberies?

Week 2

Week 2

Week 2

Hold-Up & Panic

Foot activated hold-up station Robby

Foot activated hold-up station

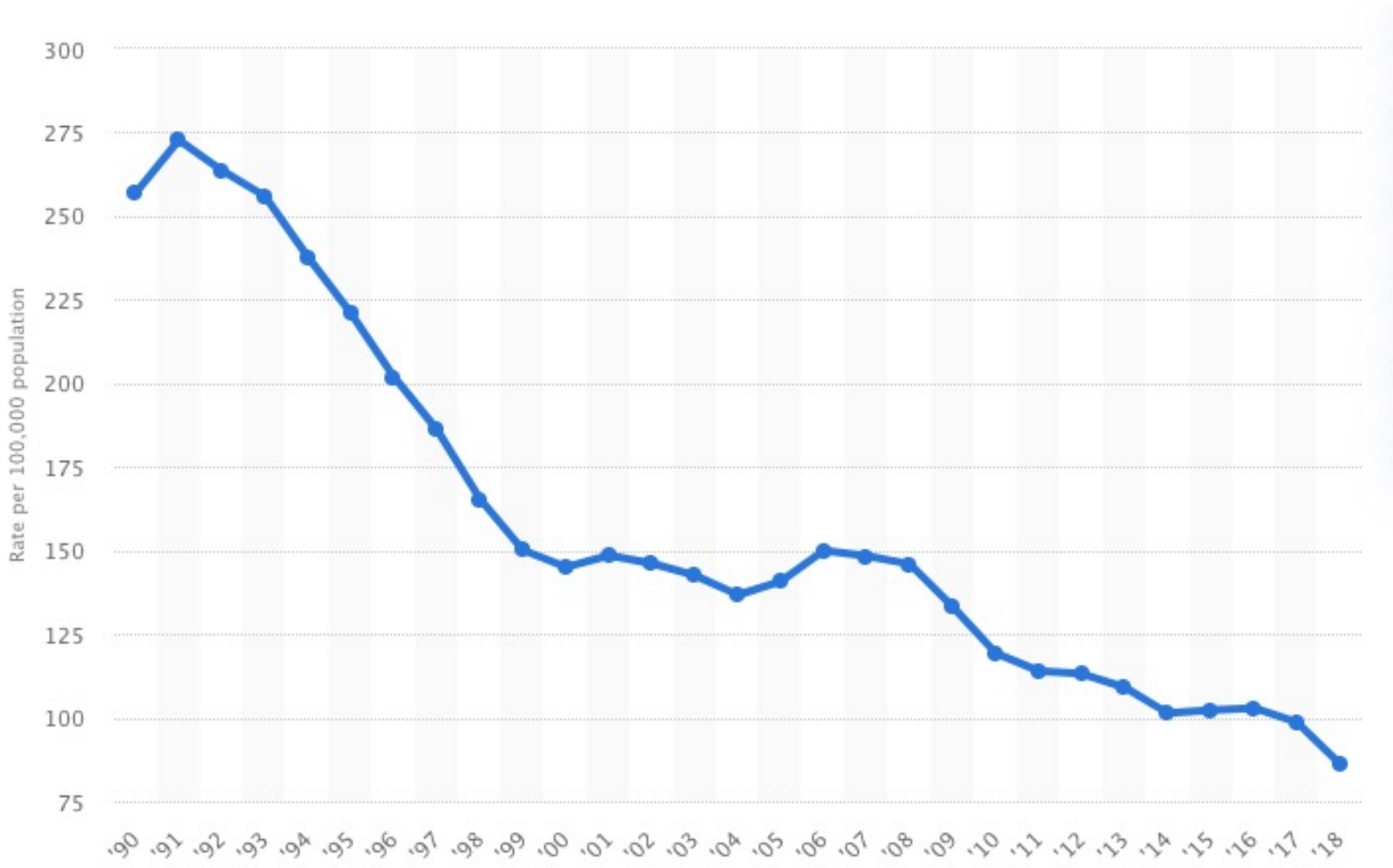
Reliable easy to operate foot activated hold-up device
Operated by lifting the foot tip
Foot activated robbery & panic station
Foot activated hod-up station with rugged metal housing
Designed to minimize the possibility of false alarms
Foot operated panic and robbery station
Designed for high-end security 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

Week 2

Societal Goal for Hacking: Robbery Rate in the US



Week 2

Long-Term Goal for Cybersecurity

To reduce the risk of cyber threats to the point where they no longer represent a significant and present danger to society (like bank robberies).

What Was the First Major Internet Hack?

Week 2

Week 2

Worm

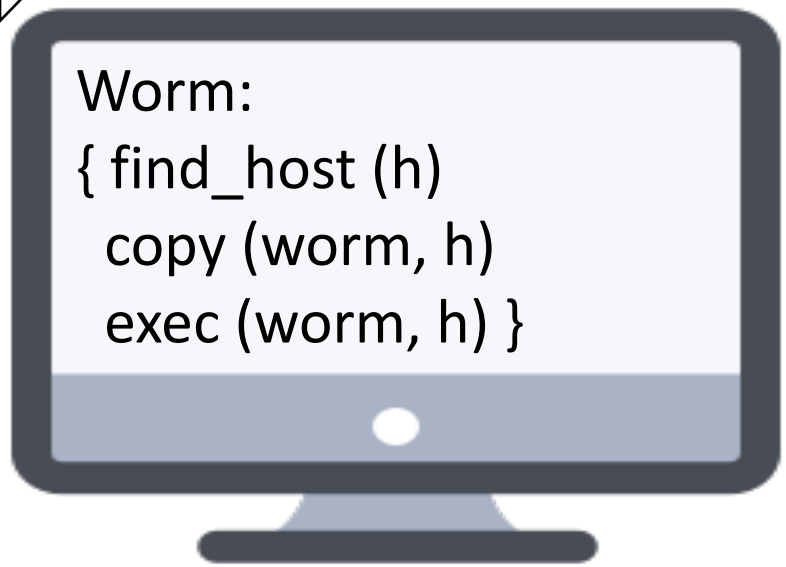
Find Someone's Computer

Copy ***Worm*** to Their Computer

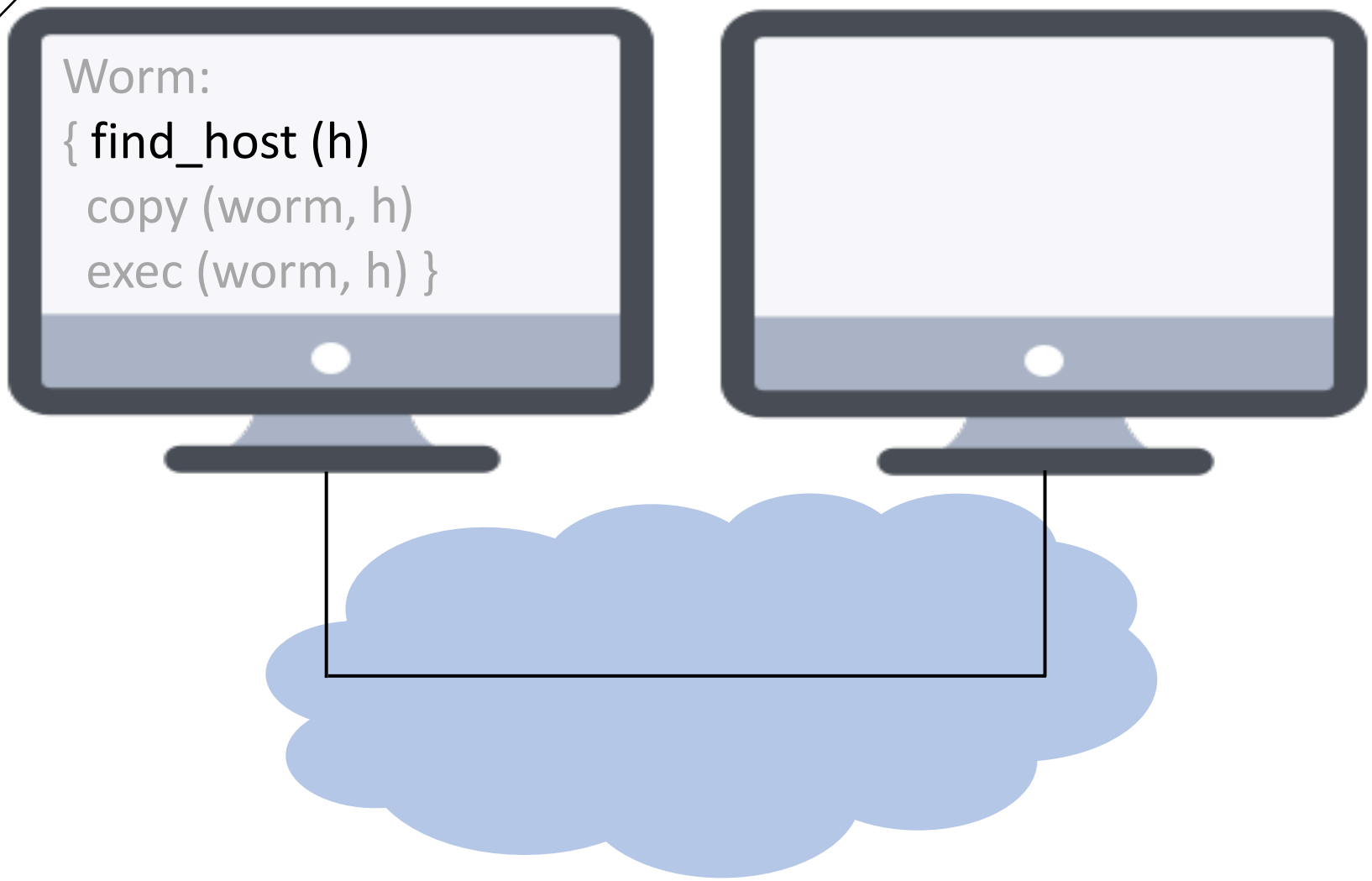
Run ***Worm*** on Their Computer

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

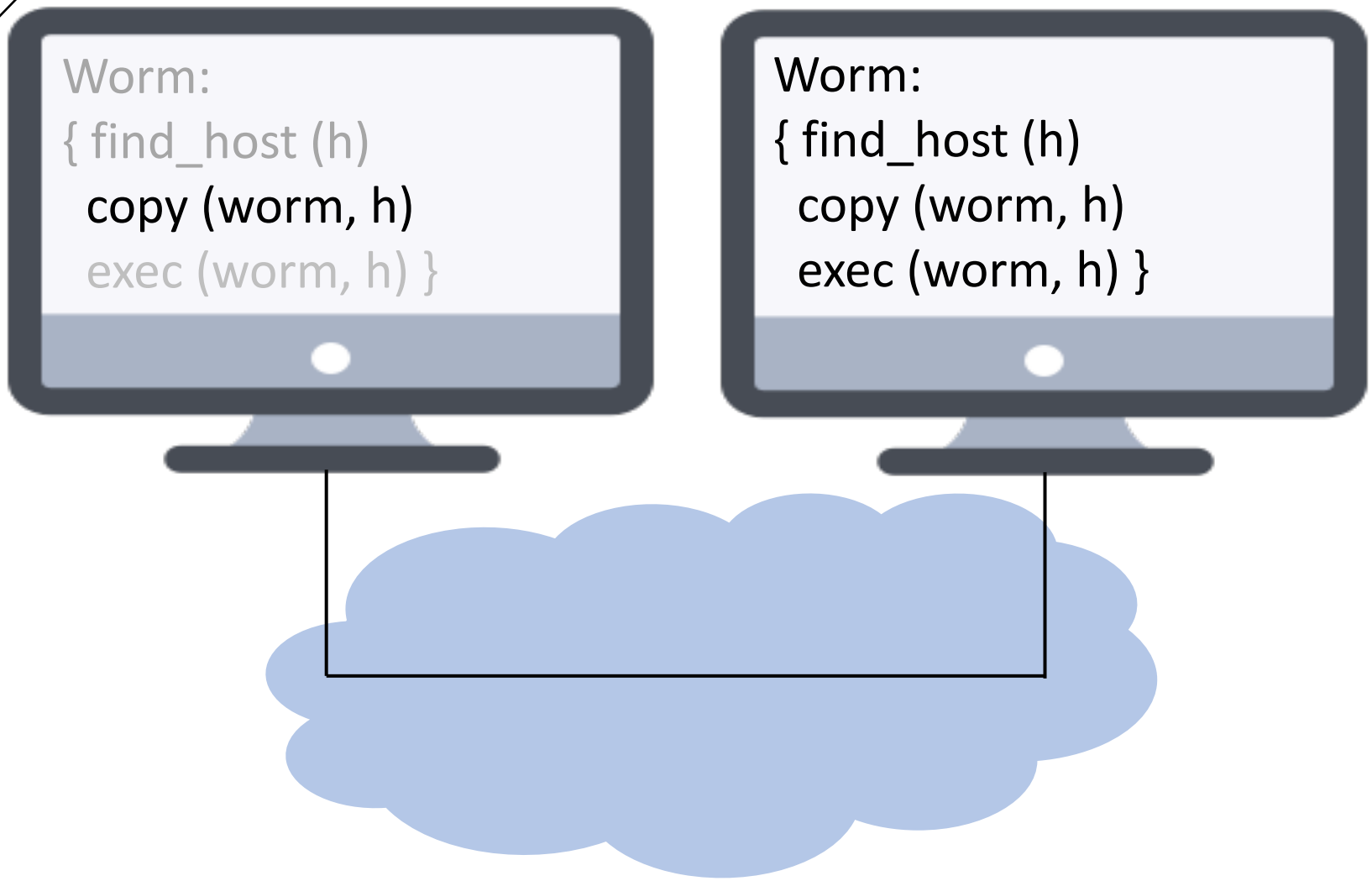
Week 2



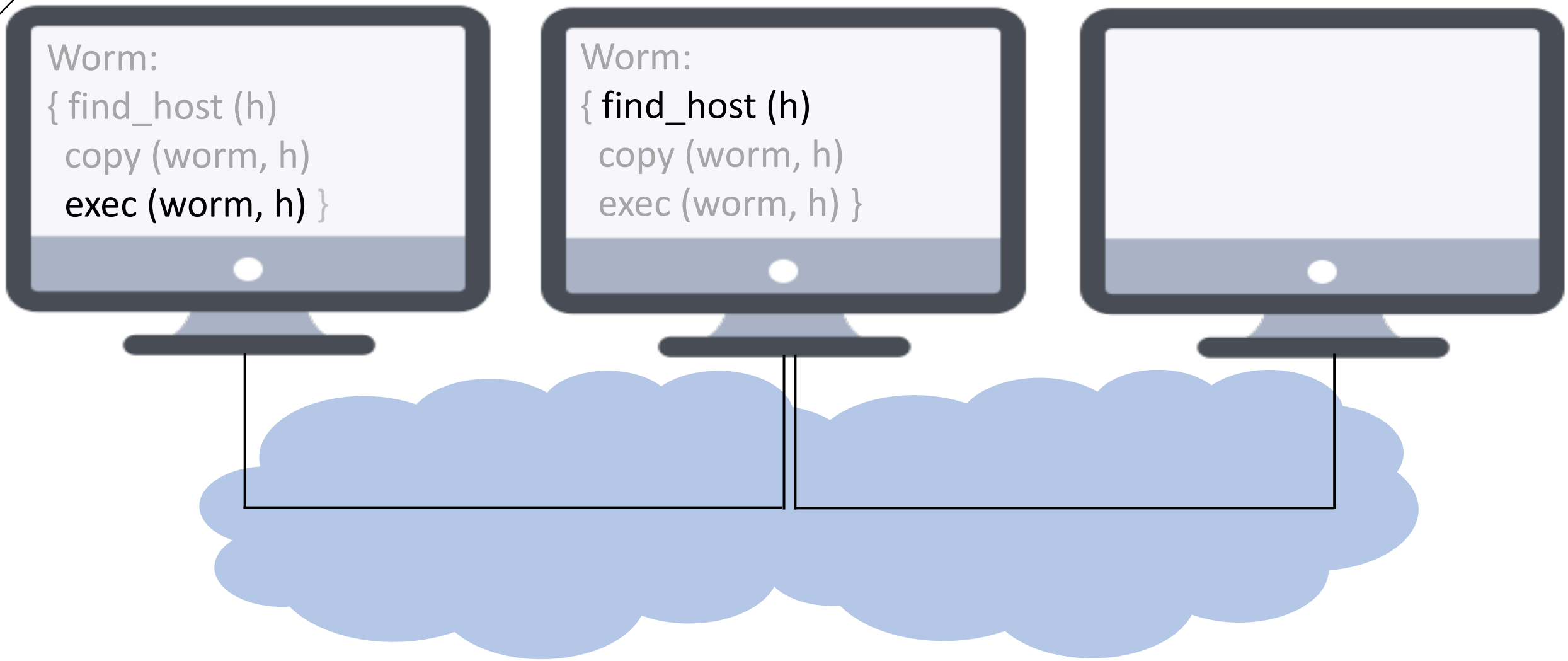
Week 2



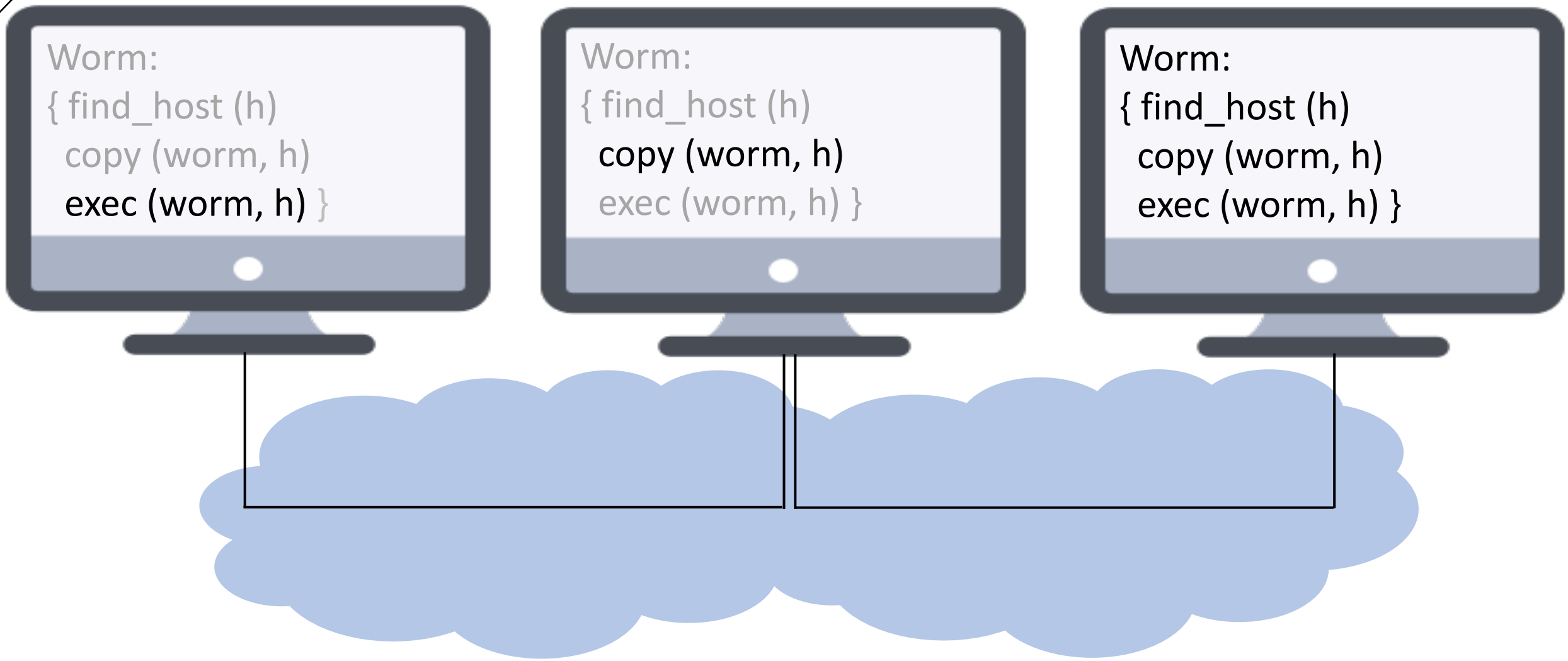
Week 2


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

Week 2


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

Week 2


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) }

Week 2

The Morris Internet Worm source code

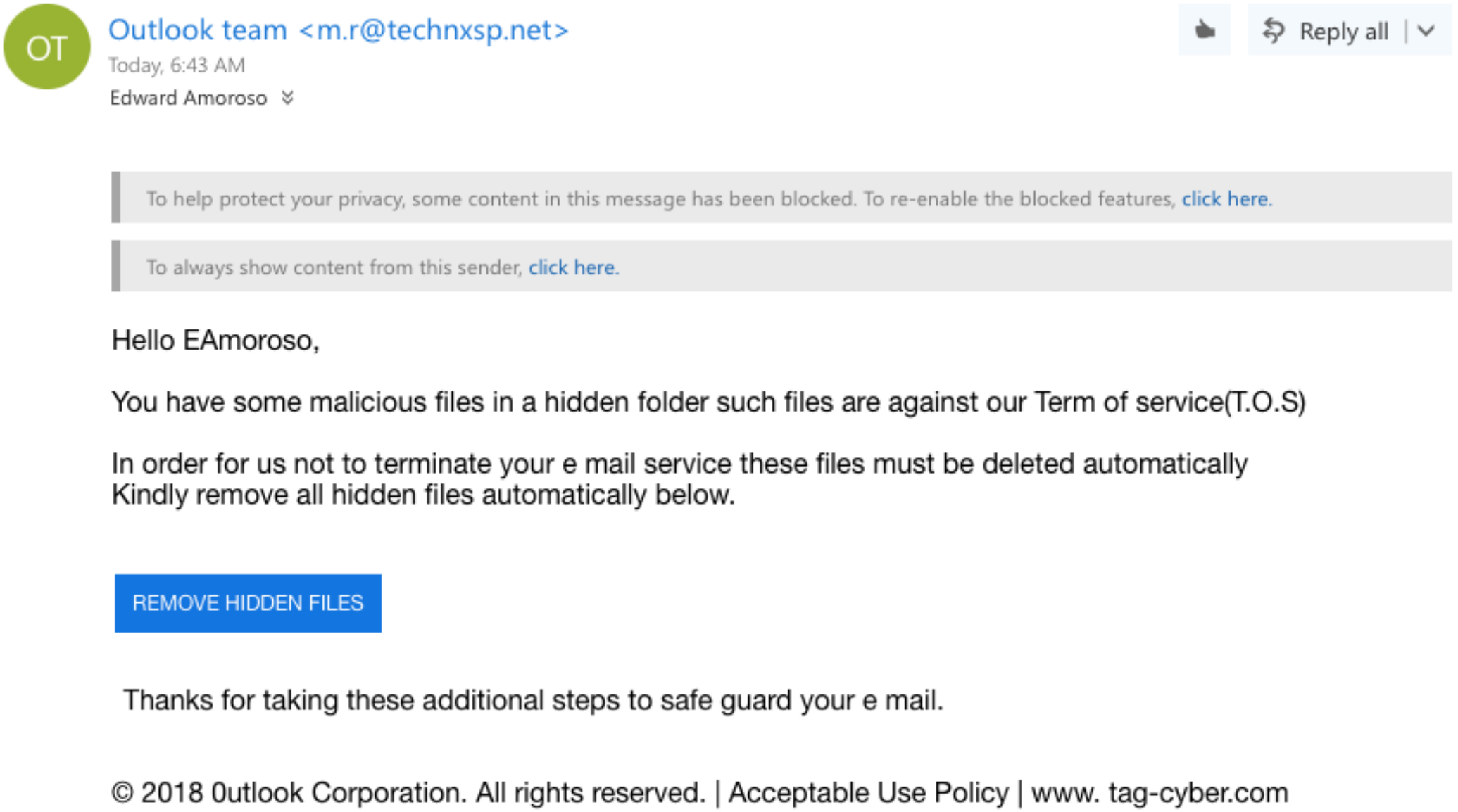
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

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

Computer History Museum

Week 2

Most Common Hacking Method



OT

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.

© 2018 0utlook Corporation. All rights reserved. | Acceptable Use Policy | www. tag-cyber.com

How is Code Maliciously Inserted?

Week 2

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

Week 2

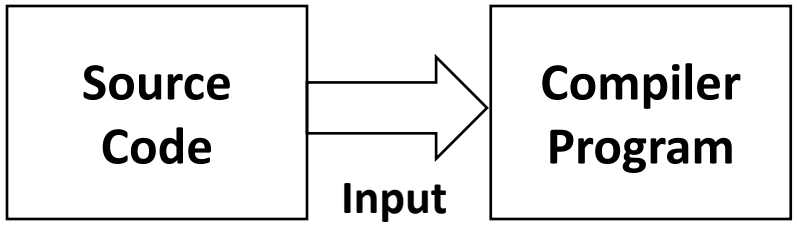
Here is a small piece of code that implements a “login” process for an app:

```
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

Week 2

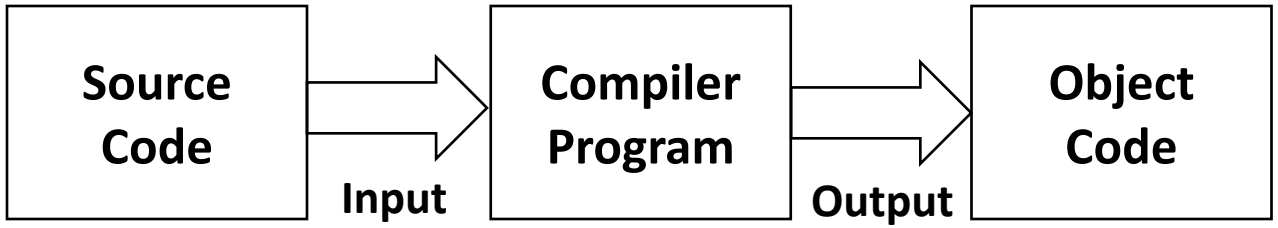
Here is the translation process to make the code executable on a computer:



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

Week 2

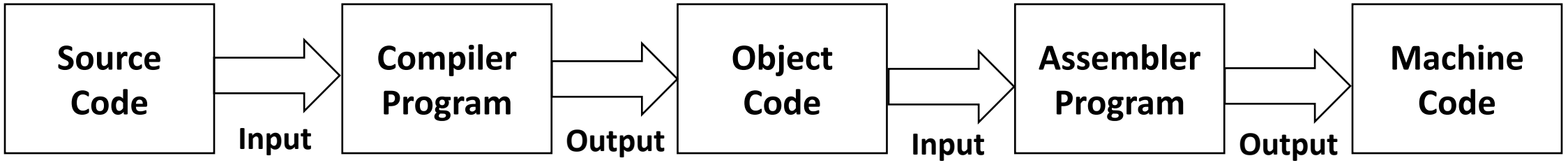
Here is the translation process to make the code executable on a computer:



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

Week 2

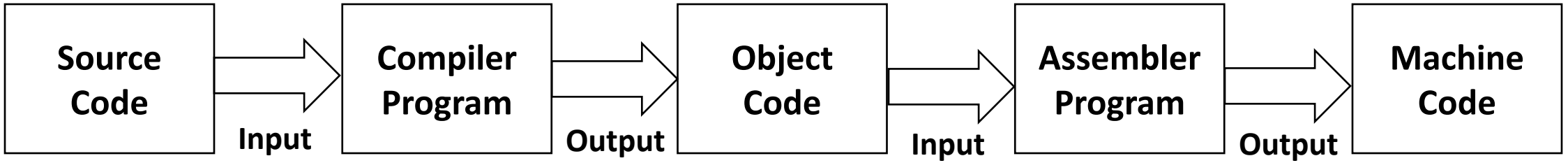
Here is the translation process to make the code executable on a computer:



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

Week 2

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

Week 2

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

Login

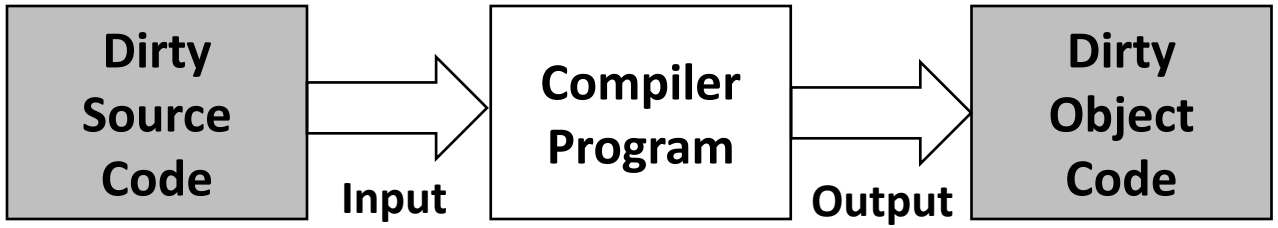
Print “Enter your name: ”
Get (Name)
Print “Enter your password: ”
Get (Password)
if OK (Name, Password) **or** Password = “STEVENS” **then** Permit
  else Deny

End

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

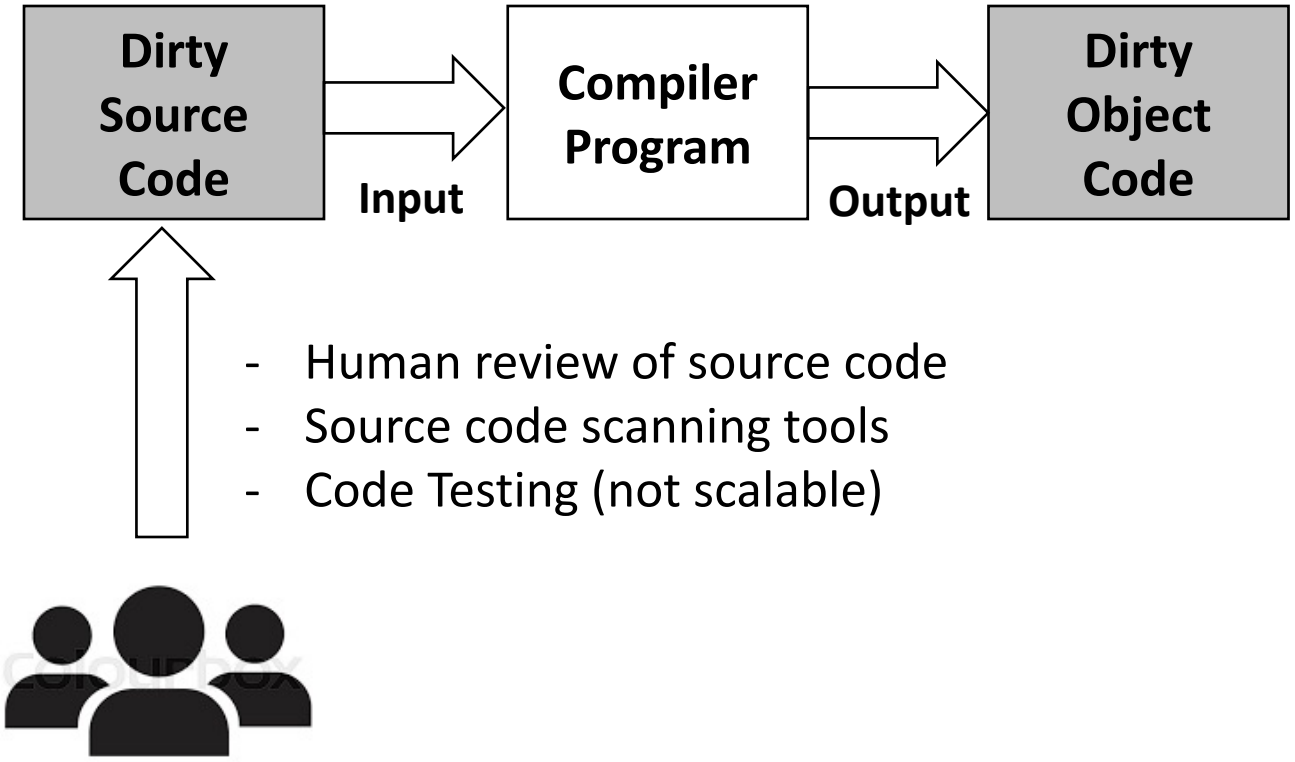
Week 2

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



Week 2

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

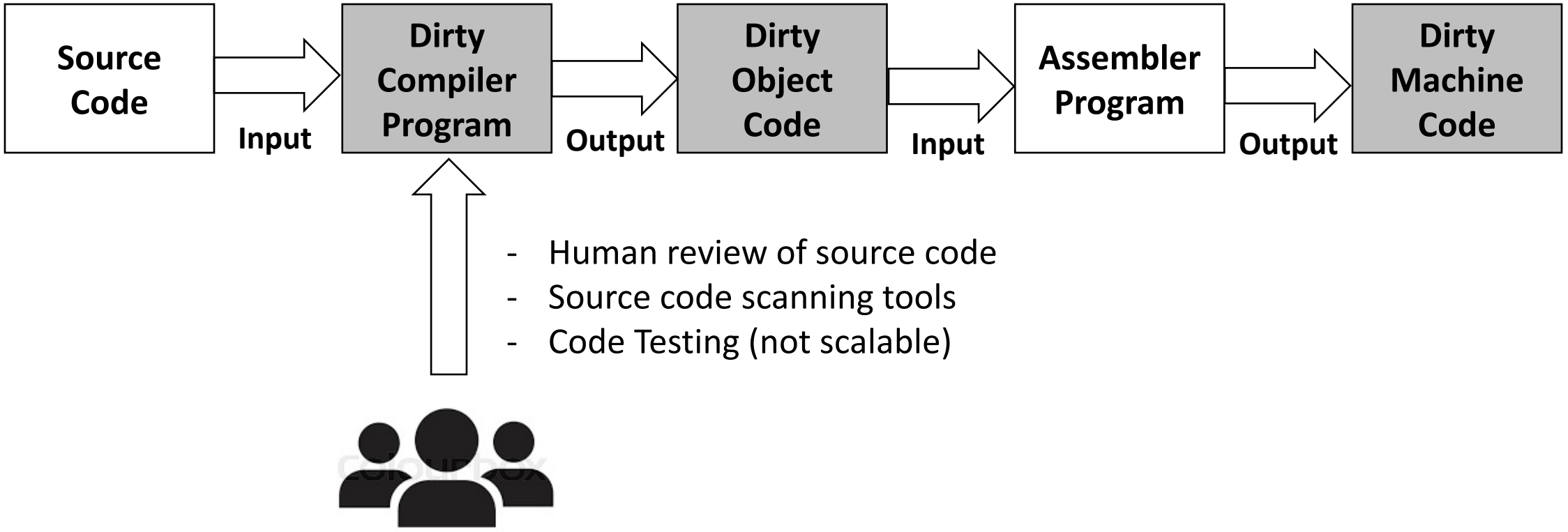
End

Week 2

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

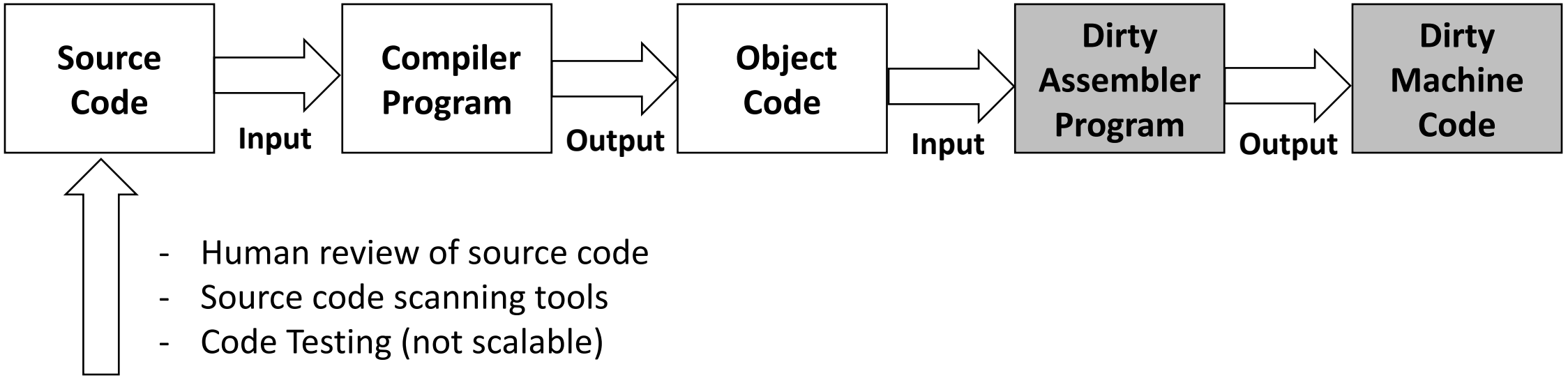
Week 2

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



Week 2

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



How Do You Mitigate Software Trojans?

Week 2

Dirty Equipment in CONUS or OCONUS Locations

CIA Model

Confidentiality

Integrity

Availability

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

Week 2

1. **Review Vendor Software Development Process**
   - **Read documentation, review checklist answers, interview vendor team**

Normal Risk Mitigation for Vendor-Inserted Trojan Horses

Week 2

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

Week 2

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

Week 2

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

Week 2

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

Week 2

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

Week 2

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

Week 2

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

Week 2

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

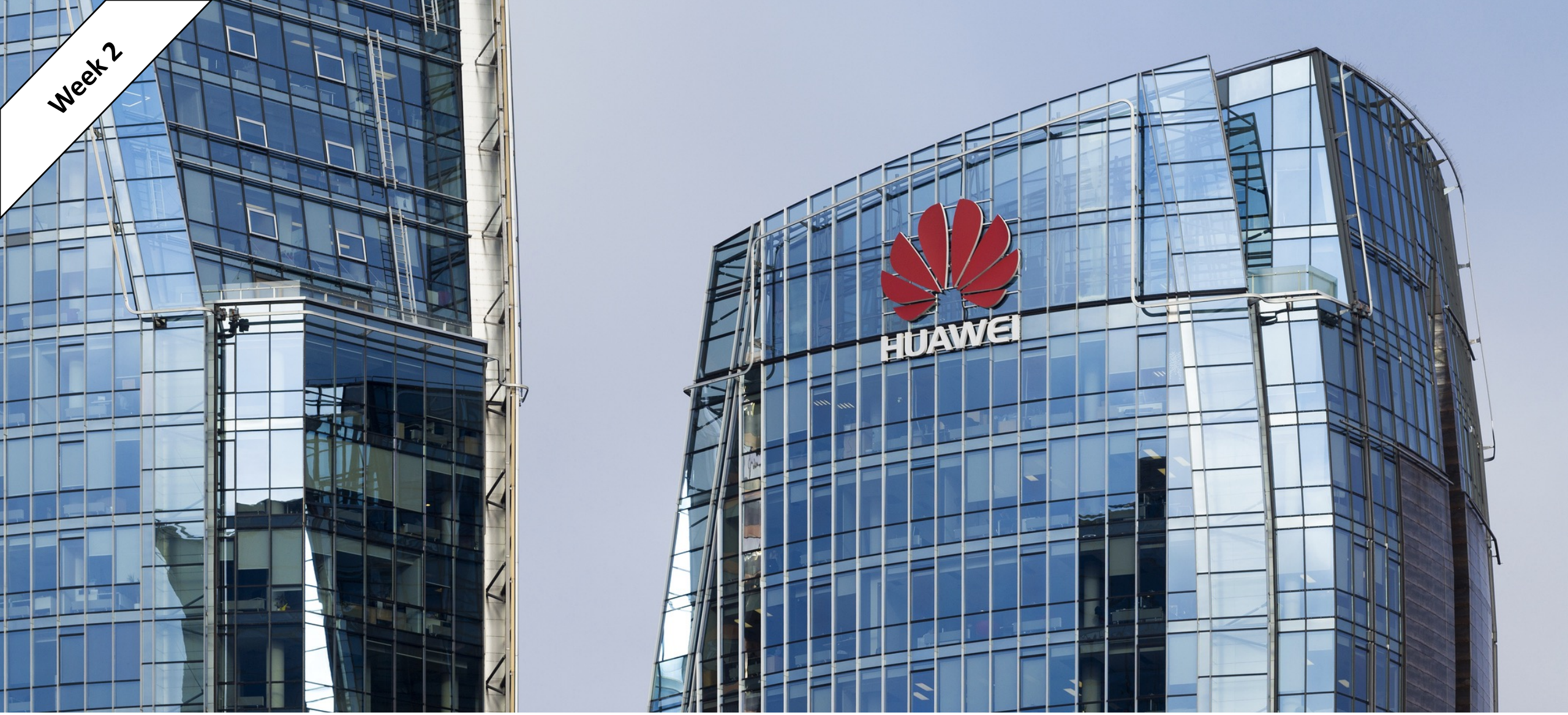
Advanced Risk Mitigation for Nation-State Controlled Trojan Horses

Week 2

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

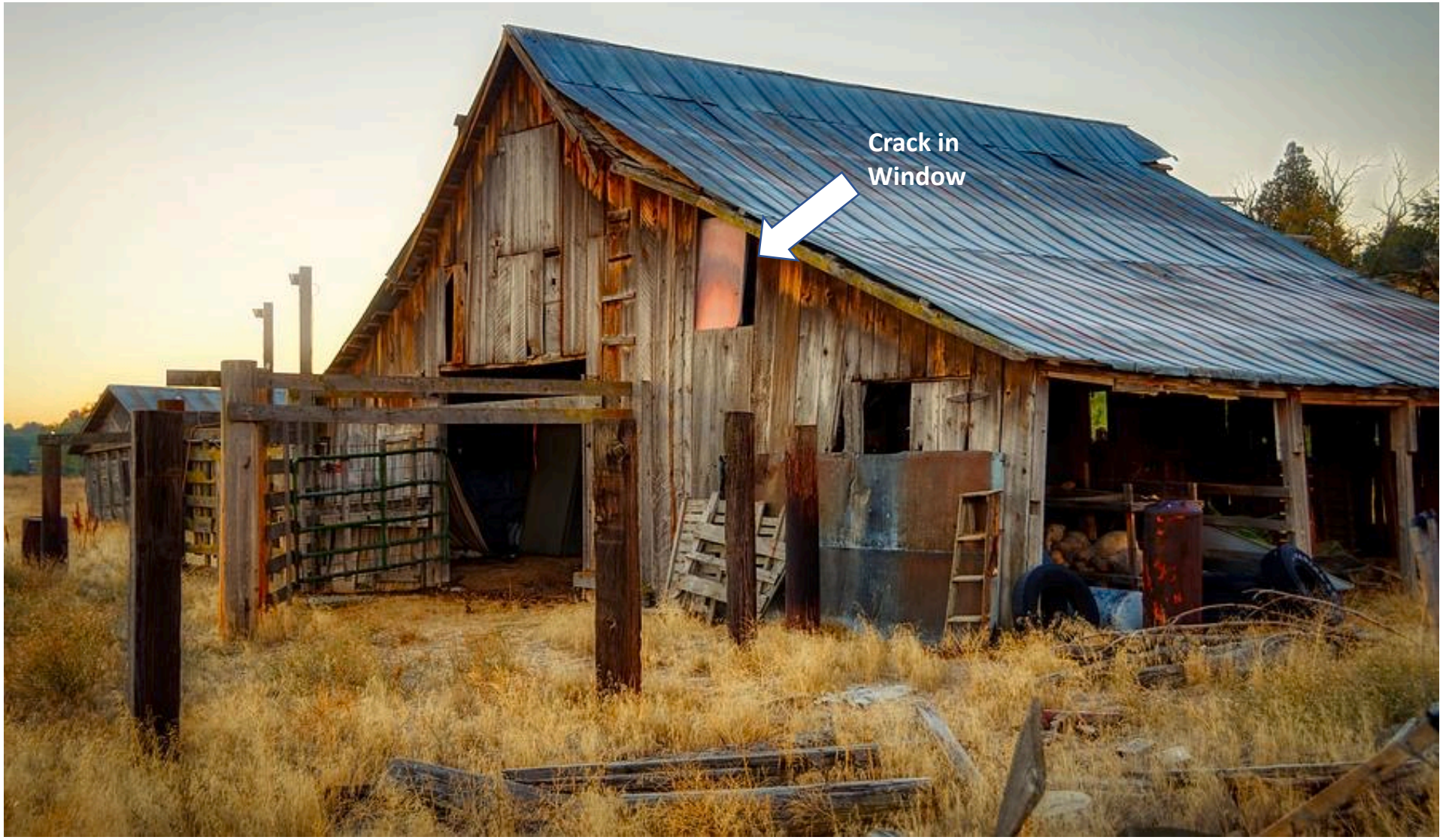
Week 2



US National Policy Regarding Chinese Telecommunications Firms

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

Week 2



Barn Analogy: Should You Worry About the Crack in the Window?

Week 2

WHY U.S. RESTRICTIONS ON CHINESE SOFTWARE WILL HAVE NO IMPACT ON CYBER RISK

DR. EDWARD AMOROSO

The actual cybersecurity benefit of Chinese product avoidance is nearly zero.

Here's something that every Washington lawmaker believes: Products from companies such as Huawei and ZTE are rigged with Trojans inserted under the direction of the Chinese government. They believe further that such malware could be invoked remotely to steal valuable intellectual property and interrupt essential services in the United States.

Viewed from this perspective, policy restrictions on the purchase of Chinese products would seem both sensible and necessary. And we know from Ken Thompson's seminal Turing address, based on his work at Bell Labs, that Trojan insertion is easy. One might thus be led to conclude that avoidance of Chinese products would have a material impact on cyber risk.

Unfortunately, the actual cybersecurity benefit of Chinese product avoidance is nearly zero. Furthermore, focusing our collective energy on this aspect of the

If you were to point to cracks in the roof as a primary issue, any reasonable observer would have to question the risk prioritization.

cyber risk equation diverts valuable time and attention from the real problem: our severe and nagging vulnerability in the United States against conventional cyberbreaches.

Let's start with the mistaken belief that Chinese government coercion can only work for companies headquartered in China. It's as if we think that malware could only be inserted into a product with full management cooperation. The view conjures the image of some conspiratorial meeting between company executives and the government to approve the Trojan plan.

In reality, government coercion would never be done this way. The approach instead would involve pressuring an individual with the right access and skills. This targeted entity would have a background or situation that could be used as influence leverage. And their supervisor would have no knowledge of the scheme. There would be no need to share this information.

This is a key observation, because such coercion could be done at virtually *any major technology company*. This includes Google, Microsoft and any other vendor with team members connected to China. Let me repeat: Avoiding software from companies headquartered in China does not remove the risk of Trojans in our software being controlled by China.

Now let's examine the mistaken belief that a nation-state needs Trojans to steal intellectual property or to disrupt systems. This is a patently absurd notion. Every cybersecurity expert knows that U.S. assets are regularly stolen or degraded by nation-state actors using basic offensive measures such as phishing, lateral traversal and DDOS.

An analogy might help: Imagine an old barn with broken doors, windows missing and cracks in the sidewalls. Obviously, if someone wanted to enter your barn, they would just come in through the open access. If you were to point to cracks in the roof as a primary issue, any reasonable observer would have to question the risk prioritization.

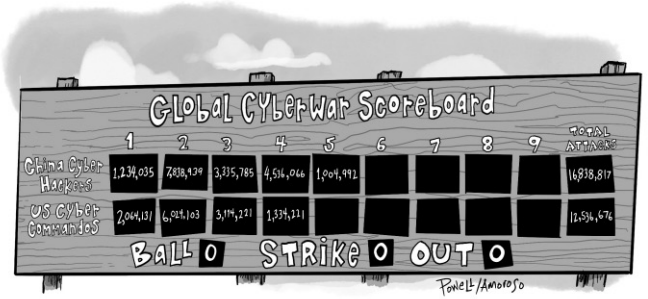
And never mind the view that it might be more obvious and dangerous to come in through the open doors—perhaps because of increased surveillance or security. The analogy does not hold for cyber:

Malicious nation-states have been coming in through our open gateways and access for many years. There has been zero need to leverage risky Trojans to steal data.

Finally, let's review the unfortunate consequence of focusing our supply chain security on country-specific avoidance. When we do this, we introduce the mistaken impression that we've reduced cyber risk in a material manner. And this can have a disastrous impact on control priorities and security budget by diverting attention away from meaningful security issues.

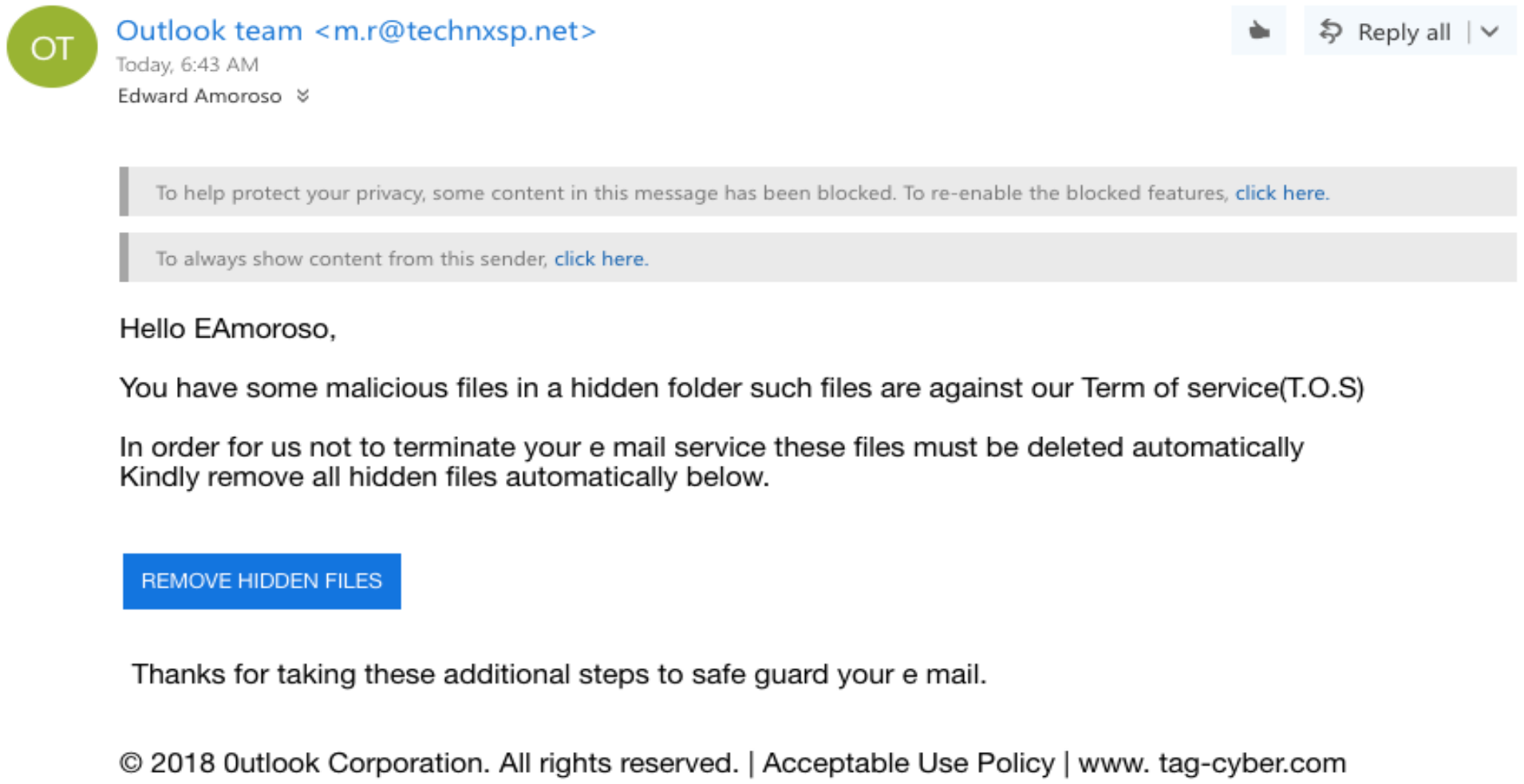
If policymakers decide to avoid China or any other country for reasons related to politics, economics or other noncyber matters, they should be clear about their motivation. But by pinning the issue on the cybersecurity community, they dilute public understanding of the real decision drivers, and, as explained above, they introduce harm to our nation's cyberposture.

The only reasonable cybersecurity policy for the United States is to significantly bolster our defenses. The details of this are beyond the scope of this article, but the main aspects of the approach would involve reduced complexity, increased resilience and greater focus on addressing our skills gap in security and information technology.



Why US Restrictions on China Will Have No Impact on Cyber Risk

Week 2



OT

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.

© 2018 0utlook Corporation. All rights reserved. | Acceptable Use Policy | www. tag-cyber.com

Still the Best Way to Steal Data (Even by Nation State Actors)