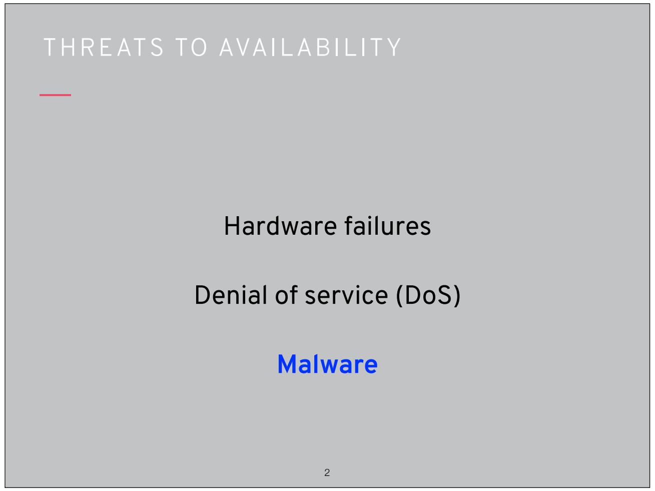
# SECURITY (COMP0141): MALWARE

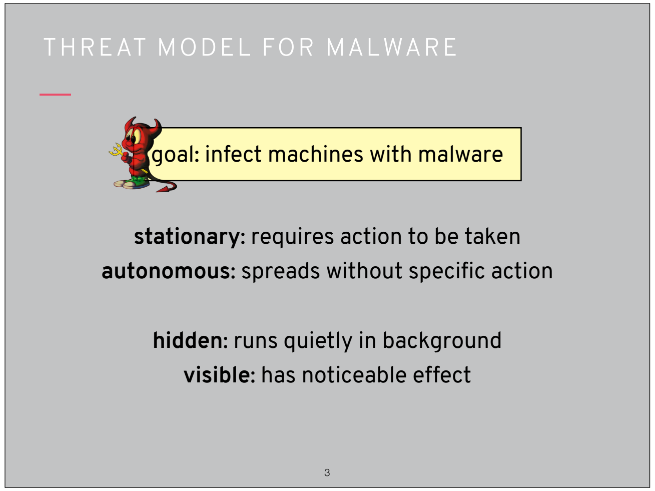


## THREATS TO AVAILABILITY

Hardware failures

Denial of service (DoS)

**Malware**



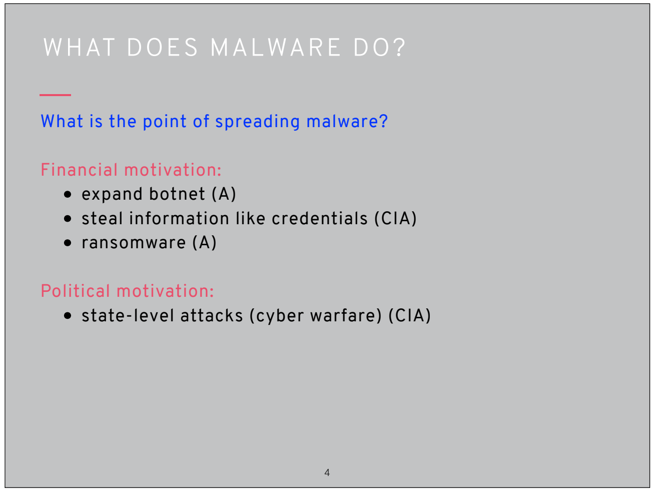
## THREAT MODEL FOR MALWARE

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

Attacker can create malware that is installed with or without specific action (like clicking on something). Malware can be noticeable or not



## WHAT DOES MALWARE DO?

What is the point of spreading malware?

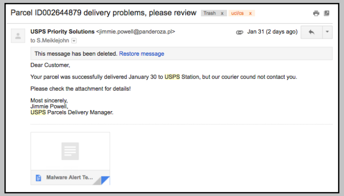
Financial motivation:

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

Political motivation:

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

## EXPANDING BOTNET: SPAM



Parcel ID002644879 delivery problems, please review

**USPS Priority Solutions** <jimmie.powell@panderoza.pl>
to S.Meiklejohn

Jan 31 (2 days ago)

This message has been deleted. Restore message

Dear Customer,

Your parcel was successfully delivered January 30 to USPS Station, but our courier cound not contact you.

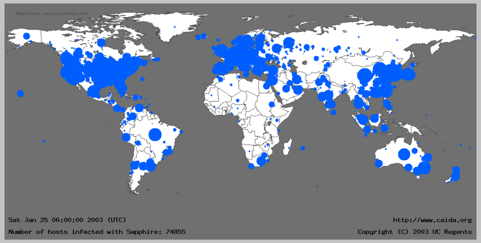
Please check the attachment for details!

Most sincerely,
Jimmie Powell,
USPS Parcels Delivery Manager.

users download attachments that contain **viruses**
viruses get replicated, attached to real code, executed

Spam is useful for infecting new machines via viruses

## EXPANDING BOTNET: WORMS



Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

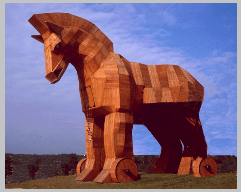
spread autonomously by exploiting vulnerabilities
spread quickly and unpredictably, easy to detect
Slammer worm infected 75,000 within 10 minutes

Worms can get out of control very quickly

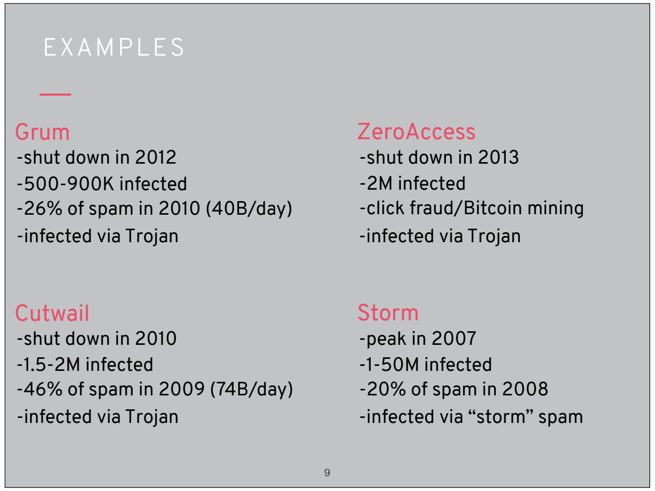
## EXAMPLE: MORRIS WORM

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

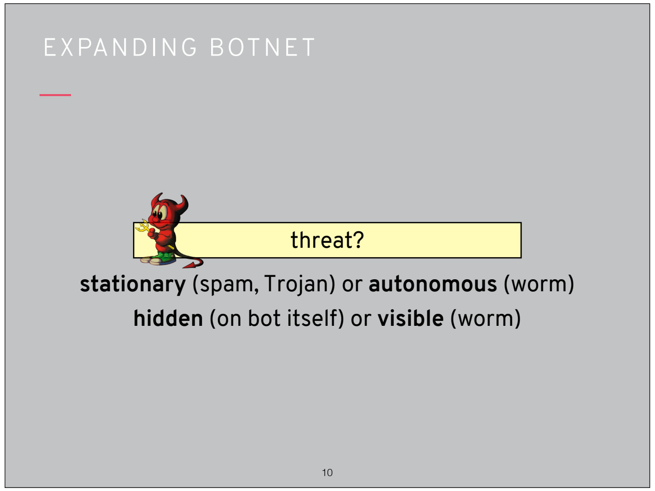
**Grum**
- shut down in 2012
- 500-900K infected
- 26% of spam in 2010 (40B/day)
- infected via Trojan

**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

Most of these infected via Trojan, except Storm (sent spam related to weather phenomena)

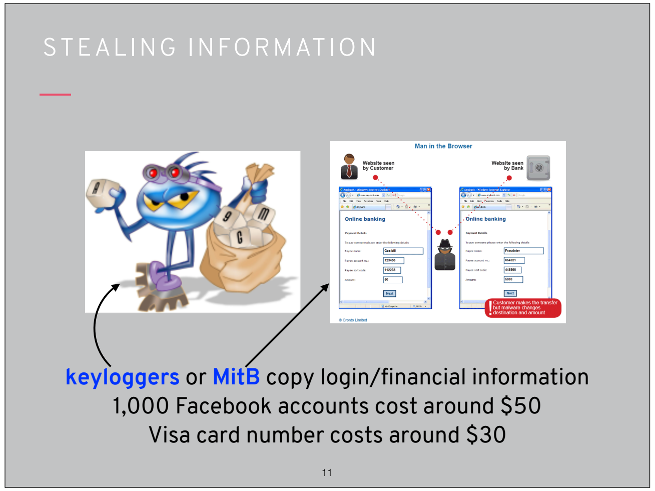


## EXPANDING BOTNET

threat?

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

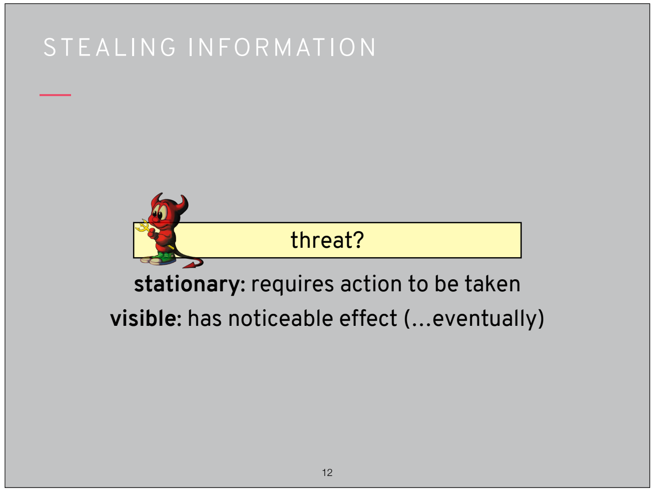
**hidden** (on bot itself) or **visible** (worm)



## STEALING INFORMATION

**keyloggers** or **MitB** copy login/financial information
1,000 Facebook accounts cost around $50
Visa card number costs around $30

Keylogger is a piece of software that logs all your keystrokes, man-in-the-browser (MitB) exploits browser vulnerability, both steal information (and then either use or sell it)



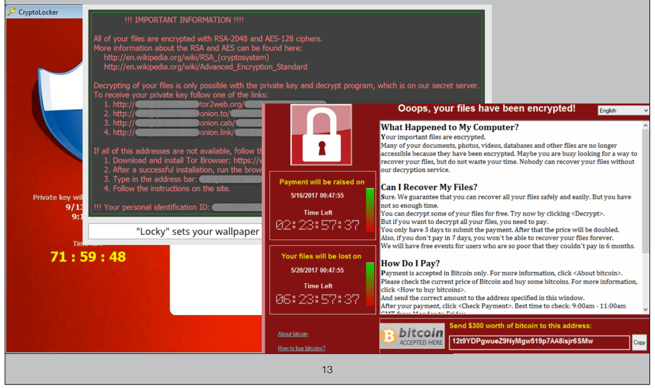
## STEALING INFORMATION

threat?

**stationary:** requires action to be taken
**visible:** has noticeable effect (...eventually)

Obviously you’ll notice eventually if an attacker uses your information

## 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://[redacted]tor2web.org/[redacted]
2. http://[redacted]onion.to/[redacted]
3. http://[redacted]onion.cab/[redacted]
4. http://[redacted]onion.link/[redacted]

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: [redacted]
4. Follow the instructions on the site.

!!! Your personal identification ID: [redacted]

"Locky" sets your wallpaper

Private key wil
9/13
9:1

71 : 59 : 48

Ooops, your files have been encrypted!

English

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?

**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

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware is very much on the rise, best known example might be WannaCry (which is an attack that shut down the NHS in 2017). It encrypts your files and demands a ransom paid in bitcoins to give the decryption key

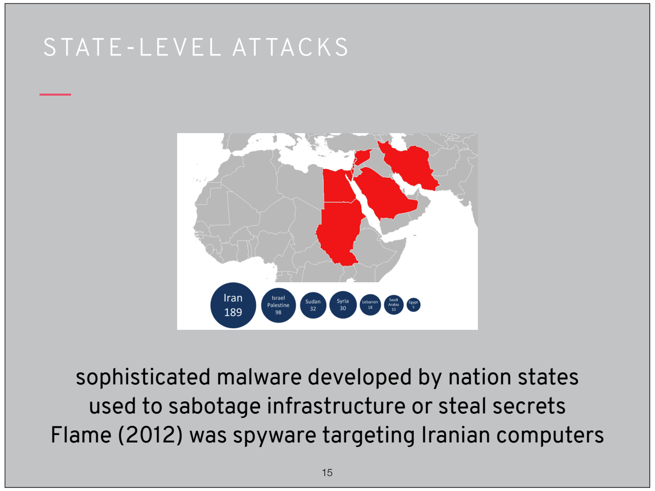
## RANSOMWARE

threat?

**stationary:** requires action to be taken

**visible:** has noticeable effect

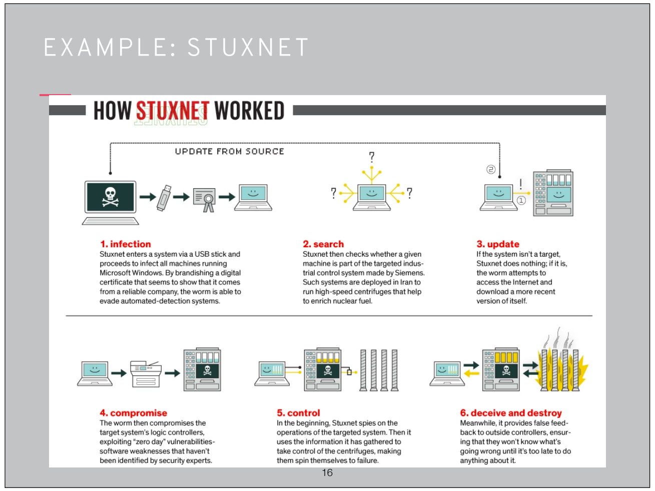
Most obviously noticeable and immediately monetizable (literally just get paid)



## STATE-LEVEL ATTACKS

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

State-level attacks are of course more sophisticated, pretty recent example was Flame



## 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.

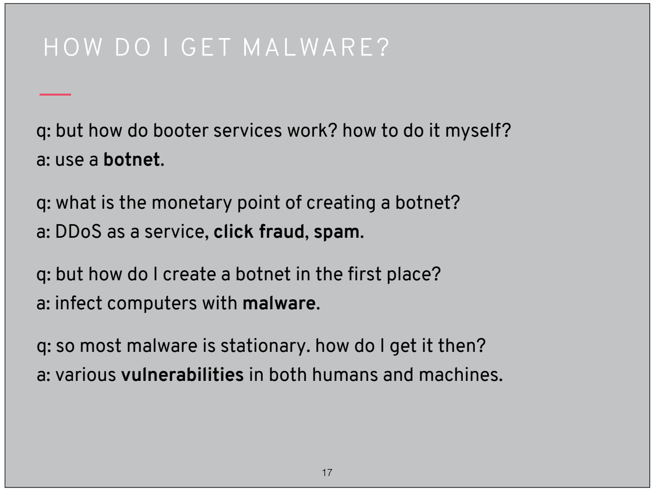
**3. update**
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

**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.

Stuxnet targeted Iranian nuclear facilities



## HOW DO I GET MALWARE?

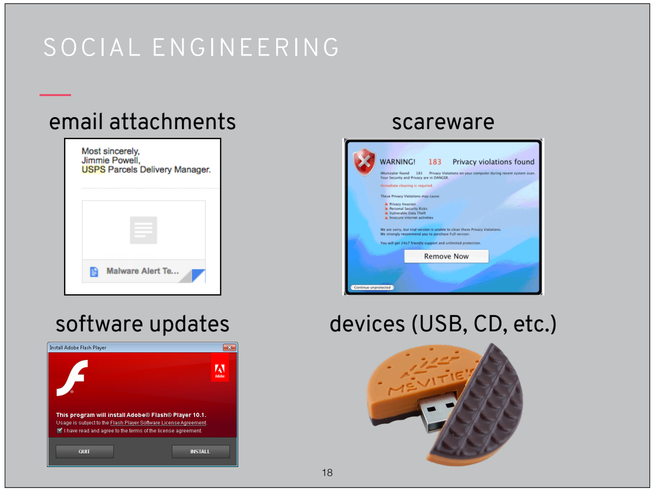
q: but how do booter services work? how to do it myself?
a: use a **botnet**.

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.

If action is required to get malware though, then how do people get infected?



## SOCIAL ENGINEERING

email attachments

Most sincerely,
Jimmie Powell,
USPS Parcels Delivery Manager.

scareware

WARNING! 183 Privacy violations found

iMunizator found 183 Privacy Violations on your computer during recent system scan.
Your Security and Privacy are in DANGER.

Immediate cleaning is required.

These Privacy Violations may cause:

- Privacy Invasion
- Personal Security Risks
- Vulnerable Data Theft
- Insecure internet activities

We are sorry, but trial version is unable to clean these Privacy Violations.
We strongly recommend you to purchase Full version.

You will get 24x7 friendly support and unlimited protection.

software updates

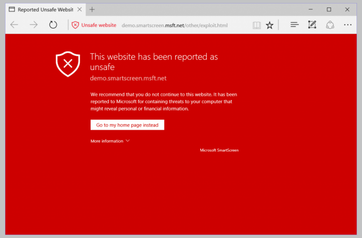
Install Adobe Flash Player

This program will install Adobe® Flash® Player 10.1.
Usage is subject to the Flash Player Software License Agreement.
☑ I have read and agree to the terms of the license agreement.

devices (USB, CD, etc.)

People click on things, or get confused and download things, or insert unknown devices

## DRIVE-BY DOWNLOAD



This website has been reported as unsafe

demo.smartscreen.msft.net

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

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

Or they just go to a bad website and something gets downloaded and installed without their knowledge

## HOW DO I *NOT* GET MALWARE?

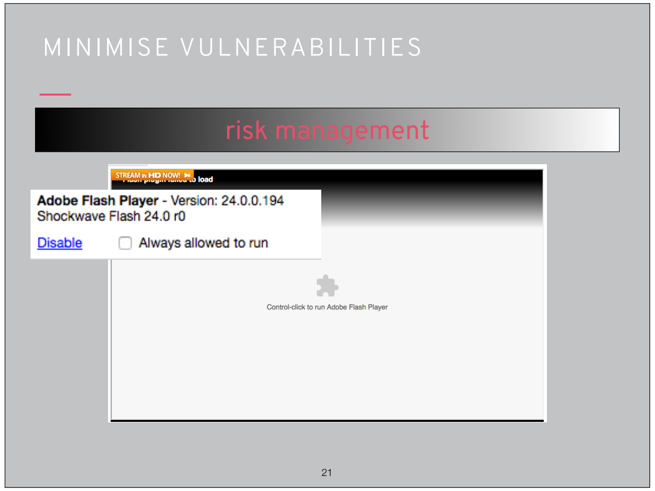
q: but how do booter services work? how to do it myself?
a: use a **botnet**.

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

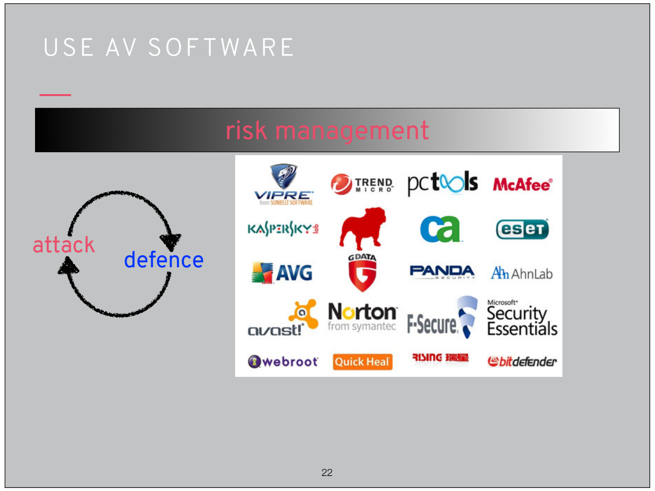
risk management

**Adobe Flash Player** - Version: 24.0.0.194
Shockwave Flash 24.0 r0

Disable ☐ Always allowed to run

Control-click to run Adobe Flash Player

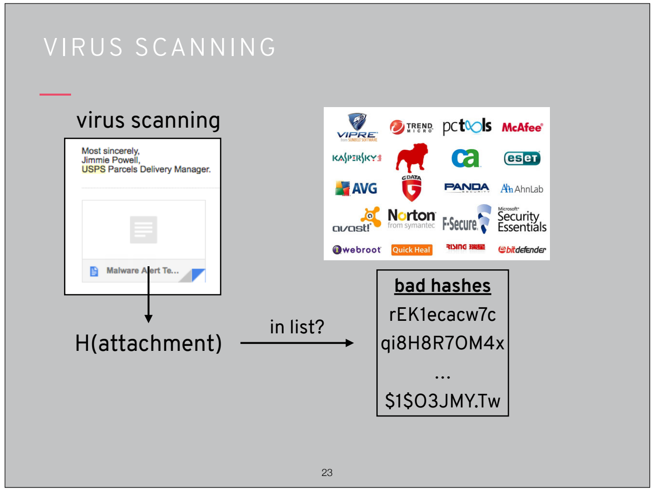
Can try to plug holes in terms of vulnerabilities, plugins like Flash are especially bad



## USE AV SOFTWARE

risk management

Anti-virus software and filters rely on seeing existing samples so are very much a heuristic approach. Again, this is very much an arms race



## VIRUS SCANNING

virus scanning

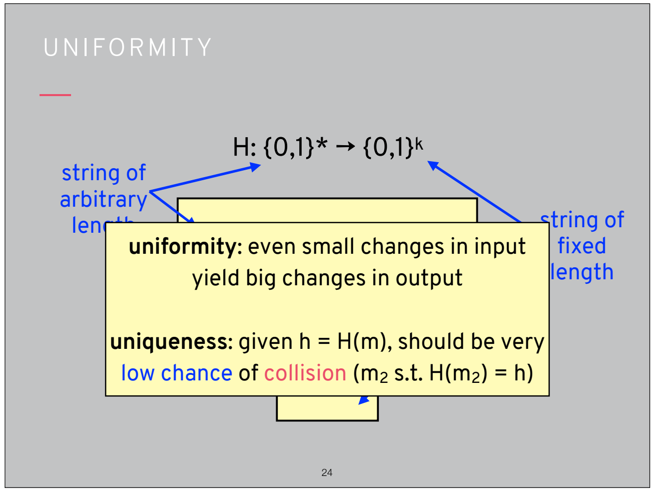
Most sincerely,
Jimmie Powell,
USPS Parcels Delivery Manager.

Malware Alert Te...

H(attachment) → in list? →

| bad hashes |
|---|
| rEK1ecacw7c |
| qi8H8R7OM4x |
| … |
| $1$O3JMY.Tw |

Anti-virus software checks to see if something is malware or not by comparing its hash to a list of known bad hashes



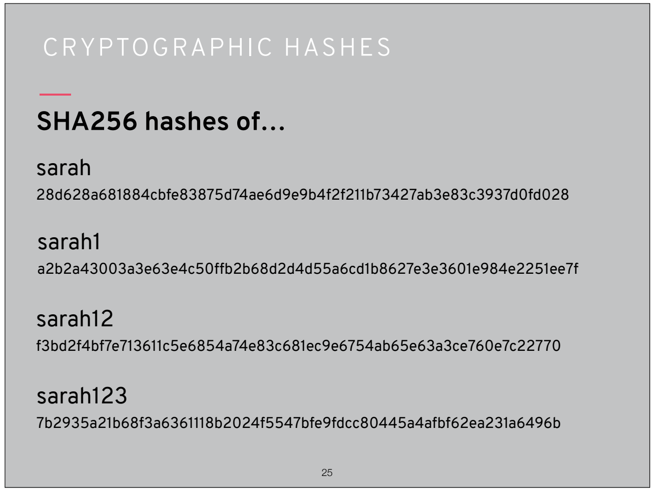
## UNIFORMITY

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

**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. $H(m_2) = h$)

One of the problems with this approach is that it’s pretty fragile, because of the uniformity property of hash functions



## CRYPTOGRAPHIC HASHES

**SHA256 hashes of…**

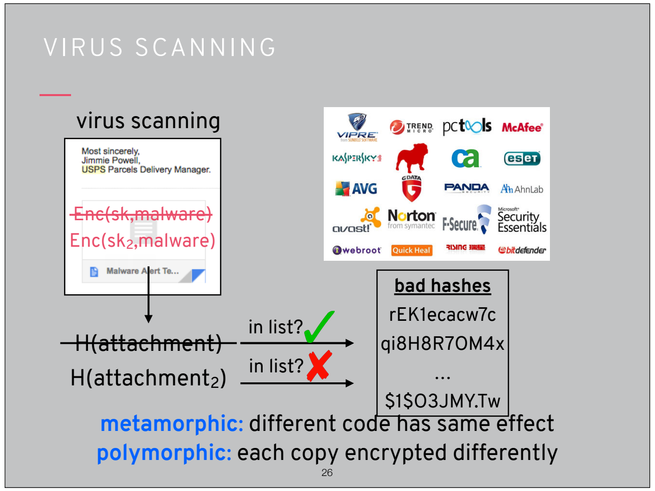
sarah
28d628a681884cbfe83875d74ae6d9e9b4f2f211b73427ab3e83c3937d0fd028

sarah1
a2b2a43003a3e63e4c50ffb2b68d2d4d55a6cd1b8627e3e3601e984e2251ee7f

sarah12
f3bd2f4bf7e713611c5e6854a74e83c681ec9e6754ab65e63a3ce760e7c22770

sarah123
7b2935a21b68f3a6361118b2024f5547bfe9fdcc80445a4afbf62ea231a6496b

Remember this means that a small difference in the input to a hash function yields a huge difference in the output



## VIRUS SCANNING

virus scanning

Most sincerely,
Jimmie Powell,
USPS Parcels Delivery Manager.

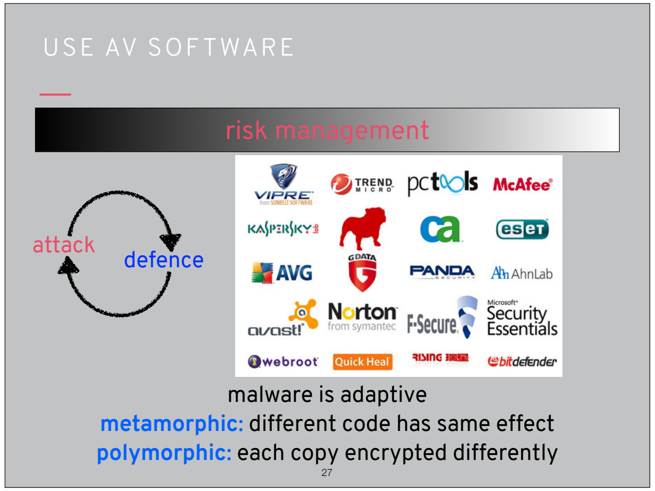
~~Enc(sk,malware)~~
Enc($sk_2$,malware)

~~H(attachment)~~ in list? ✓
H($attachment_2$) in list? ✗

**bad hashes**
rEK1ecacw7c
qi8H8R7OM4x
...
$1$O3JMY.Tw

**metamorphic:** different code has same effect
**polymorphic:** each copy encrypted differently

This means that an attacker can change malware in very small ways (so different copy for each different victim) and it will look completely unfamiliar to the anti-virus software



## USE AV SOFTWARE

risk management

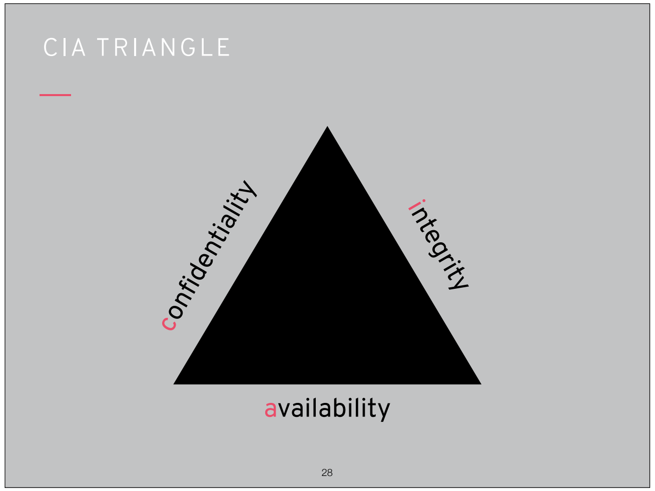
attack
defence
VIPRE
TREND MICRO
pctools
McAfee
KASPERSKY
ca
eset
AVG
G DATA
PANDA
AhnLab
avast!
Norton from symantec
F-Secure
Microsoft Security Essentials
webroot
Quick Heal
RISING
bitdefender

malware is adaptive

**metamorphic:** different code has same effect

**polymorphic:** each copy encrypted differently

Basically malware just needs to slightly adapt in order to evade detection



## CIA TRIANGLE

That’s it (for now) for the CIA triangle: saw many cryptographic security mechanisms for confidentiality and integrity but security mechanisms tend to be much more heuristic for availability