SECURITY (COMP0141): MALWARE

THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

Malware

THREAT MODEL FOR MALWARE

goal: infect machines with malware

stationary: requires action to be taken
autonomous: spreads without specific action

hidden: runs quietly in background
visible: has noticeable effect

WHAT DOES MALWARE DO?

What is the point of spreading malware?

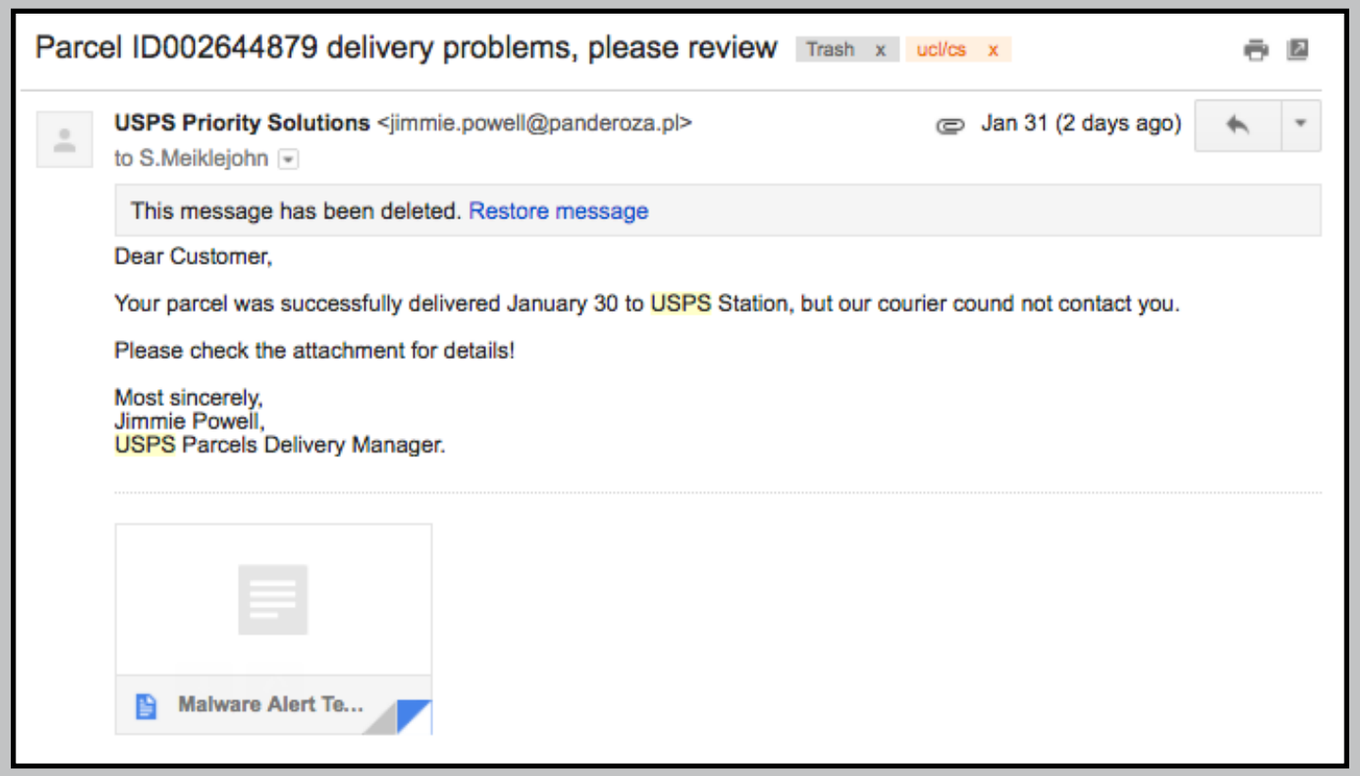
Financial motivation:

- expand botnet (A)
- steal information like credentials (CIA)
- ransomware (A)

Political motivation:

- state-level attacks (cyber warfare) (CIA)

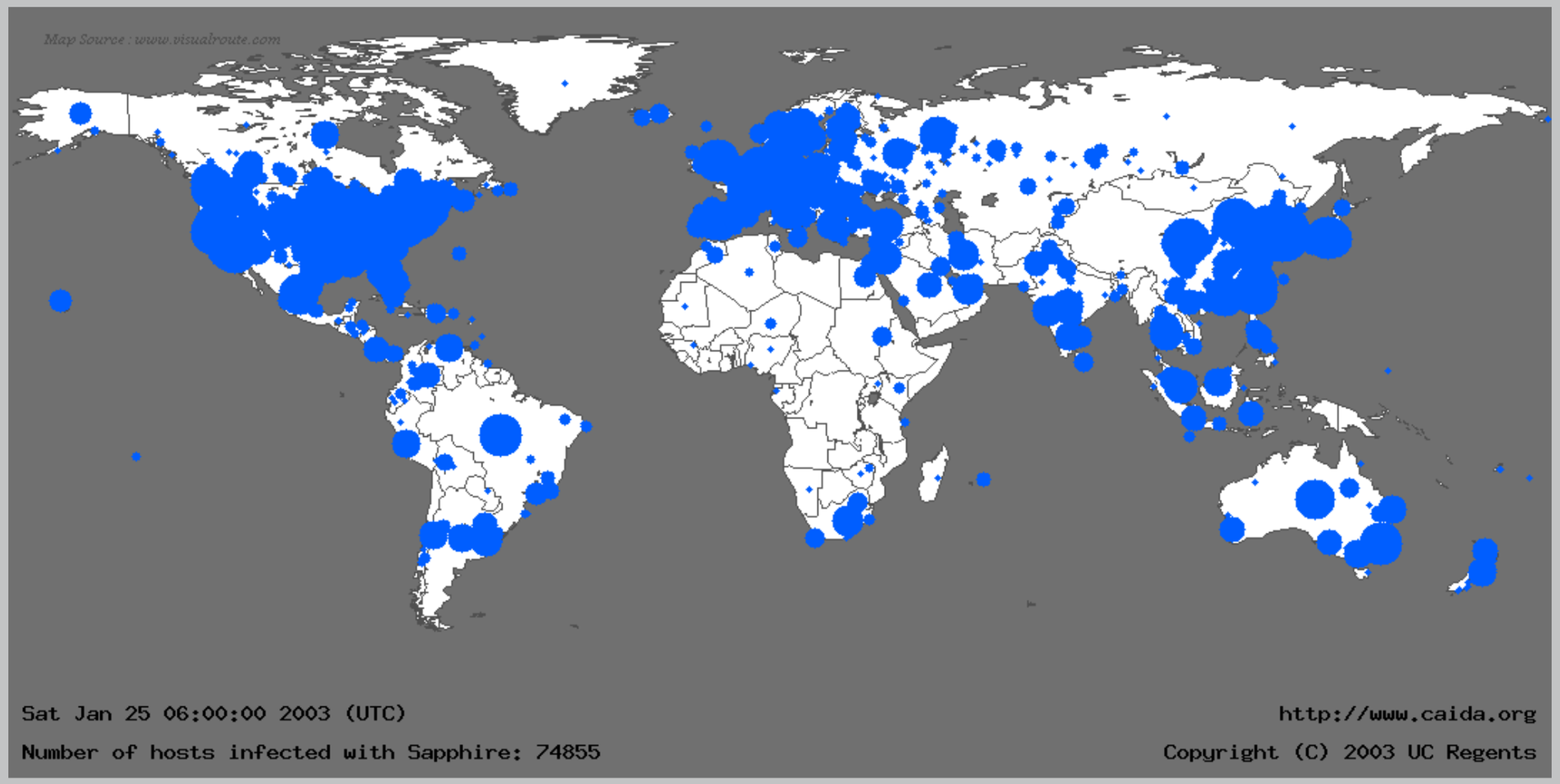
EXPANDING BOTNET: SPAM



users download attachments that contain **viruses**

viruses get replicated, attached to real code, executed

EXPANDING BOTNET: WORMS



spread autonomously by exploiting vulnerabilities

spread quickly and unpredictably, easy to detect

Slammer worm infected 75,000 within 10 minutes

EXAMPLE: MORRIS WORM

first (accidental) worm (1988)

required **the entire Internet** to reboot

EXPANDING BOTNET: TROJANS

disguise themselves as useful tools
can modify OS, so difficult to detect

EXAMPLES

Grum

-shut down in 2012
-500-900K infected
-26% of spam in 2010 (40B/day)
-infected via Trojan

ZeroAccess

-shut down in 2013
-2M infected
-click fraud/Bitcoin mining
-infected via Trojan

Cutwail

-shut down in 2010
-1.5-2M infected
-46% of spam in 2009 (74B/day)
-infected via Trojan

Storm

-peak in 2007
-1-50M infected
-20% of spam in 2008
-infected via “storm” spam

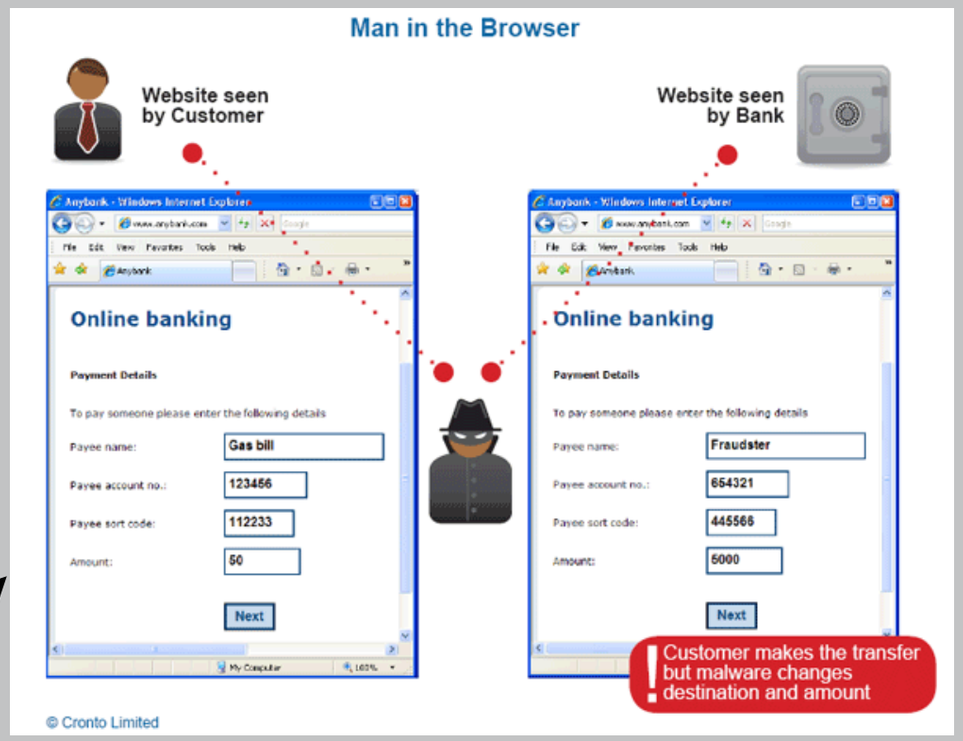
EXPANDING BOTNET

threat?

stationary (spam, Trojan) or **autonomous** (worm)

hidden (on bot itself) or **visible** (worm)

STEALING INFORMATION



keyloggers or **MitB** copy login/financial information

1,000 Facebook accounts cost around $50

Visa card number costs around $30

STEALING INFORMATION

threat?

stationary: requires action to be taken

visible: has noticeable effect (…eventually)

RANSOMWARE


CryptoLocker
!!! IMPORTANT INFORMATION !!!!
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://
tor2web.org/
2. http://
onion.to/
3. http://
onion.cab/
4. http://
onion.link/
If all of this addresses are not available, follow th
1. Download and install Tor Browser: https://v
2. After a successful installation, run the brow
3. Type in the address bar:
4. Follow the instructions on the site.
!!! Your personal identification ID:
"Locky" sets your wallpaper
Private key wil
9/13
9:1
71 : 59 : 48
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

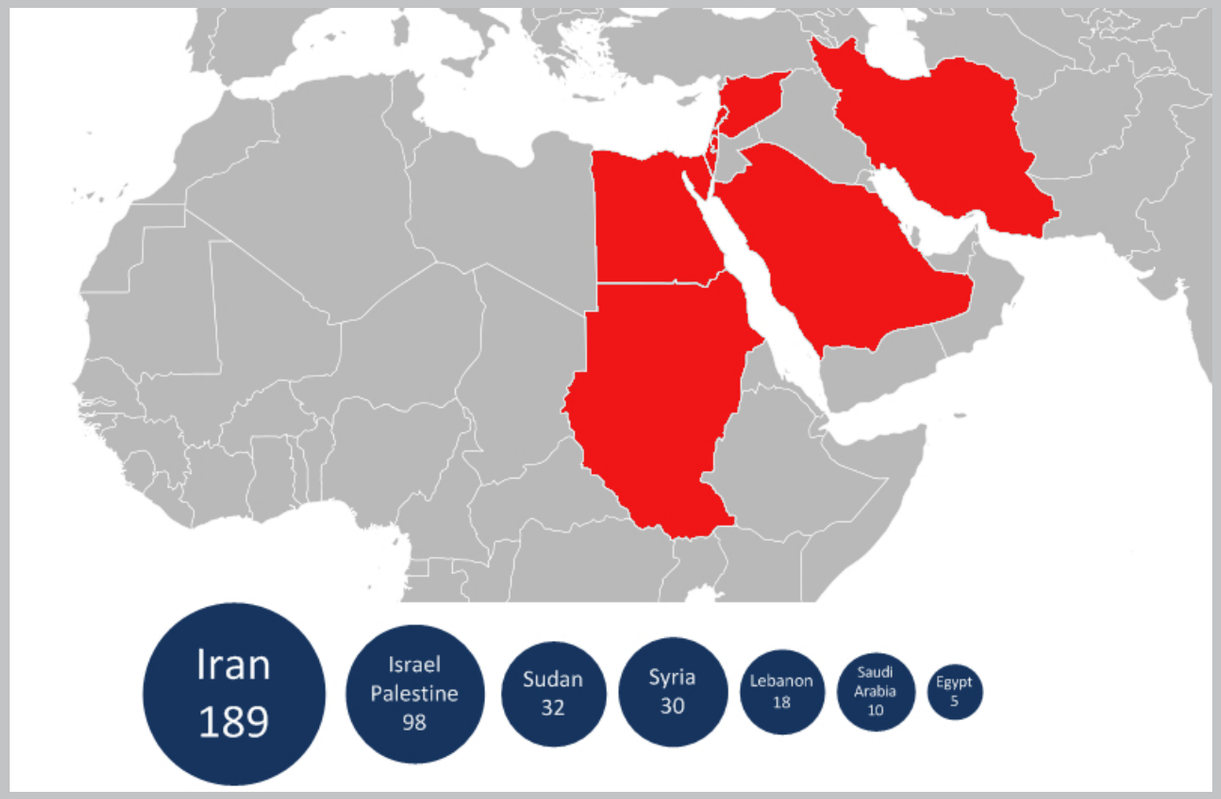
RANSOMWARE

threat?

stationary: requires action to be taken

visible: has noticeable effect

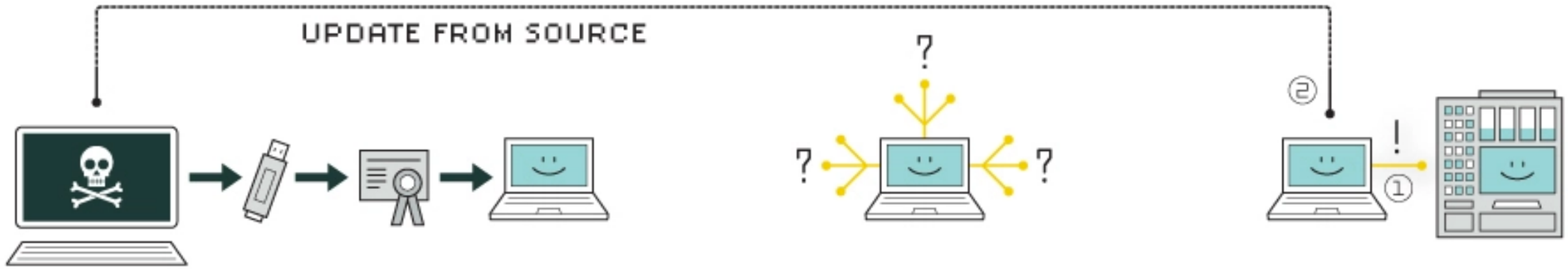
STATE-LEVEL ATTACKS



sophisticated malware developed by nation states
used to sabotage infrastructure or steal secrets
Flame (2012) was spyware targeting Iranian computers

EXAMPLE: STUXNET

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

HOW DO I GET MALWARE?

q: but how do booter services work? how to do it myself?

a: use a **botnet**.

q: what is the monetary point of creating a botnet?

a: DDoS as a service, **click fraud**, **spam**.

q: but how do I create a botnet in the first place?

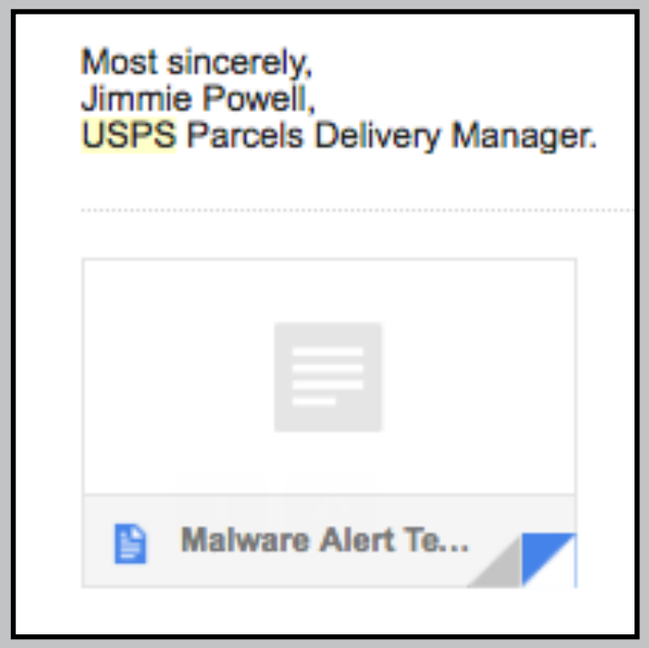
a: infect computers with **malware**.

q: so most malware is stationary. how do I get it then?

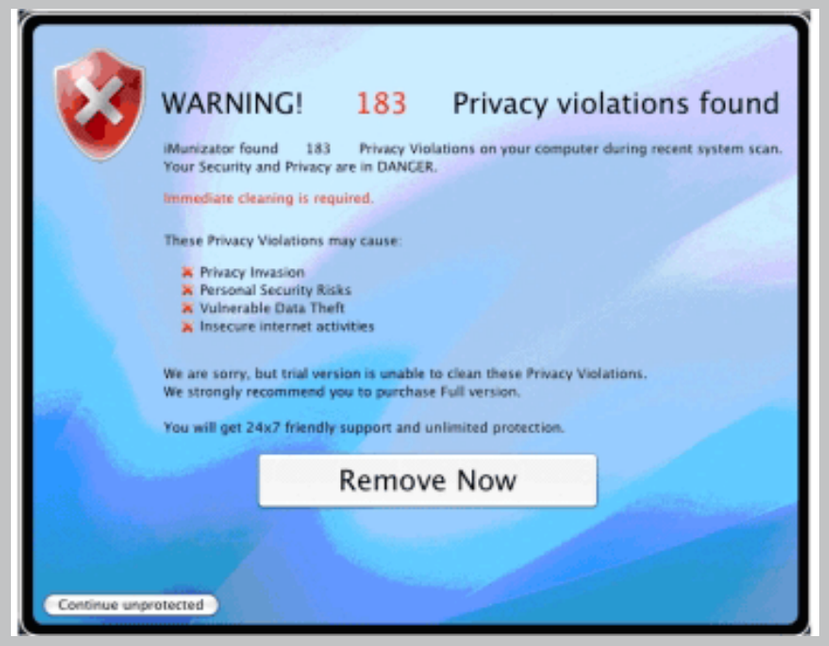
a: various **vulnerabilities** in both humans and machines.

SOCIAL ENGINEERING

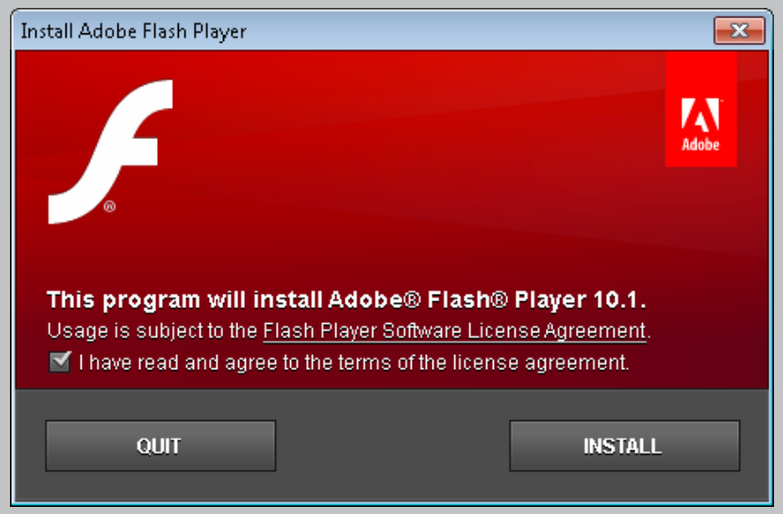
email attachments



scareware

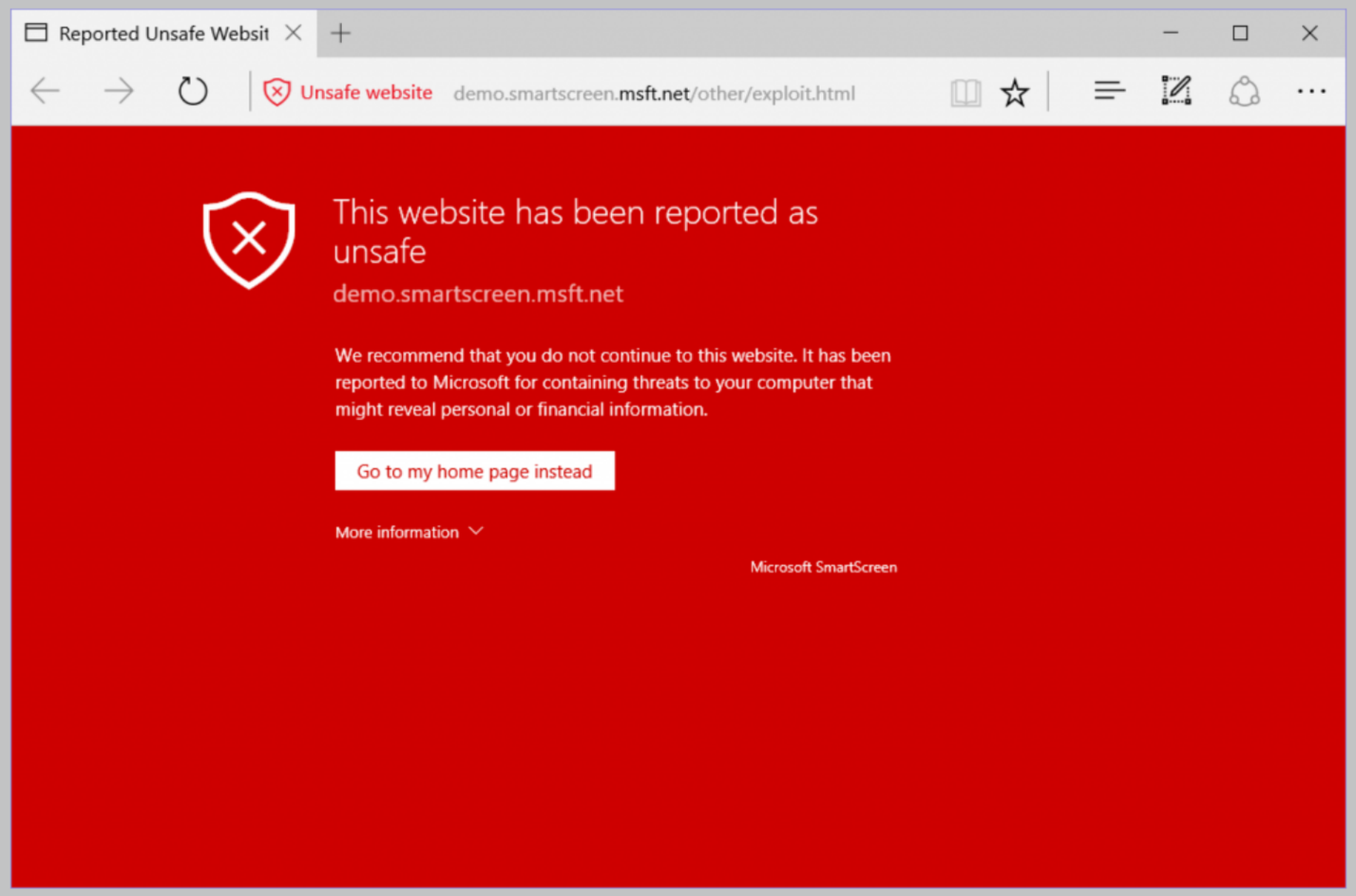


software updates



devices (USB, CD, etc.)

DRIVE-BY DOWNLOAD



vulnerability (in browser, plugin, etc.) is exploited
computer **automatically** installs malware

HOW DO I *NOT* GET MALWARE?

q: but how do booter services work? how to do it myself?

a: use a **botnet**.

q: what is the monetary point of creating a botnet?

a: DDoS as a service, **click fraud**, **spam**.

q: but how do I create a botnet in the first place?

a: infect computers with **malware**.

q: so most malware is stationary. how do I get it then?

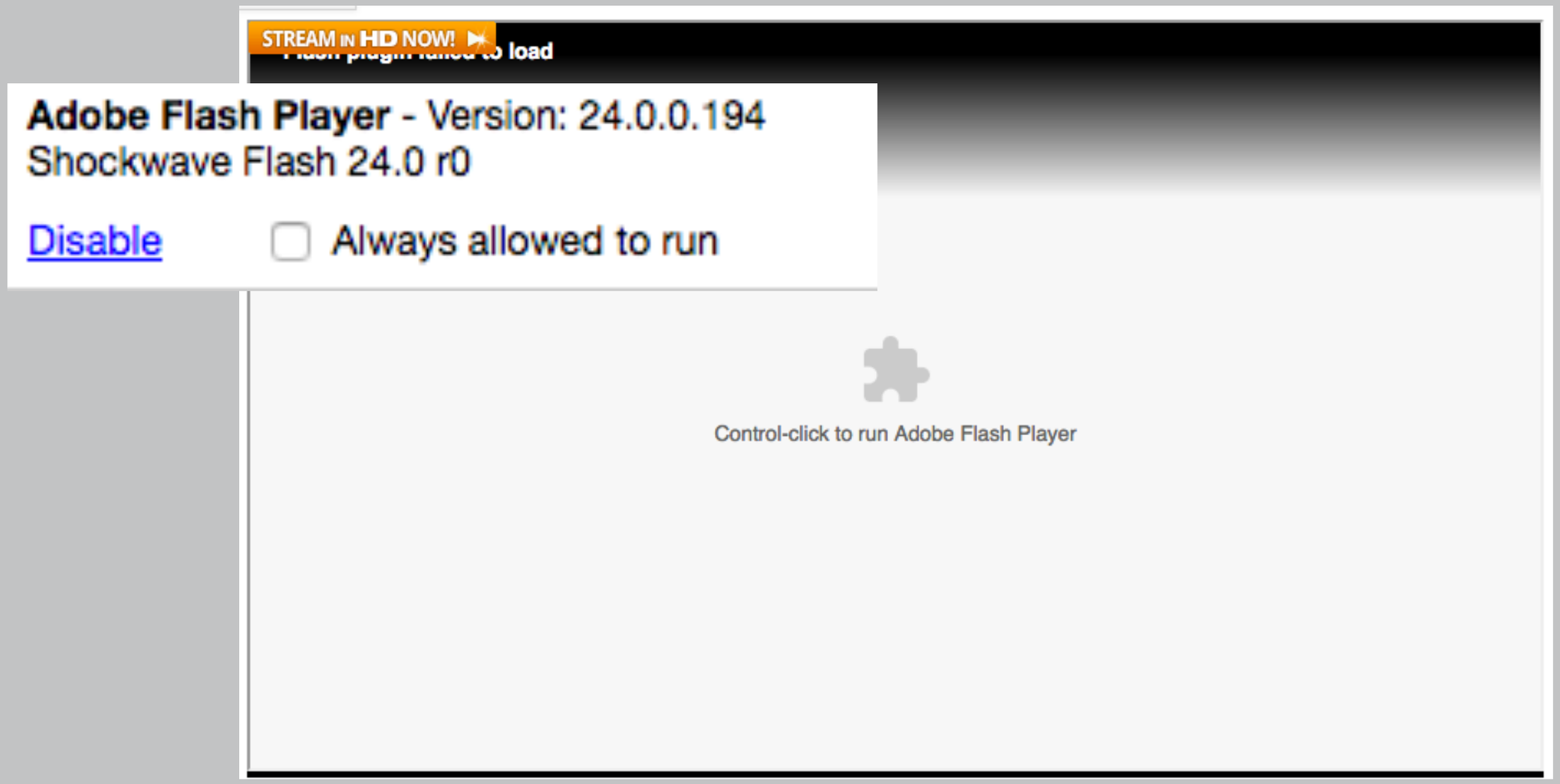
a: various **vulnerabilities** in both humans and machines.

q: I'm scared! how do I avoid getting malware?

a: don't go to bad sites, use software, extensions, etc.

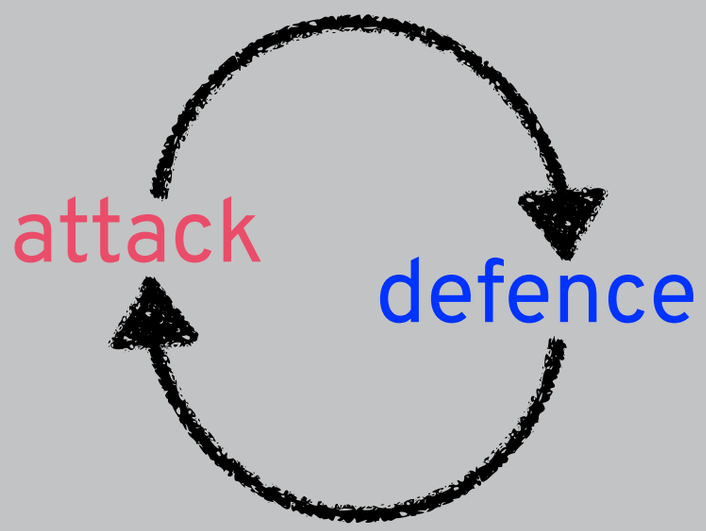
MINIMISE VULNERABILITIES

risk management



USE AV SOFTWARE

risk management



VIRUS SCANNING

virus scanning

H(attachment) → in list? →

bad hashes

rEK1ecacw7c

qi8H8R7OM4x

...

1O3JMY.Tw

UNIFORMITY

$H: \{0,1\}^* \rightarrow \{0,1\}^k$

string of arbitrary length

string of fixed length

uniformity: even small changes in input yield big changes in output

uniqueness: given $h = H(m)$, should be very low chance of collision (m_2 s.t. $H(m_2) = h$)

SHA256 hashes of…

sarah

28d628a681884cbfe83875d74ae6d9e9b4f2f211b73427ab3e83c3937d0fd028

sarah1

a2b2a43003a3e63e4c50ffb2b68d2d4d55a6cd1b8627e3e3601e984e2251ee7f

sarah12

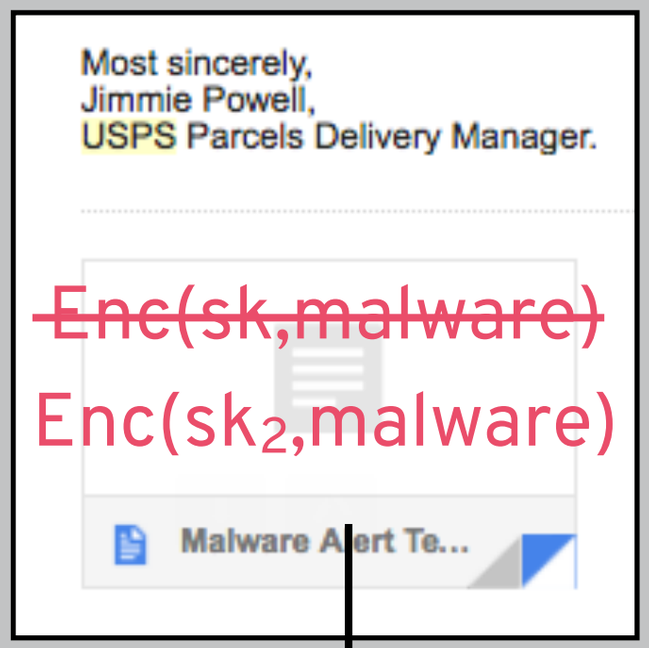
f3bd2f4bf7e713611c5e6854a74e83c681ec9e6754ab65e63a3ce760e7c22770

sarah123

7b2935a21b68f3a6361118b2024f5547bfe9fdcc80445a4afbf62ea231a6496b

VIRUS SCANNING

virus scanning



~~Enc(sk,malware)~~

Enc(sk_2,malware)

~~H(attachment)~~ —in list? ✓→

H($attachment_2$) —in list? ✗→

bad hashes

rEK1ecacw7c

qi8H8R7OM4x

...

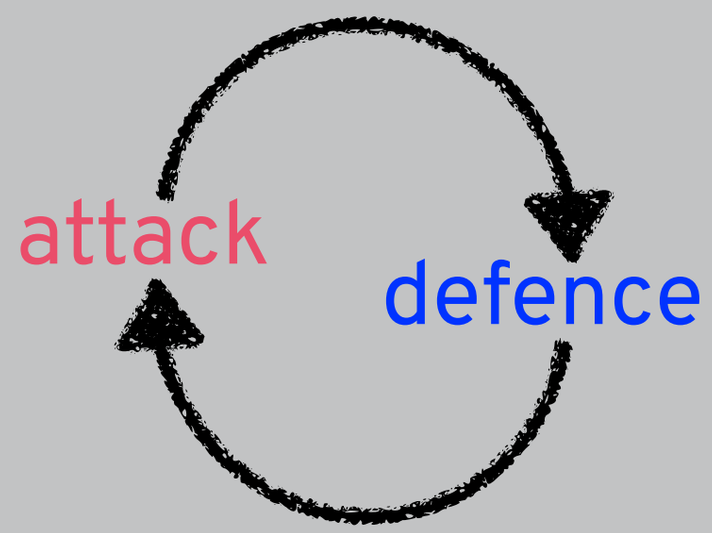
1O3JMY.Tw

metamorphic: different code has same effect

polymorphic: each copy encrypted differently

USE AV SOFTWARE

risk management



malware is adaptive

metamorphic: different code has same effect

polymorphic: each copy encrypted differently

CIA TRIANGLE