

CS 4630
logistics / terminology

lectures

via Zoom

recorded, attendance not required

some questions during lecture, using Zoom's poll feature
not graded

prerequisites

CS 3710 — I understand there's some variation...

knowledge of C, C++, assembly

CS 2150 should be enough, but refresher

CS 3330 or similar might be better

homework assignments

many approx. one week assignments

mostly due Friday at 11:59pm ET – but see calendar

some reverse-engineering oriented

several demonstrating an exploit

weekly quizzes

weekly written quizzes

released after Wednesday lecture

due before Monday lecture

textbook

no required textbook

some lecture material based on textbook stuff

Peter Szor, “The Art of Computer Virus Research and Defense”
(and may use other security textbooks)

office hours

posted on calendar on website

will be via Discord

using office hour queue

sorts mainly by last-time-helped

(w/ first-in, first-out queue for approx. 3 students)

Discord invite posted on Collab

I will be splitting my office hour time between OS and this course
(so if it's not obvious why I'm not getting to you that fast...)

piazza, etc.

linked on Collab

TAs and I should be monitoring

use private questions if assignment code, etc. involved

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

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:   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?



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

Mailings

Clipboard

Font

Times New Roman 12

B *I* U abc x₂ x²

ab A Aa A⁺ A₊

Paragraph



Security Warning

Macros have been disabled.

Options...

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 commercial 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

most commonly: programs bundled with other programs

sometimes disclosed but in (deceptive?) fine print

sometimes considered malware, sometimes not

bad behavior by 'normal' programs

some mostly-legitimate programs also do malware-like things

location info collected by cell phone apps?

advertisements injected by useful browser extensions?

Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

By JENNIFER VALENTINO-DeVRIES, NATASHA SINGER, MICHAEL H. KELLER and AARON KROLIK DEC. 10, 2018

The millions of dots on the map trace highways, side streets and bike trails — each one following the path of an anonymous cellphone user.

One path tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour. Another represents a person who travels with the mayor of New York during the day and returns to Long Island at night.

what is malware...

opinion question:

if you're making anti-malware software, what should it do for...?

- (1) pre-installed browser extension that displays coupon codes but sends domain name of all websites to third-party to do so
- (2) remote administration software that shows a subtle icon in the corner of the screen when used to monitor the machine

- A. remove it, no prompting
- B. prompt to remove it, default to yes
- C. prompt to remove it, default to no
- D. don't flag it
- E. something else (discuss?)

The Spyware Used in Intimate Partner Violence

Rahul Chatterjee*, Periwinkle Doerfler[†], Hadas Orgad[‡], Sam Havron[§], Jackeline Palmer[¶], Diana Freed*, Karen Levy[§], Nicola Dell*, Damon McCoy[†], Thomas Ristenpart*

* Cornell Tech

[†] New York University

[‡] Technion

[§] Cornell University

[¶] Hunter College

	App types	Description	Examples	Capabilities
Personal tracking	Find-my-phone	Locate phone remotely	Find my Android	Location tracking, remote locking and wiping
	Anti-theft	Catch the phone thief	Wheres My Droid	Record location, photos & ambient audio; alert on SIM change
	Call recorder	Record incoming / outgoing calls	Call Recorder	Record calls and back them up to a server
	Data syncing	Sync data from phone to other device	mySMS	Sync SMS and call log, media, browser history
	Phone control	Control phone remotely	TrackView	Full control with capabilities exceeding combination of data syncing and anti-theft
Mutual tracking	Family tracking	Track location of family members	Family Tracker	Mutual location sharing
	Couple tracking	Consensual sharing of location and more	Couple Tracker	Syncs location, media content, SMS and call logs
	Friends tracking	Track friends if they are in vicinity	Friends Tracker	Like family tracker, and alerts if friend in vicinity
Subordinate tracking	Employee tracking	Track employees whereabouts	Where's my Staff	Similar to anti-theft
	Parental control	For parents to monitor their children	MMGuardian	Capabilities very similar to phone control
	Overt spyware	Claims to be spying app	Cerberus, mSpy, HelloSpy	Surreptitious phone monitoring & control

Fig. 5: Different categories of IPS-relevant apps and their typical capabilities.

dual-use, context-sensitivity

this class: mostly talking about clearly anti-user software
...and how it tries to be covert

but there are also problems of *dual-use* software
phone tracking anti-theft software
computer remote administration software

(also problems of intentionally 'evil' software masquarding as legit)
(e.g. marketted on "how to spy on your _____" blog)
(e.g. unnecessairily well hidden when installed)

ideally, prevent "bad" use somehow
phone OS should prevent *covert* tracking?
antimalware software should notice such software?

...

making money from malware

often malware authors trying to make money

adware — from ad revenue

ransomware — ransom user's files/usability of system

resell personal info

resell computation/network time

- advertising fraud

- distributed denial of service

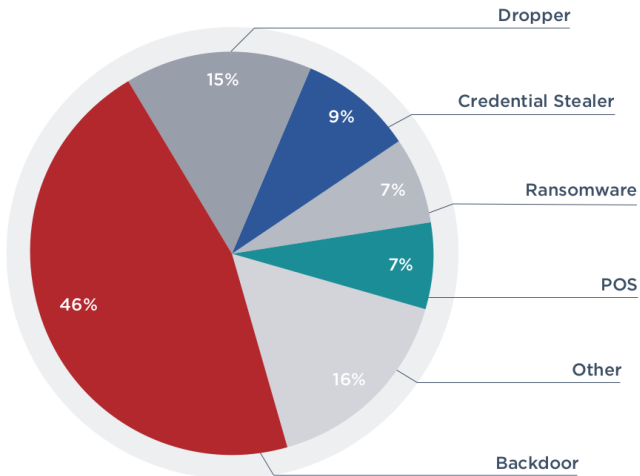
- cryptocurrency mining

aside on malware statistics

most malware statistics come from antivirus companies

probably a biased data source

Category Mandiant analysts assign categories to malware samples based on their classification and behavior (Fig. 5). Each binary is placed into only one category. While a backdoor might have the ability to steal credentials, if the primary purpose of the malware was to function as a backdoor it would be counted as a backdoor. Inversely, something will only be labeled as a credential stealer only if it's primary function is to steal credentials.



Measuring *Pay-per-Install*: The Commoditization of Malware Distribution

Juan Caballero[†], Chris Grier^{‡}, Christian Kreibich^{*‡}, Vern Paxson^{*‡}*

[†]IMDEA Software Institute ^{}UC Berkeley [‡]ICSI*

juan.caballero@imdea.org {grier, vern}@cs.berkeley.edu christian@icir.org

FAMILY	MILKED	DIST.	DAYS	CLASS	PPI
<i>Rustock</i>	61,017	15	31	spam	L
<i>LoaderAdv-ack</i>	60,770	62	31	ppi	L
<i>CLUSTER: A</i>	11,758	8	31	clickfraud	G
<i>Hiloti</i>	10,045	43	31	ppi	L
<i>CLUSTER: B</i>	8,194	9	31	?	G
<i>Gleishug</i>	7,620	15	31	clickfraud	L
<i>Nuseek</i>	5,802	2	30	clickfraud	G
<i>Palevo2</i>	16,101	21	29	botnet	G,L
<i>Securitysuite</i>	15,403	100	29	fakeav	L
<i>Zbot</i>	3,684	49	29	infosteal	G,L
<i>CLUSTER: D</i>	5,723	1	28	?	G
<i>SmartAdsSol.</i>	18,317	6	26	adware	L
<i>Spyeye</i>	4,522	16	25	infosteal	G,L
<i>Securitysuite-avm</i>	4,732	45	20	fakeav	L
<i>Grum</i>	2,974	54	20	spam	G,L
<i>Tdss</i>	4,893	12	19	ppi	G,L
<i>Otlard</i>	677	7	16	botnet	G,L
<i>Blackenergy1</i>	1,135	15	15	ddos	L
<i>Palevo</i>	2,594	2	14	botnet	G
<i>Harebot</i>	1,617	13	14	botnet	G,L,V

Table 3: Top 20 malware families we milked during August 2010. The columns indicate the total number of executables milked, distinct executables per family, the number of days seen, the families’ general class, and PPI services that distribute the family: *LoaderAdv* (L), *GoldInstall* (G), *Virut* (V).

making money from malware

often malware authors trying to make money

adware — from ad revenue

ransomware — ransom user's files/usability of system

resell personal info

resell computation/network time

- advertising fraud

- distributed denial of service

- cryptocurrency mining

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

Amazon.com: blu-ray

www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&field-keywords=blu-ray&rh=i%3Aaps%2Ck%3Ablu

amazon **Try Prime** Your Amazon.com Today's Deals Gift Cards Sell Help

AMAZON PILOT SEASON presented by GEICO Watch now for free

Shop by Department Search All blu-ray Go Hello, Sign in Your Account Try Prime Cart Wish List

1-16 of 37,405 results for "blu-ray"

Show results for

Electronics >
 Blu-Ray Disc Players
 Streaming Media Players
 Blank BD-R Discs
 DVD Players
 HDMI Cables

Computers & Accessories >
 Internal Blu-ray Drives

Movies & TV >
 Blu-ray
 Music Videos & Concerts
 Action & Adventure
 Movies
 Science Fiction

• See All 31 Departments

Refine by

Eligible for Free Shipping
 Free Shipping by Amazon

Television Feature
 3D
 Internet Ready

Brand
 LG
 Sony

"Samsung BD-H5100 Blu-ray disc player"
 ChuppiShop.com
 "Samsung BD-H5100 Blu-ray disc player"
Samsung BD-H5900 - 3D Blu-ray
 Dell.com
 Samsung BD-H5900 - 3D Blu-ray disc player - Ethernet, Wi-Fi
Oppo BDP-105 (BK) Blu-ray player
 Crutchfield
 Oppo BDP-105 (BK) Blu-ray player with networking
Philips BDP2185/F7 Smart 3D Blu-ray
 Walmart.com
 Philips BDP2185/F7 Smart 3D Blu-ray Player with Built-In WiFi, Refurbished

Hot Deals!

Best Deal "Samsung BD-H5100 Blu-ray disc..." **\$53.99** **CHUPPI**

Samsung Bd-h5100 Blu-ray Disc ... **\$94.88** **eBay**

Samsung BD-H6500 - 3D Blu-ray ... **\$147.99** **DELL**

Samsung BD-H5900 - 3D Blu-ray ... **\$97.99** **DELL**

KOHL'S WE'RE CELEBRATING THE FIRST ANNI **KOHL'S REWA** WON'T YOU JOIN? (YOU'LL EARN POINTS ON YC

Ads by wsDownload

Did you mean: [blu ray](#)

Recently Bought

Best Deal "Samsung BD-H5100 Blu-ray disc..." **\$53.99** **CHUPPI**

Samsung BD-F5100/ZA Blu-ray PL... **\$69.98** **Walmart**

layer by E Shipping tronics: See all 1.511 items

Powered by wsDownload

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)

Google removes two Chrome ad blockers caught collecting user data

Nano Adblocker and Nano Defender have been removed from the official Chrome Web Store.



By [Catalin Cimpanu](#) for [Zero Day](#) | October 20, 2020 -- 13:45 GMT
(06:45 PDT) | Topic: [Security](#)

The data collection code was added at the start of this month, in October 2020, after the original author [sold the two extensions](#) to "a team of Turkish developers."

making money from malware

often malware authors trying to make money

adware — from ad revenue

ransomware — ransom user's files/usability of system

resell personal info

resell computation/network time

- advertising fraud

- distributed denial of service

- cryptocurrency mining

cryptolockers

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

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:   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?



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

other ransomware

we have your private data, pay us or it gets released

more targetted stealing/extortion

To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild

Brown Farinholt[†], Mohammad Rezaeirad[‡], Paul Pearce[§], Hitesh Dharmdasani[¶], Haikuo Yin[†]
Stevens Le Blond^{||}, Damon McCoy^{††}, Kirill Levchenko[†]

Abstract—Remote Access Trojans (RATs) give remote attackers interactive control over a compromised machine. Unlike large-scale malware such as botnets, a RAT is controlled individually by a human operator interacting with the compromised machine remotely. The versatility of RATs makes them attractive to actors of all levels of sophistication: they’ve been used for espionage, information theft, voyeurism and extortion. Despite their increasing use, there are still major gaps in our understanding of RATs and their operators, including motives, intentions, procedures, and weak points where defenses might be most effective.

to catch ratter results

2016/7 study

61% attempt to access webcam; 26% microphone
(both not present in experimenter's 'honeypot')

31% enable keylogger (passwords?)

approx. 5% harass legit user

approx. 2% try to phish legit user

the underground economy (1)

<A> Sell Cvv US(1\$ each),Uk(2\$ each)Cvv with SSN & DL(10\$ each)and ePassporte Account with 560\$ in acc(50\$),Hacked Host(7\$),Tut Scam CC Full in VP-ASP Shop(10\$).shopadmin with 4100 order(200\$), Tool Calculate Drive Licsence Number(10\$).... I'm sleeping. MSG me and I will reply U as soon as I can !

advertisement for stolen credentials on an IRC (Internet Relay Chat) server via Team Cymru, "The underground Economy: Priceless" (2006, Usenix ;login: magazine)

(CVV = card verification value — verification number on back of credit cards)(DL = driver's lic

the underground economy (2)

<A> i have wells and boa logins and i need to good drop manripper
f#@! off

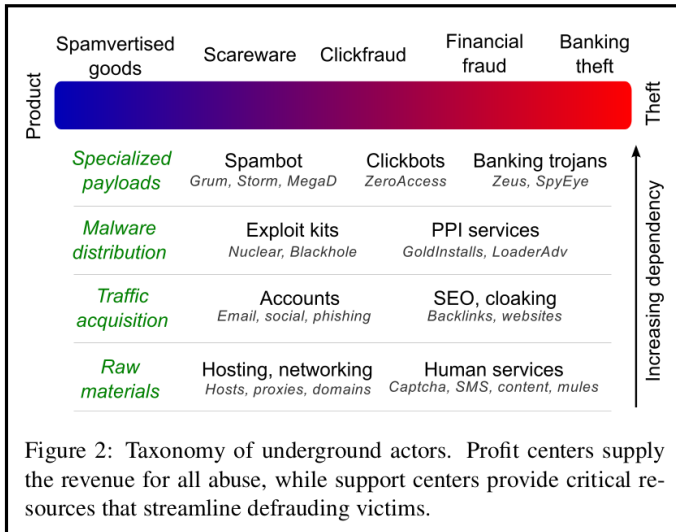
 <=== .Have All Bank Infos. US/Canada/ Uk ...Legit Cashiers Only
Msg/me

<C> HELLO room... I am Ashley from the State... I got drops for US banks
and i need a very trust worthy and understanding man to do deal with ...
the share its 60/40...Msg me for deal

advertisements for 'drops' (bank accounts for money laundering) and
for 'cashiers' (criminals who will clean out accounts)

via Team Cymru, "The underground Economy: Priceless" (2006, Usenix ;login: magazine)

the underground economy (3)



via Thomas et al, "Framing Dependencies Introduced by Underground Commoditization" (2015)

targeted attacks / espionage

information gathering

SolarWinds (network monitoring software) attack (“supply chain”)
exploits via subject-specific links (“here’s an interesting PDF”)

sabotage

Stuxnet: Iranian enrichment controls

SolarWinds

supplier of network-monitoring software

...used by many big customers, including US Gov't

attacked by third-party to spy (?) on customers

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

why talk about why/what?

doesn't change malware much

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

...but, attacking monetization is an effective strategy

vulnerabilities

for viruses, worms

for trojans + PUP that do more than is supposed to do be allowed
e.g. getting location information without “permission”

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 spreading with human help

installed by other malware

installed manually after illegitimate access

including in deceptively marketed software

malware spreading without human help

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

- program analysis?

- blacklisting after the fact?

“sandboxing” policies

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

- don't let weather app access your microphone



**"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.

VM

homework assignments

first assignment — get an appropriate VM working

VM environment

64-bit Ubuntu 20.04 LTS

I'll make an effort for assignments
to work in other 64-bit Linux envs

but this is what we'll test in

(and some assignments are very sensitive to environment details)

related assignment

assignment on website

submission on Collab

just get some suitable environment working

semester outline

assembly/reverse-engineering
including binary formats
hiding in innocent programs

heuristic malware detection cat-and-mouse game
signature-based detection
evading signature-based detection

memory-mismanagement exploits and mitigations


(less certain topics)

command-injection exploits and mitigations

timing attacks and mitigations

sandboxing

backup slides

 MUST READ: [Raspberry Pi 400: The inside story of how the \\$70 Pi-powered PC was made](#)

Some ransomware gangs are going after top execs to pressure companies into paying

Ransomware gangs are prioritizing stealing data from workstations used by executives in the hopes of finding and using valuable information to use in the extortion process.



By [Catalin Cimpanu](#) for [Zero Day](#) | January 9, 2021 -- 08:00 GMT (00:00 PST) | Topic: [Security](#)

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.

non-vulnerabilities?

with trojans/potentially unwanted software, problem is subtle

usually unintended consequence of designed-for level of access

e.g. browser extensions supposed to be able to add content to webpages

e.g. applications you install supposed to be able to change/delete files

not what we'll call a *vulnerability*

but still a security problem

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**

often 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

reselling others machines

botnets

making money from other people's computers/Internet connection

denial of service attacks

advertising fraud

sending spam

'mining' cryptocurrency

denial of service attacks

Attack Type	Attacks	Targets	Class
HTTP flood	2,736	1,035	A
UDP-PLAIN flood	2,542	1,278	V
UDP flood	2,440	1,479	V
ACK flood	2,173	875	S
SYN flood	1,935	764	S
GRE-IP flood	994	587	A
ACK-STOMP flood	830	359	S
VSE flood	809	550	A
DNS flood	417	173	A
GRE-ETH flood	318	210	A

Table 9: **C2 Attack Commands**—Mirai launched 15,194 attacks between September 27, 2016–February 28, 2017. These include [A]pplication-layer attacks, [V]olumetric attacks, and TCP [S]tate exhaustion, all of which are equally prevalent.

advertizing fraud

Measuring lower bounds of the financial abuse to online advertisers: A four year case study of the TDSS/TDL4 Botnet

Yizheng Chen ^a  , Panagiotis Kintis ^a , Manos Antonakakis ^b , Yacin Nadji ^b , David Dagon ^a , Michael Farrell ^c 

one of the most complex, sophisticated, and long-lived botnets: TDSS/TDL4. Using passive datasets from a large [Internet Service Provider](#) in the United States, we estimated conservative [lower bounds](#) of advertisers' loss caused by the botnet. Over its entire life span, less than 15% of TDSS/TDL4 population caused *at least \$346 million* in damages to advertisers, primarily due to impression fraud. This translates to an average of \$340 thousand daily loss to advertisers, which is three times the last reported estimate from the analysis of ZeroAccess botnet ([Pearce et al., 2014](#)) and more than ten times of the daily impact the DNSChanger botnet ([Meng et al., 2013](#)) had to the ad ecosystem. Our study is the first to reveal the extent of the abuse that botnets bring to the ad ecosystem from the outside: the edge of the Internet.