Defense against the Dark Arts
Overview / Terminology

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **20/01/15 - 16:13** the cost of decrypting files will increase **2** times and will be **1000 USD/EUR**

Prior to increasing the amount left:

167h 59m 00s

Your system: Windows XP (x32) First connect IP: [redacted] Total encrypted **2860** files.

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

bitcoin

1. **You should register Bitcon wallet (click here for more information with pictures)**

2. **Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.**

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of**

malware

“evil software”

malware

"evil software"

display a funny message

send passwords/credit card numbers to criminals

take pictures to send to criminals

delete data

hold data hostage

insert/replace ads in webpages

...

viruses

malware that inserts itself into another program

"infects" other programs when run

- usually modifies executables directly

macro viruses

Word, Excel, other office software support macros

- scripts embedded in Word/Excel/etc. documents

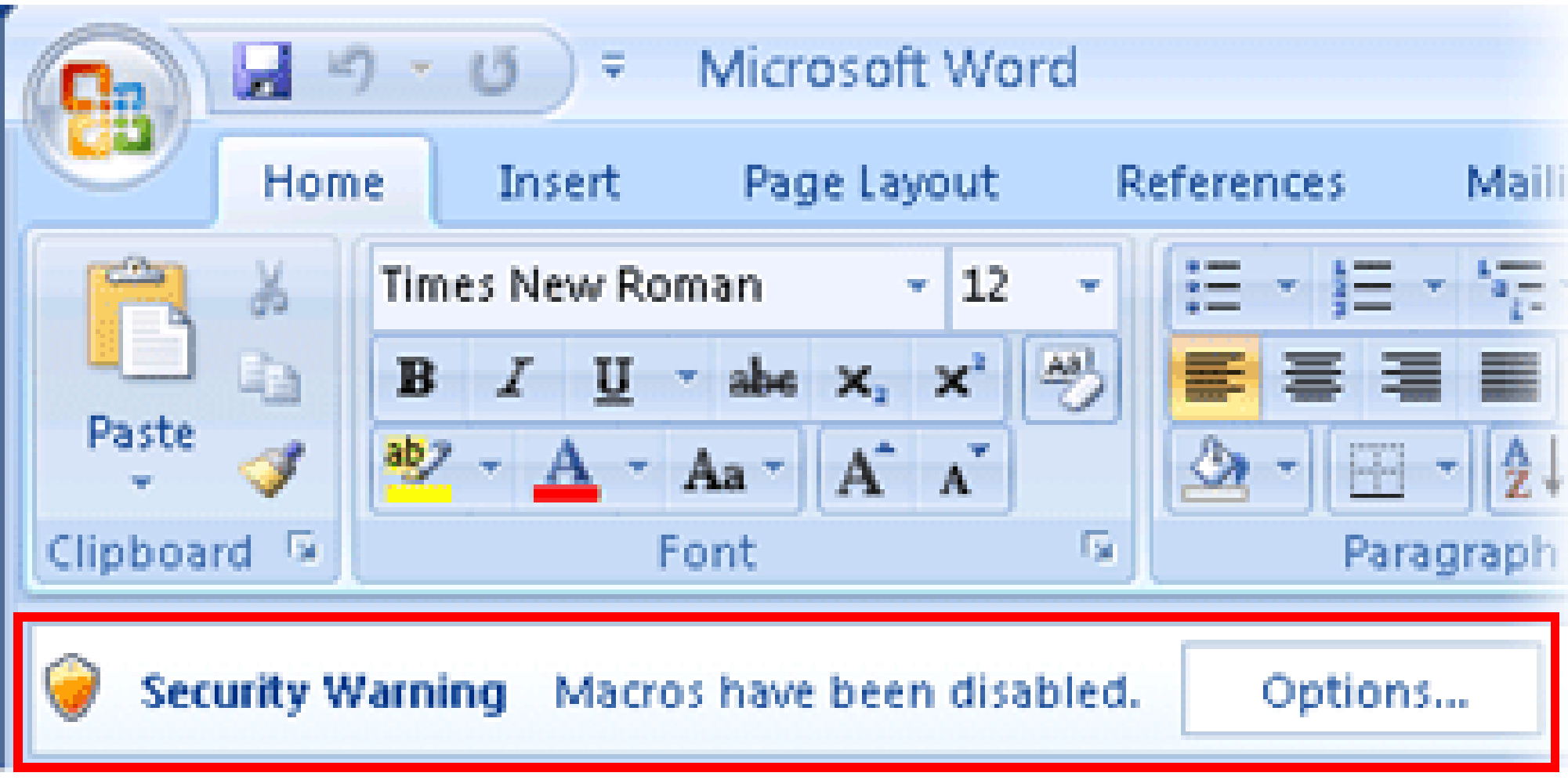
viruses written in a scripting language

- Visual Basic for Applications

spread to office documents, not executables

- easily spread in corporate environments

vendor reaction: macros disabled by default now


Microsoft Word
Home
Insert
Page Layout
References
Paste
Times New Roman
12
Clipboard
Font
Paragraph
Security Warning
Macros have been disabled.
Options...

all viruses?

some sources call almost all malware *virsues*

or all self-propagating malware

I won't — but I will avoid testing you on this

goal of hierarchy is knowing variety, not characterizing

worms

independent program

usually “blends in” with system programs

copies itself to other machines or USB keys, etc.

sometimes configures systems to run it automatically

trojan (horse)s

useful-looking program that is malware:

- 'cracked' version of commerical software
- fake anti-virus software
- or looks like useful PDF doc
- ...

maybe is (or not), but also does something evil

common form for targeted attacks

potentially unwanted programs

unwanted software bundled with wanted software

sometimes disclosed but in deceptive fine print

sometimes considered malware, sometimes not

rootkit

root = full privileges

common name for Unix administrator account

rootkit = malware for maintaining full control

thing that malware/attackers install

rootkits evade removal, detection

e.g. program made invisible to "task manager"/ps

e.g. reinstall malware if removed "normally"

logic bomb

dormant malicious code

e.g. from disgruntled employee before quitting

vulnerabilities

trojans: the vulnerability is the user

and/or the user interface

otherwise?

software vulnerability

unintended program behavior
that can be used by an adversary

vulnerability example

website able to install software without prompting

not intended behavior of web browser

software vulnerability classes (1)

memory safety bugs

- problems with pointers
- big topic in this course

"injection" bugs — type confusion

- commands/SQL within name, label, etc.

integer overflow/underflow

...

software vulnerability classes (2)

not checking inputs/permissions

```
http://webserver.com/../../../../
file-I-shouldn't-get.txt
```

almost any 's "undefined behavior" in C/C++

synchronization bugs: time-to-check to time-of-use

... more?

vulnerability versus exploit

exploit — something that uses a vulnerability to do something

proof-of-concept — something = demonstration the exploit is there

example: open a calculator program

malware logistics: how?

what are they written in?

malware languages (1)

assembly language/machine code

hand-coded or partially hand-coded

vulnerabilities deal with machine code/memory layout

better for hiding malware from anti-malware tools

malware languages (2)

high-level scripting languages

- fast prototyping
- maintainability/efficiency not priority
- sometimes malicious scripts
- non-machine-code parts can use anything!

sometimes specialized "toolkits"

example: Virus Construction Kit

malware spreading

vulnerable network-accessible services

shared files/folders

- autorun on USB sticks
- macros in Word/Excel/etc. files

email attachments

websites + browser vulnerabilities

- JavaScript interpreter bugs
- Adobe Flash Player bugs

malware defenses (1)

"antivirus" software:

Windows Defender

avast!

Avira

AVG

McAfee

...

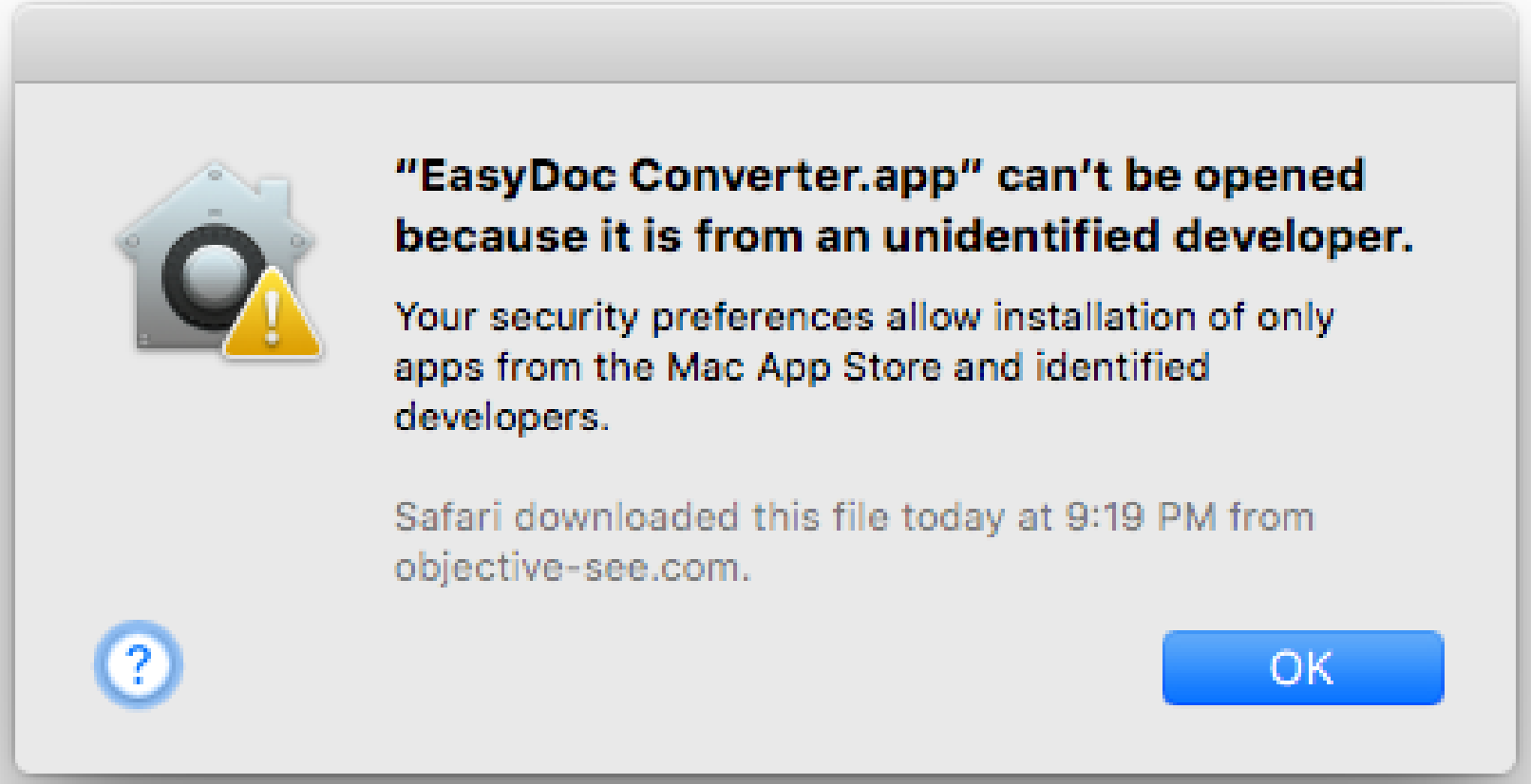
malware defenses (2)

app stores/etc. filtering (in theory)

- require developer registration
- blacklisting after the fact?

"sandboxing" policies

- don't let, e.g., game access your taxes


"EasyDoc Converter.app" can't be opened because it is from an unidentified developer.
Your security preferences allow installation of only apps from the Mac App Store and identified developers.
Safari downloaded this file today at 9:19 PM from objective-see.com.
OK

Allow Facebook to use your phone's storage?

This lets Facebook store and access information like photos on your phone and its SD card.

DENY ALLOW

malware defenses (3)

some email spam filters

blacklists for web browsers

- Google Safe Browsing list (Chrome, Firefox)
- Microsoft SmartScreen (IE, Edge)

malware counter-defenses

malware authors tries to make it hard-to-detect

obfuscation:

- make code harder to read
- make code different each time
- blend in with normal files/applications/etc.

New York Times

NEW YORK, FRIDAY, NOVEMBER 4, 1988

50 cents beyond 75 miles from New York City

'Virus' in Military Computers Disrupts Systems Nationwide

By JOHN MARKOFF

In an intrusion that raises questions about the vulnerability of the nation's computers, a Department of Defense network has been disrupted since Wednesday by a rapidly spreading "virus" program apparently introduced by a computer science student.

military officials, researchers and corporations.

While some sensitive military data are involved, the computers handling the nation's most sensitive secret information, like that on the control of nuclear weapons, are thought not to have been

"All the News That's Fit to Print"

The New York T

VOL.CXXXVIII . . . No. 47,680 NEW YORK, SATURDAY, NOVEMBER 5, 1988

Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security

Cornell Graduate Student Described as 'Brilliant'

By JOHN MARKOFF

The "virus" program that has plagued many of the nation's computer networks since Wednesday night was created by a computer science student who is the son of one of the Government's most respected computer security experts.

The program writer, Robert T. Morris Jr., a 23-year-old graduate student at Cornell University whom friends describe as "brilliant," devised the set of computer instructions as an experiment, three sources with detailed knowledge of the case have told The New York Times.

The program was intended to live innocently and undetected in the Arpanet, the Department of Defense computer network in which it was first introduced, and secretly and slowly make copies that would move from computer to computer. But a design error caused it instead to replicate madly out of control, ultimately jamming more than 6,000 computers nationwide in this country's most serious computer "virus" attack.

The dent's program jammed the computers of corporate research centers including the Rand Corporation and SRI International, universities like the University of California at Berkeley and the Massachusetts Institute of Technology as well as military research centers and bases all over the United States.

Meeting with the Authorities

The virus's creator could not be reached for comment yesterday. The sources said the student flew to Washington yesterday and is planning to hire a lawyer and meet with officials of the Defense Communications Agency, in charge of the Arpanet network.

Friends of the student said he did not intend to cause damage. They said he

'VIRUS' ELIMINATED, DEFENSE AIDES SAY

POLAND IS BUYING 3 BOEING AIRLINERS FOR $220 MILLION

EAST BLOC ORDER A FIRST

Sale to Be Financed Through a Lease-Purchase Accord With Western Banks

By AGIS SALPUKAS

The Boeing Company received an order yesterday from the national airline of Poland, the first order for advanced American aircraft from an Eastern bloc country.

The order from the LOT airline is for three 767 wide-bodied aircraft and is worth about $220 million. The transacton is to be financed through a lease-purchase agreement with Western banks, under which the airline will own the planes after 12 years.

Airline officials, at a news conference at the Polish Consulate in New York yesterday, would not identify the

MOSCOW OF ITS A CHARGE

U.S. Expresses Disappointment

President Reagan said yesterday that he was disappointed by the Soviet Union's decision to suspend the withdrawal from Afghanistan. The State Department said the suspension was disturbing.

Marlin Fitzwater, the White House spokesman, said the Soviets' actions "can only increase tensions in the region and raise speculation that they aren't going to live up to the Geneva accords."

But Administration officials nevertheless drew attention to Moscow's statement that the Soviet Union still intends to adhere to the accords, which call for the troop withdrawal to be

Morris worm mechanisms

used vulnerabilities in some versions of:

- mail servers (`sendmail`)
- user information servers (`fingerd`)

also spread using `rsh`/`rexec` (predecessor to ssh)

hid by being called `sh` (default shell)

strings obscured slightly in binary

the early Internet

pretty homogeneous — almost all Unix-like systems

`sendmail` was "the" email server to run

most institutions vulnerable

Morris worm intent versus effect

code in viruses tried to avoid “reinfecting” machines

... but not actually effective

Stuxnet

targeted Iranian nuclear enrichment facilities

physically damaged centrifuges

designed to spread via USB sticks

publicly known 2010, deployed 2009

US + Israel gov't developed

according to press reports

Ransomware

encrypt files, hold for “ransom”

decryption key stored only on attacker-controlled server

possibly decrypt files if victim pays

many millions in revenues

- accurate numbers are hard to find

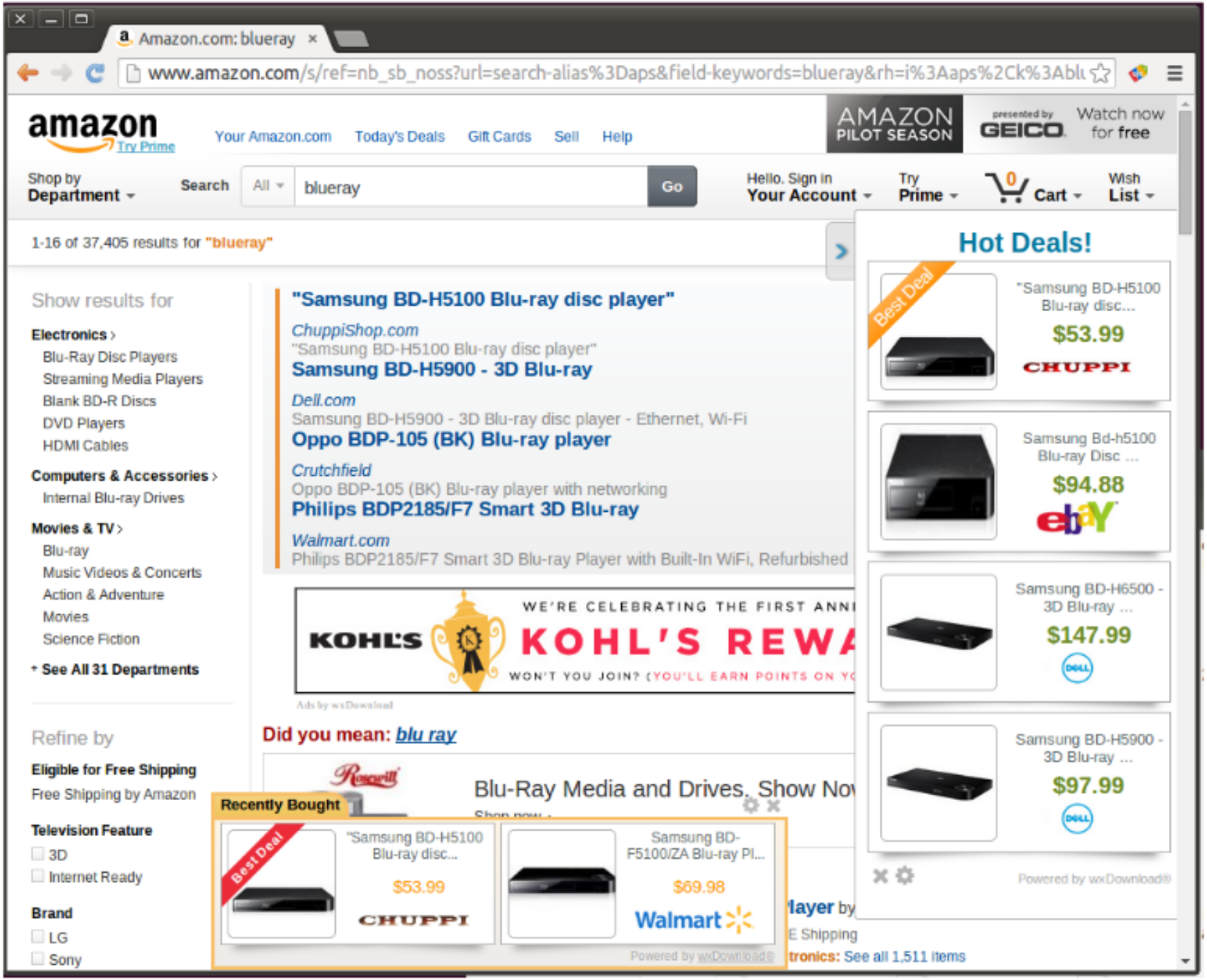
ad injection (1)

internet advertising is big business

... but you need to pay websites to add ads?

how about modifying browser to add/change ads

mostly bundled with legitimate software



From Thomas et al, "Ad Injection at Scale: Assessing Deceptive Advertisement Modifications"

ad injection (2)

5% of Google-accessing clients (2014)

>90% using code from VC-backed firm SuperFish:

$19.3 M in investment (CrunchBase)

$38M in revenue (Forbes, 2015)

defunct after Lenovo root CA incident (2015)

... but founders reported started new, similar venture (JustVisual; according to TechCrunch)

Adware prevalence: Thomas et al, "Ad Injection at Scale: Assessing Deceptive Advertisement Modifications"

stealing banking credentials

Products	Number	Proportion (%)	Price ($)
CVVs	465	47.1	10.08
Classic	*98*	*9.9*	*9.93*
Gold	*14*	*1.4*	*16.86*
Amex	*66*	*6.7*	*12.34*
others	*16*	*1.6*	*13.00*
unspecified	*271*	*27.5*	*9.06*
Dumps	234	23.7	34.52
Fullz	140	14.2	31.82
PayPal	133	13.5	3.01
WU ($100)	15	1.5	15.00
Total	987	100.0	

Table 3: Products and prices (mean) in total.

rom Haslebacher et al, "All Your Cards Are Belong To Us: Understanding Online Carding Forms", arXiv preprint 1607.0017v1

web-camera blackmail

ORANGE COUNTY
REGISTER

« Return to Article Click to Print

Man gets 18 months for 'sextortion' of Miss Teen USA, others

BY ERIC HARTLEY
2014-03-17 12:32:05

SANTA ANA – A man who hacked the computers of women including Miss Teen USA, then secretly took nude photos of them and extorted some into undressing during video chats, was sentenced Monday to 18 months in federal prison.

Jared James Abrahams, 20, of Temecula pleaded guilty in November to unauthorized computer access and extortion.

Before being sentenced, he read a statement in court apologizing for the pain he'd caused, but said he did not set out to hurt anyone or be "mean."

Abrahams' parents and lawyer said he is autistic and has serious difficulties making friends or having normal social interactions. His parents said examinations have found he has the emotional maturity of a 12-year-old.

flooding websites

distributed denial of service

example: October 2016 against DNS provider Dyn

- used by Twitter, GitHub, Amazon, ..., ...

monetized DDoS

Suspected members of Bitcoin extortion group DD4BC arrested

Two suspected members of the DDoS group have been arrested and detained.

By Charlie Osborne for Zero Day | January 13, 2016 -- 11:25 GMT (03:25 PST) | Topic: Security

other motivations

"cloud" of hijacked machines for computation

pride, vengeance (website defacement, etc.)

...

why talk about why/what?

doesn't change malware much

(also, not a likely topic later in this course)

...but, attacking monetization is a real strategy

attacker's willingness to spend?

Website

linked off Collab

`https://www.cs.virginia.edu/~cr4bd/4630/S2017/`

will include slides, assignments, lecture recordings

lectures and attendance

I recommend coming to lecture

I will not be taking attendance (except exams)

Lectures will be recorded

Prerequisites

technically CS 2150

CS 3330 will be very helpful

things from 3330 we care about

more review of x86 assembly

exceptions and virtual memory

(but probably not in much detail)

Exams/Assignments

many approx. one week assignments

two midterms — schedule on website

one final

can't make it? need accommodations? tell us ASAP!

Textbook

no required textbook

optional materials:

Szor, *The Art of Computer Virus Research and Defense*

I can recommend more general books, too

TAs/Office Hours

TAs posted on website

my office hours posted on website

TA office hours will be posted

Piazza, etc.

Piazza — linked of Collab

TAs and I should be monitoring

anonymous feedback on Collab

(almost) always appreciated

Misc. Policies

possibly exceptional circumstances? ask!

there is a late policy

assignments are individual

don't cheat

don't know if it's cheating? ask!

On Ethics

don't use someone's computer without their permission

- or in excess of what they've permitted

don't assume it's just a harmless prank

- unintended (but likely) consequences

don't assume the system owner would give you permission

- if you're afraid to ask, it's not okay

On Law

probably illegal (Federal and/or State crime):

accessing computers without authorization

even if nothing is done with the access

deliberately overloading a service

“backhacking” into a malware operator’s machine

deploying a worm that patches security holes

ethics pledge — please read and sign

on website, or I have copies

questions about ethics?

VM

homework assignments

first assignment — get an appropriate VM working

VM environment

64-bit Ubuntu 16.04 LTS

some assignments will require exactly this

(not some other Linux, not 32-bit)

VM problems?

tiny possibility your machine **can't** run 64-bit VM

(**no** CPU support — not "it's hard to setup")

we can find alternative solutions for you

talk to us!

related assignment

due 27 Jan (week from Friday) at 5PM

assignment on website

submission on Collab

next time: on VMs

virtual machines — what, why, how

virtual machines and malware

topics outline

prerequisite: assembly review

malware history

cat-and-mouse: anti-malware

software vulnerabilities

- memory management related

bonus topics:

- "safe" languages
- web browser security

Conclusion

malware: "evil" software

- originally — thrill? proof of concept?
- commonly — monetary motives

vulnerabilities:

- exploitable unintended program behavior