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

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

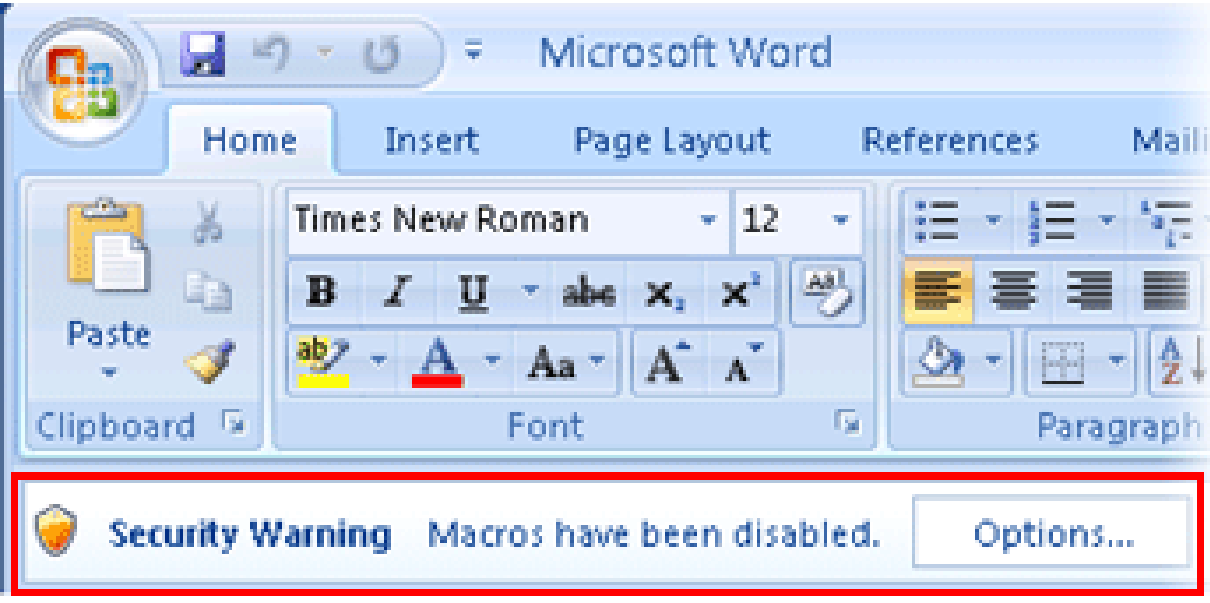
viruses written in a *scripting language*

- 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
Mail
Paste
Times New Roman
12
Clipboard
Font
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 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

Nearly 80 Chrome extensions caught spying -- how to protect yourself

By Nicholas Fearn June 18, 2020

79 malicious browser extensions booted by Google from the Chrome Web Store

Comments (2)

(Image credit: Shutterstock)

More than 100 malicious and fake Google Chrome browser extensions have amassed around 33 million downloads in total, according to an investigation by security firm Awake.

Security researchers discovered 111 malicious extensions that were downloaded by users of the Google Chrome browser and spread dangerous spyware.

potentially unwanted programs (PUP)

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?

advertisments 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.

2021 IEEE Symposium on Security and Privacy (SP)

How Did That Get In My Phone? Unwanted App Distribution on Android Devices

Platon Kotzias*, Juan Caballero†, Leyla Bilge*
*NortonLifelock Research Group, † IMDEA Software Institute

TABLE VII: Summary of app distribution.

	Installs		Installer					Children			
Vector	**All**	**Unw.**	**All**	**Unw.**	**Plat.**	**Pkg.**	**Sig.**	**Pkg.**	**Sig.**	**VDR**	**RVDR**
Playstore	87.2%	67.5%	10	3	0	2	9	1.2M	816K	0.6%	1.0
Alt-market	5.7%	10.4%	102	31	15	87	67	128K	77K	3.2%	5.3
Backup	2.0%	4.8%	49	2	24	31	39	528K	355K	0.9%	1.5
Pkginstaller	0.7%	10.5%	79	5	25	11	74	197K	127K	2.4%	4.0
Bloatware	0.4%	6.0%	54	2	28	37	41	2.1K	1.3K	1.2%	2.0
PPI	0.2%	0.1%	21	0	2	20	11	1.5K	1.3K	0.3%	0.5
Fileshare	<0.1%	<0.1%	13	3	4	13	11	8.8K	7.4K	1.3%	2.1
Themes	<0.1%	<0.1%	2	0	2	2	2	634	14	0.3%	0.5
Browser	<0.1%	<0.1%	47	4	3	40	38	4.8K	3.3K	3.8%	6.3
MDM	<0.1%	<0.1%	7	1	1	7	6	766	489	0.3%	0.5
Filemanager	<0.1%	<0.1%	58	11	9	32	43	6.6K	4.7K	2.6%	4.3
IM	<0.1%	<0.1%	13	2	0	10	11	2K	1.2K	2.9%	4.8
Other	<0.1%	0.3%	151	68	28	125	98	9.1K	5.3K	3.9%	6.5
Unclassified	3.7%	<0.1%	3.5K	2.4K	386	3.3K	814	91K	16K	<0.1%	0.1
All	100.0%	100.0%	4.2K	2.5K	79	3.6K	1.0K	1.6M	992K	1.6%	2.6

VDR=portion detected as unwanted; PPI=pay-per-install; MDM=mobile device management

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

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

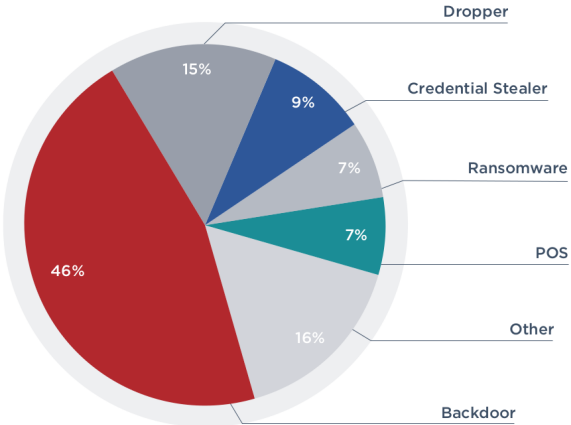
- advertising fraud
- distributed denial of service
- cryptocurrency minining

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.



Source: FireEye M-Trends Report 2020

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*

2011, Usenix Security

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

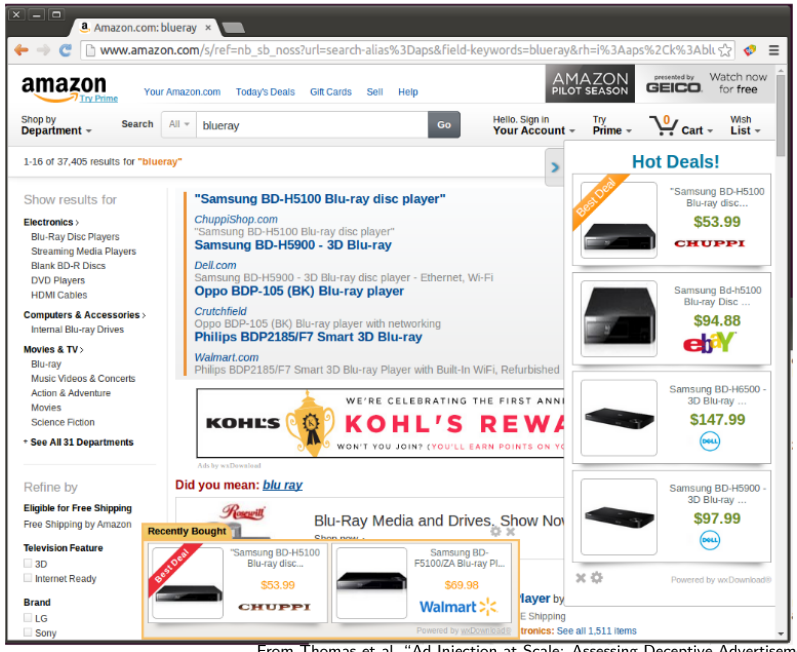
ad injection (1)

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"

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 minining

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: [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

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 !

advertisment 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 license?)

the underground economy (2)

<A> i have wells and boa logins and i need to good drop man .....ripper f#@! off
<B> <=== .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 econmomy (3)

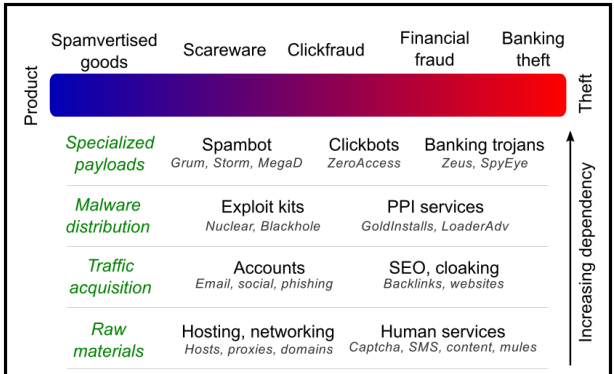


Figure 2: Taxonomy of underground actors. Profit centers supply the revenue for all abuse, while support centers provide critical resources that streamline defrauding victims.

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/other goals often effective...

may be more effective than our focus on exploits/code/etc.

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 “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 marketted 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

...

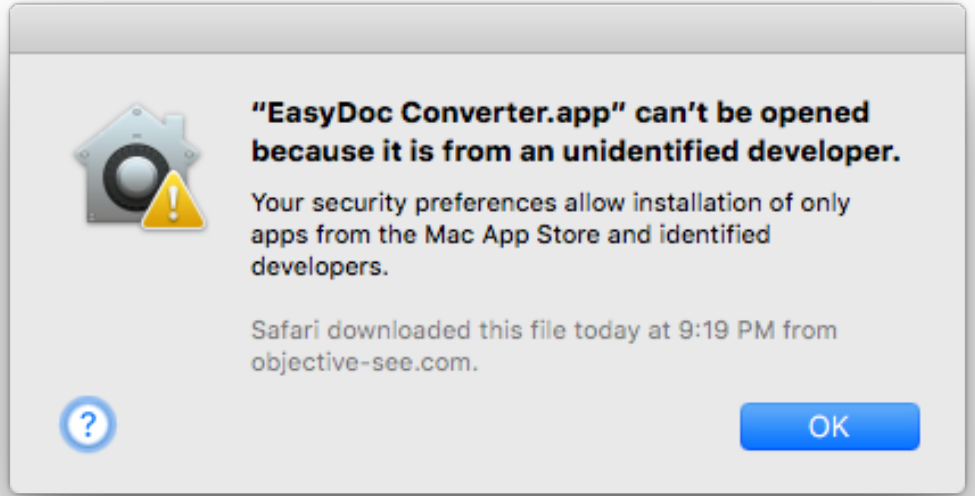
malware defenses (2)

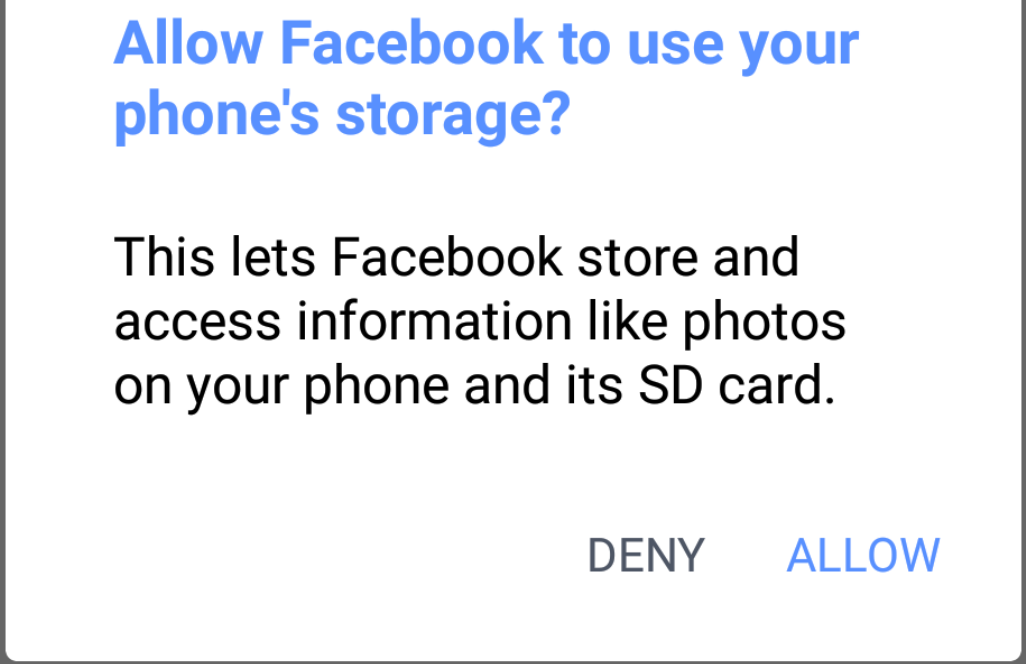
app stores/etc. filtering (in theory)

- 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.