CS 261: Cybercrime

Created	Mar 29, 2021 1:06 PM
Lecturer	Professor David Wagner
Discussion leader	Itai Smith
Scribe	Orr Paradise

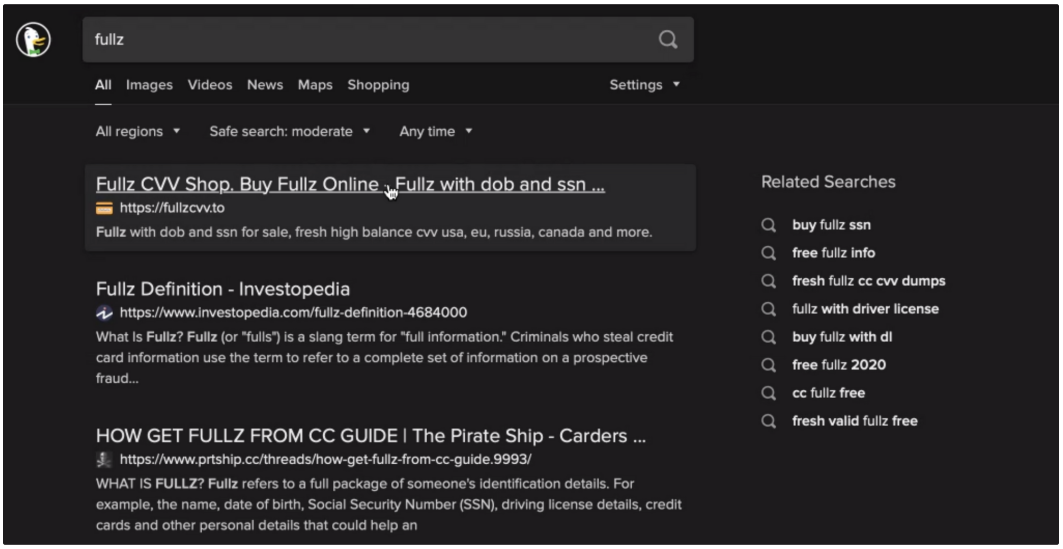
CS 261: Cybercrime

Background

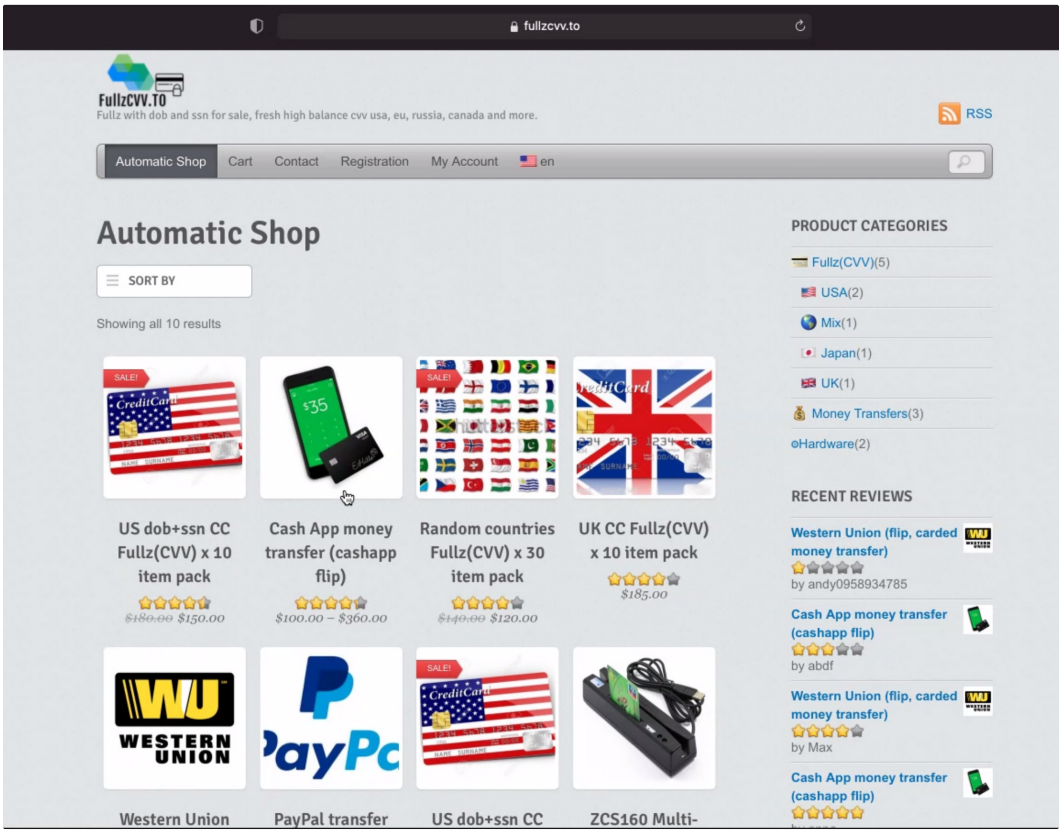
When Dave was a grad student, most attacks online were done for fun or mild vandalism (digital equivalent of graffiti). Somewhere in the early 2000s that changed That changed in the early 2000s, with an increase in attacks primarily driven by financial incentives.

Warm-up

A *full* (plural *fullz*) is a bundle that contains personal information about a person, such as their name, date of birth and credit card number. Let's see what happens when we search the web for *fullz.*



Let's look at the first website



Why can we find this sensitive information so easily? One possible answer is that the websites are advertising operation. The harder you are to be found, the less likely you are to get business.

We see one *full* sell Why are they so cheap?

- There is a risk of getting caught for buying or using a *full*.

- Credit card fraud detection. Is it easy to use a *full*? Is there really value in bulk?
- The card has already been blocked by the owner. For example if this seller has already sold these *fullz*.
- It may take a long time to get payoff.
- The miscreant may be able to buy the item, but how will they get it delivered? Certainly not by delivering to their own address...

Monetization

Suppose you can hack into machines. Let's discuss what we can do to maximize profit:

- Get access to banking website.
  - Caveat: banking transactions are reversible. Instead, use Western Union which pay out in cash.
- Install ransomware. Then you do not need to worry about getting the cash, since the victim takes care of that for you. Indeed, ransomware yields over one-hundred million dollars per year.
- Log in to Amazon and sending out physical goods.
- Sell your hacking abilities to less-technical criminals. ('Exploits as a service')
- Use the computational power itself, e.g. mine bitcoin.
- If you have a lot of power, you could short a company and then disrupt their infrastructure. You could also simply extort the company.
- Uncover personal secrets of someone and extorting them.
- Use the fame or credibility of large influencers. For example, hack into Elon Musk's twitter and announce you will buy stock of some company.
- Change all ads in every website to a provider that pays you.
- Click-fraud: have many computers click on ads on your website.

- Run a racket: write good viruses, and good anti-viruses to protect against them. More extremely, scareware: pop-ups warnings against hundreds of viruses, pay us to remove them! But there were never any viruses at all...
- Send spam email using the victim's email.

Specialization

As a criminal, you don't have to be an expert in all steps of the value-chain. Some examples:

- *Money transfer scam*. After gaining access to someone's bank account, a different criminal agent hires an unsuspecting person Patsy to be the financial agent for their fraudulent company. Patsy is told that they will be sent $8,000, of which they may keep $500 and send the remaining $7,500 to some (hacker-owned) account. Then, when the bank reverses the fraudulent $8,000 transaction from the victim's account to Patsy's, Patsy will be left $7,500 short.
    - The criminal 'operating' Patsy is a laundering specialist.
- *Drops*. Some criminals specialize in obtaining goods via shipping.
- *Voice actors* specialize in fooling banks' vocal identificaiton methods.

Opportunities for defenders

What opportunities are there for defenders to prevent cybercrime? We'll consider this question with respect to *monetization* and the *underground market*.

- Monetization: instead of making it harder to hack into people's computers, law enforcement agents can make it harder to convert a hacked machine into money.
    - Where should they intervene? Consider the following figure (Levchenko *et al.*, 2011)

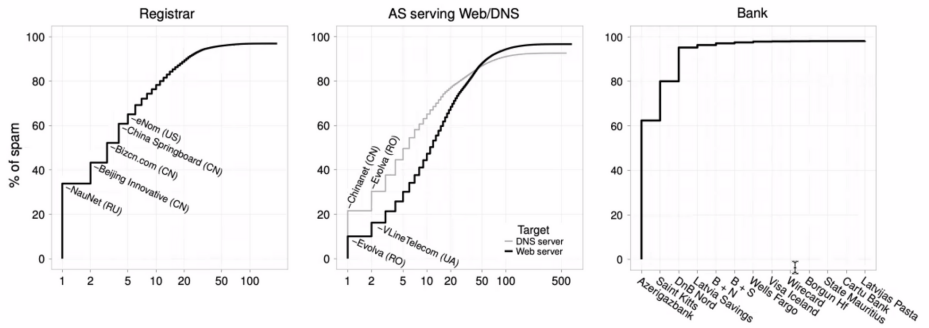


Figure 5: Takedown effectiveness when considering domain registrars (left), DNS and Web hosters (center) and acquiring banks (right).

Securing three banks covers 90% of spam. To get similar coverage via DNS, ~50 services would need to be secured.

- Underground market: You'd think the criminals all exist on the dark web, but if you are too obscure then your customers can't find you.
    - Shadowcrew (2002-2004) was the prime forum for illegal activity online. The Secret Service 'turned' one of the admins of this forums. They then:
        1. Migrated the forum to servers run by the Secret Service, and got users to use Secret Service-run VPN.
        2. Gradually arrested all other admins.
        3. Did nothing for about a year, just to analyze the network.
        4. One day, they made over 100 arrests.

        This had a noticeable (yet temporary) impact on cybercrime.

Ethics

Where do we draw the line between ethical or unethical? Let's discuss some proposals:

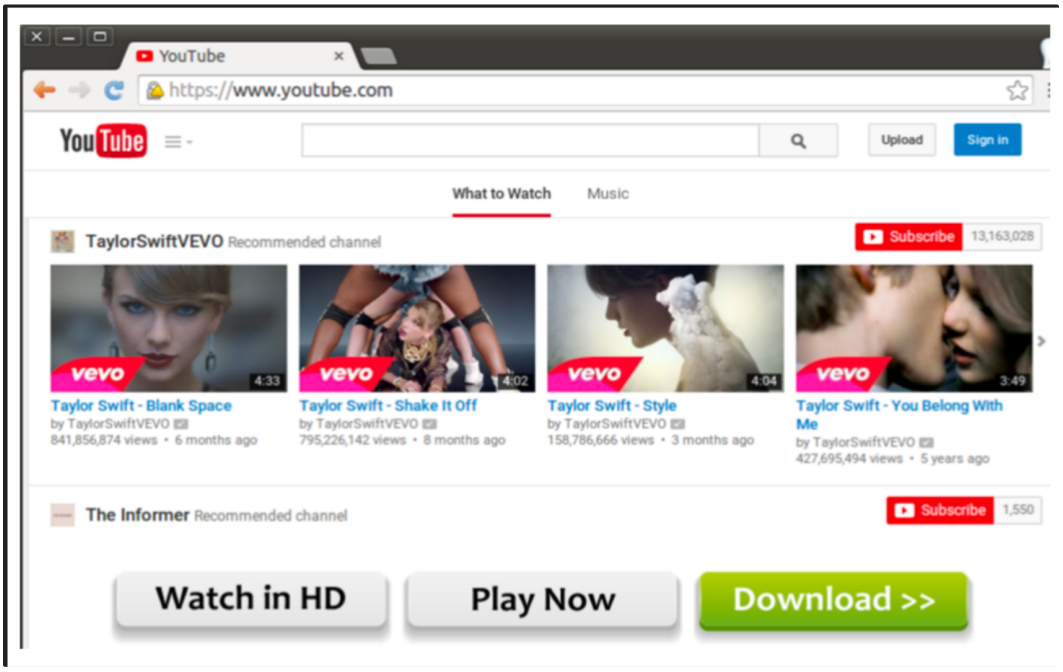
- Don't actively cause anyone any harm.

- If you observe harm, stop it or report it. Don't passively observe it without doing nothing.
    - What if you're only scratching the surface of the problem? By acting to soon you might miss the opportunity to make an impactful intervention.
    - Is it clear what counts as harmful?
- Don't stop illegal activity by doing your own illegal activity.
- It's easy or tempting to say that "it might be contributing to the market a bit, we're really not going to make a big difference". But that doesn't sound quite right.
- General point: what is the role of the researcher? Are they more like an agent of the state? A journalist?

Discussion: Unwanted Software

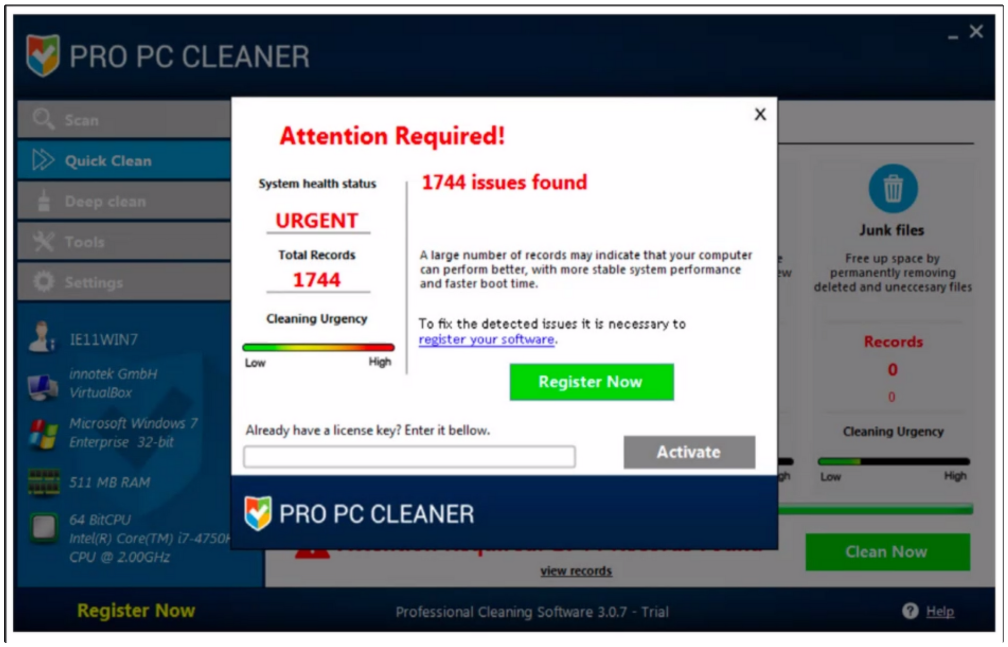
Unwanted software is software that is not malicious *per se*, but often modifies the user's experience on their browser or operating system in a way they did not intent. It often leads to revenue for the developer.

- Ad-injectors: Inject ads to websites.

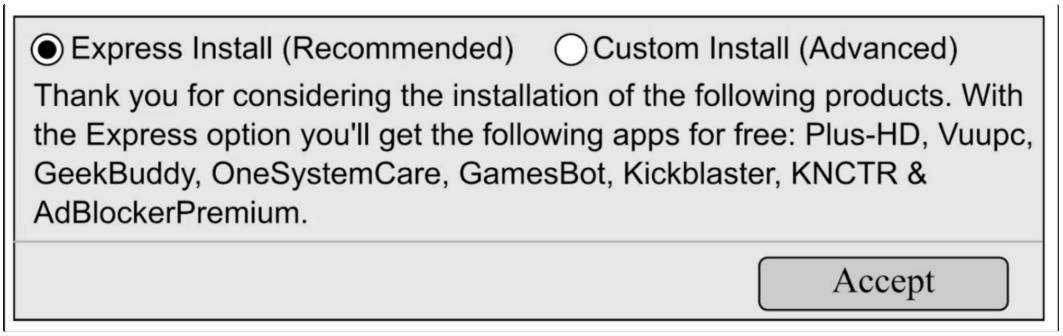


- Browser-setting hijackers: e.g. modify the user's homepage.

- System utilities: software that presents nebulous claims about users computer. Similar to fake anti-virus, however they do sometimes do *something*, e.g. deleting meaningless registry values.



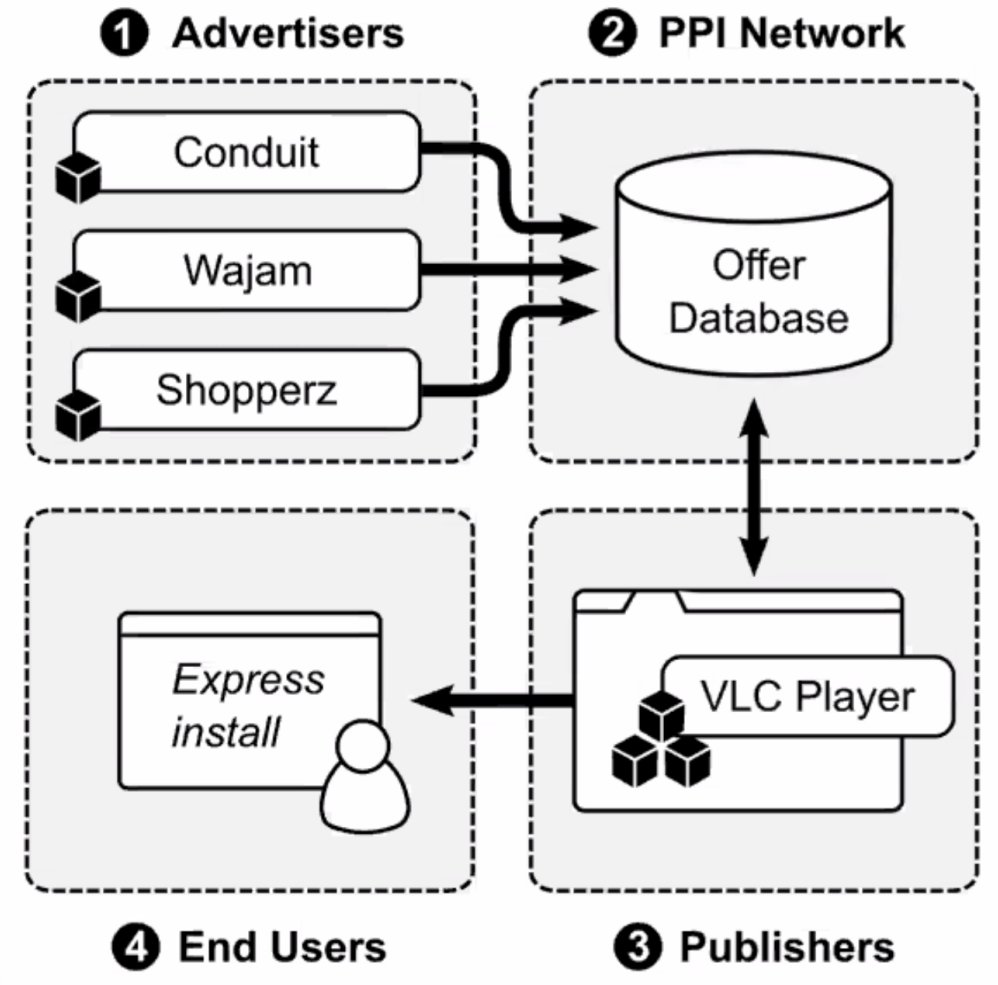
Typically, a user is enticed or social-engineered to install something. That installation is bundled with the unwanted software. These are called pay-per-install (PPI) software, because developers pay the bundler for each installation of their unwanted software.



In Thomas *et al.* (2016) authors downloaded PPI software into sandboxed environments and analyzed them for a year. They identified three main PPI players.

1. Advertisers
2. Publishers

3. PPI affiliate networks



The authors found that unwanted software installation is much more common than malware.