Tools and Techniques used in Automated Threats

Shain Singh | Cloud Security Lead

Ben Francis | Automated Fraud Specialist

Our Speakers

Shain Singh

F5

Cloud/5G Security Architect

@shainsingh

Ben Francis

Shape Security – part of F5

Automated Fraud Specialist

Agenda

THE BASICS

- What is an automated threat?
- Elements of a threat profile

TOOLS AND TECHNIQUES

- Common toolsets
- Uncommon toolsets
- Generating entropy
- Motivation

COMMON MITIGATION METHODS

- Rate limits
- Signatures
- IP Address blocking
- CAPTCHA
- MFA

WHERE TO NEXT?

- Using OWASP Automated Threats
- Who cares about Automated Threats?

ATTACK ANALYSIS

- Aggregators

ATTACK ANALYSIS

- Gift Card Fraud

ATTACK ANALYSIS

- MFA Bypass

The Basics

What is an Automated Threat?

Abuse inherent functionality to conduct automated and manual fraud

Attackers abuse functionality ***as designed*** but not ***as intended***

Reading is good but…

The Automated Threat Handbook

Web Applications

The Automated Threat Handbook provides actionable information and resources to help defend against automated threats to web applications.

OAT-020 Account Aggregation
OAT-019 Account Creation
OAT-003 Ad Fraud
OAT-009 CAPTCHA Defeat
OAT-010 Card Cracking
OAT-001 Carding
OAT-012 Cashing Out
OAT-007 Credential Cracking
OAT-008 Credential Stuffing
OAT-021 Denial of Inventory
OAT-015 Denial of Service
OAT-006 Expediting
OAT-004 Fingerprinting
OAT-018 Footprinting
OAT-005 Scalping
OAT-011 Scraping
OAT-016 Skewing
OAT-013 Sniping
OAT-017 Spamming
OAT-002 Token Cracking
OAT-014 Vulnerability Scanning

Let’s start with an example

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Search OWASP.org

Donate Join

Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

Example vulnerability

Your Information

Member Email Address

Confirm Member Email Address

Company Name

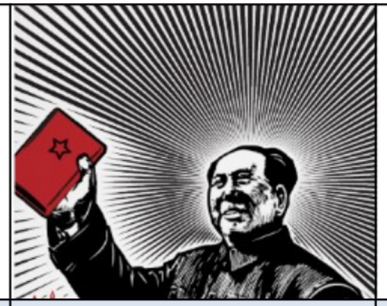
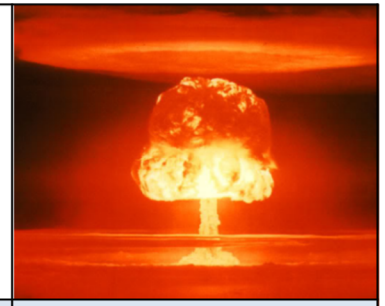
Member Name

SUBMIT

By submitting this form, you are consenting to receive communications from the OWASP Foundation concerning the status of your membership and agree to adhere to the OWASP Foundation Code of Conduct. Membership Dues are not prorated nor can they be cancelled once purchased. Discounted and Student Memberships are only offered to qualifying individuals. Fraudulent membership submissions will be revoked without notice for no refund. You can elect to receive marketing mails from us by also selecting "Join the OWASP Marketing Mail List." Marketing mails include information and special offers for upcoming conferences, meetings, and other opportunities offered to you. You can revoke your consent to receive Marketing Mail List emails at any time by using the Unsubscribe link found at the bottom of these emails.

data entry can be automated by script or webdriver recording

Examples of a Threat Profile

				
Assets	**Actors**	**Motives**	**Resources**	**Outcomes**
Items of value that we wish to protect.	Whom or what may be a threat.	Underlying objective or behavior causing the actor to become a threat.	Talent, budget, advantages, and access that may be available to the actors to bolster attack efforts.	Specific result to prevent.

Motivation

Ran “pirate subscription” sites

HyperGen, WickedGen, Autoflix & AccountBot

" *… $10 for a lifetime subscription*"

" *… more than 150,000 users*"

Evan Leslie McMahon

23 years old

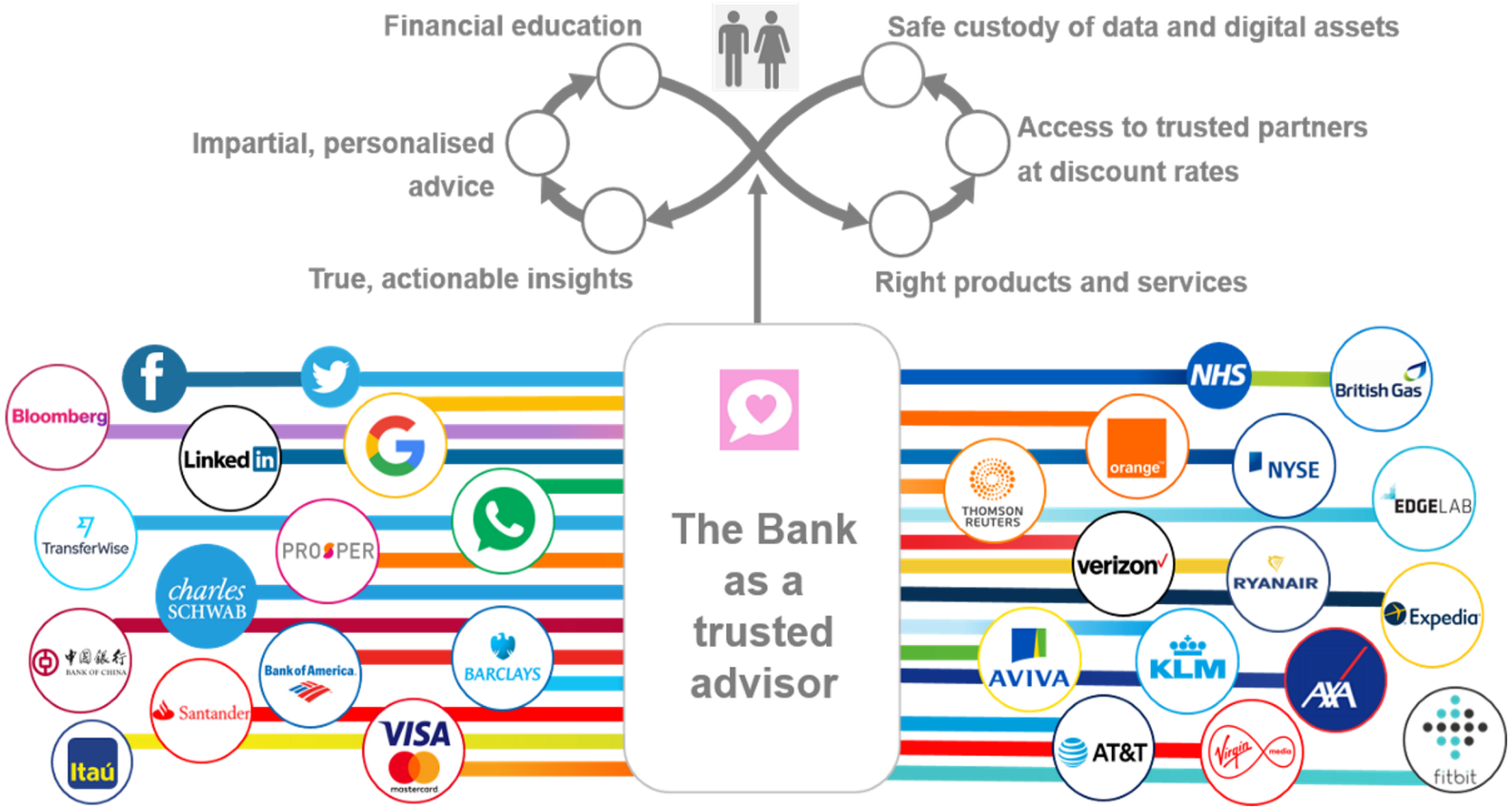
$ 535,000 (USD)

Attackers invest time, effort and money.

Why?

ATTACK ANALYSIS

Aggregators

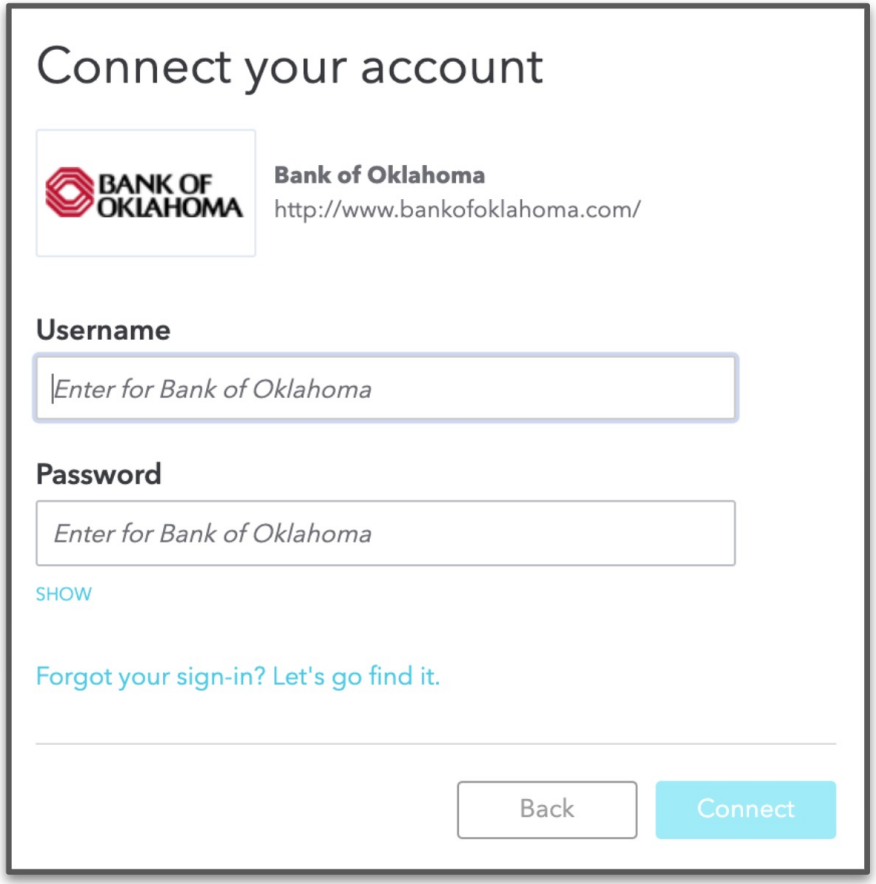


Financial data aggregation enables a single view

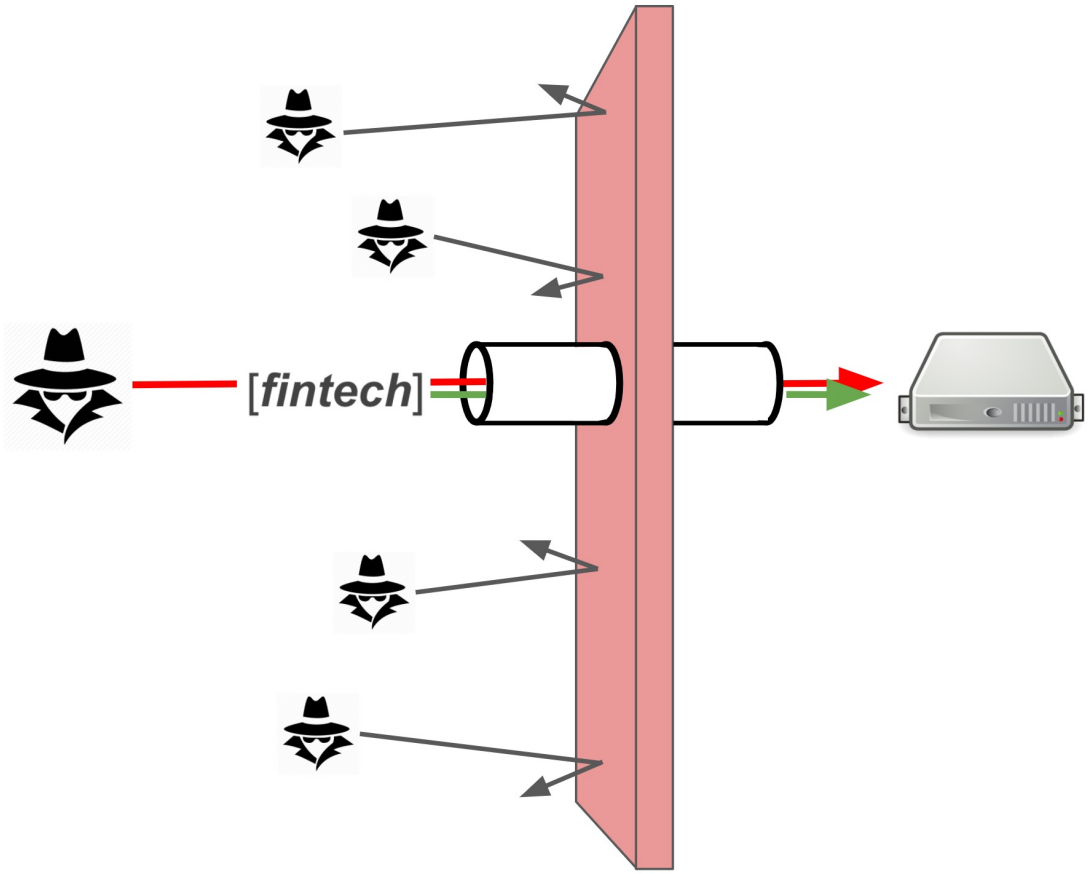
Who is accountable for security ?

Customer

Attacker



Attack via Fintech



Dark web forum

Open a [fintech] account and add the bank account using the username and password. This will

- *Check if the account is still live,*
- *Let you see the balance of the accounts, and*
- *If needed, let you check for deposits from PayPal, as well as to keep an eye on it.*

Research the background of account holder and get their SSN from ssnvalidator.com

Bad Behavior

BANK

Q : Please use our API ?

1. Sign in directly with Chase

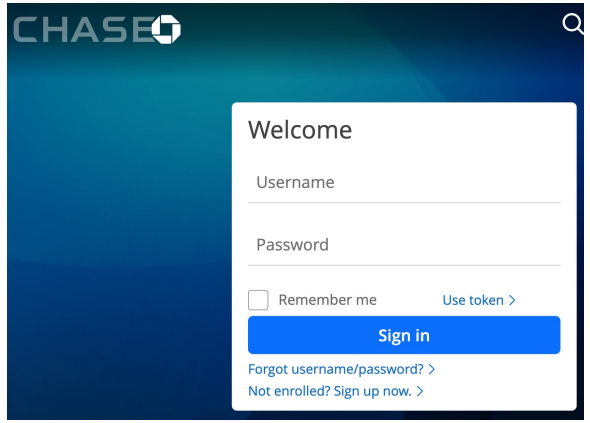
2. Choose what accounts they can access

3. Remove access whenever you want

https://www.chase.com/digital/data-sharing
https://developer.jpmorgan.com/

FINTECH

A : That doesn't work for us



We do what we want !
And there is nothing you can do about it
Or is there ?

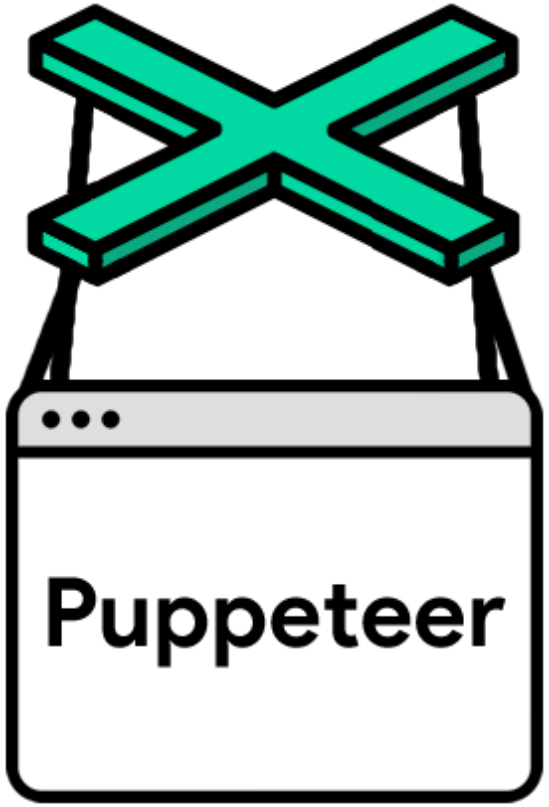
Tools and Techniques

Attacks Using Python


```
import requests
import os
import random
import string
import json

chars = string.ascii_letters + string.digits + '!@#$%^&*()'
random.seed = (os.urandom(1024))

url =
'http://craigslist.pottsfam.com/index872dijasydu2iuad27aysdu2yytaus6d2ajsdhasdasd2.php'

names = json.loads(open('names.json').read())

for name in names:
                name_extra = ''.join(random.choice(string.digits))

                username = name.lower() + name_extra + '@yahoo.com'
                password = ''.join(random.choice(chars) for i in range(8))

                requests.post(url, allow_redirects=False, data={
                                'auid2yjauysd2uasdasdasd': username,
                                'kjauysd6sAJSDhyui2yasd': password
                })

                print 'sending username %s and password %s' % (username,
password)
```

Script based attacks are trivial to implement

Tools - Puppeteer



Purpose built automation tools are widely used by developers

Tools - Selenium

Selenium automates browsers. That's it!

What you do with that power is entirely up to you.

Primarily it is for automating web applications for testing purposes, but is certainly not limited to just that.
Boring web-based administration tasks can (and should) also be automated as well.

… and can be very effective in automated attacks

Tools - Sikuli

Add user behaviour

SikuliX's Visual Approach

SikuliX automates anything you see on your Windows, Mac or Linux screen. It uses image recognition powered by OpenCV.

Automate Workflows Visually

Mimic user behaviour on any user interface on your screen. Including automating keyboard and mouse actions.

Use it for Visual Testing

Augment your GUI testing with SikuliX's visual approach if internals are not available. Look at it like a human.

Tools - Hackium

https://github.com/jsoverson/hackium

“Professionals”

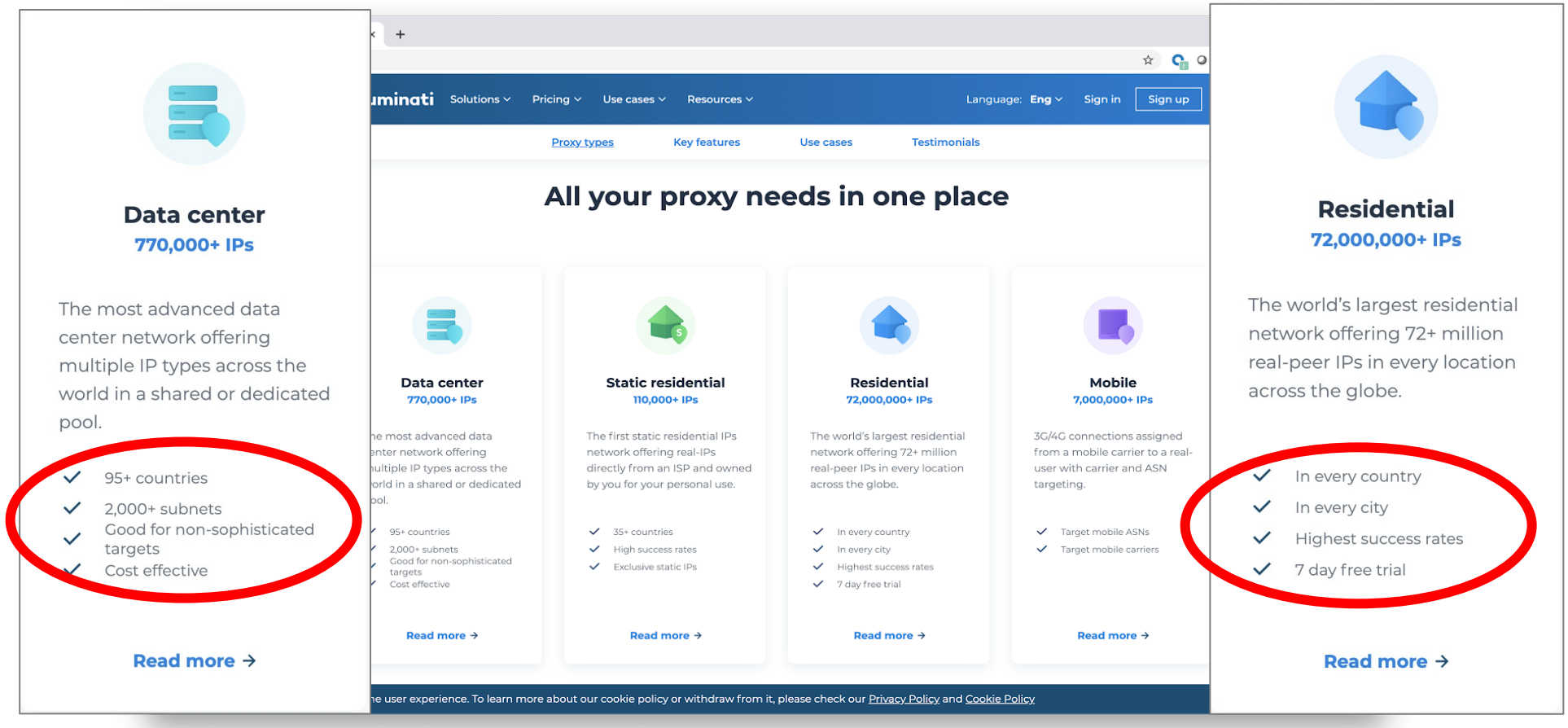
will build

their own tools

Network-level rate limiting is easily bypassed

Rotating IPs, randomizing user agents defeats rate limits, blacklists

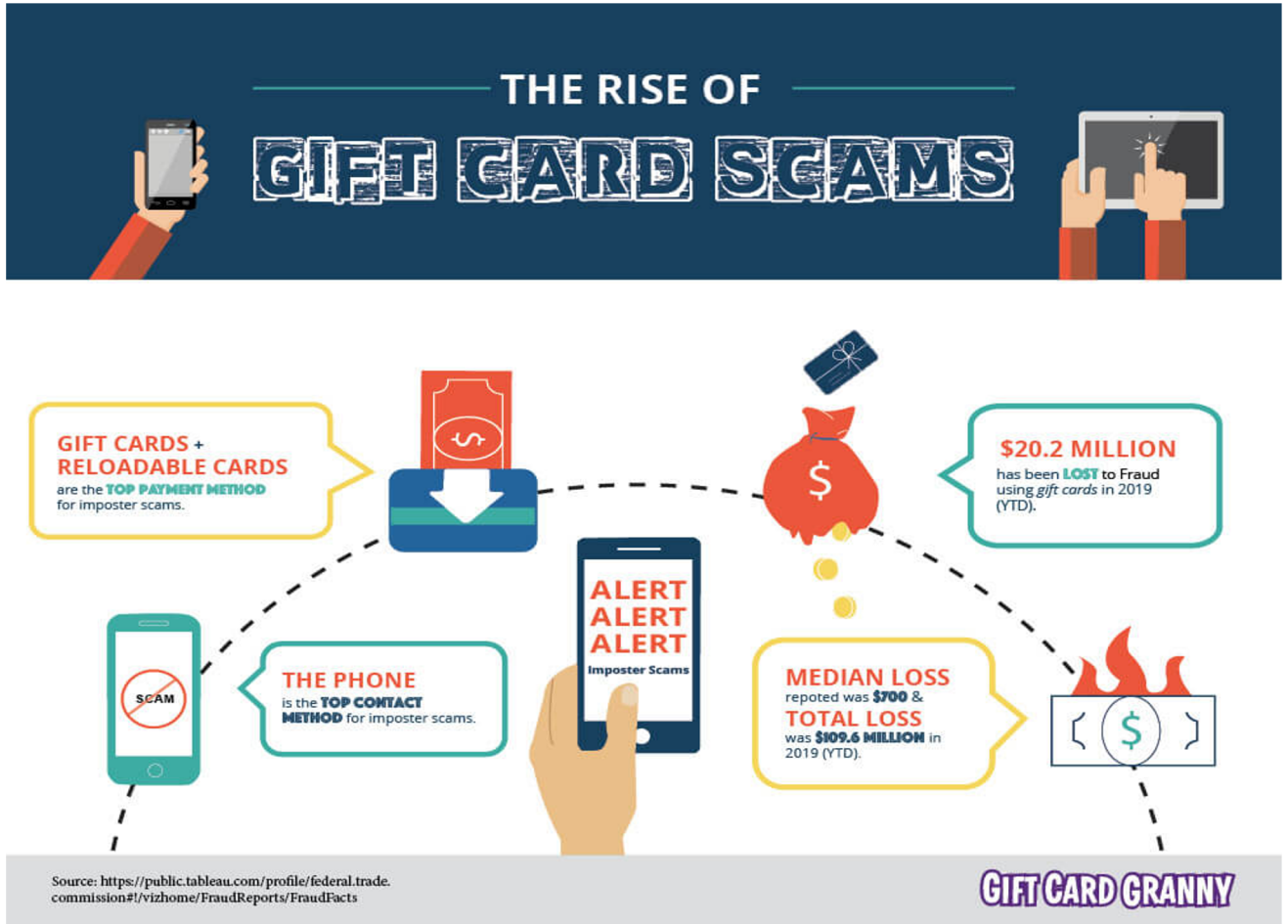
Proxy services are now mainstream and reliable. The same services used for commercial obfuscation enables criminals to hide, too



https://luminati.io/ https://oxylabs.io/

ATTACK ANALYSIS

Gift Card Fraud

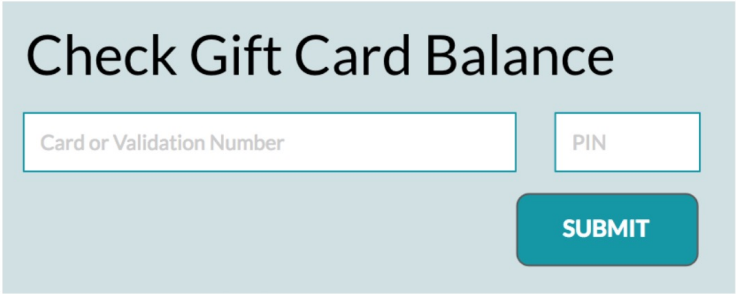


Commerce loves loyalty and giftcard programs

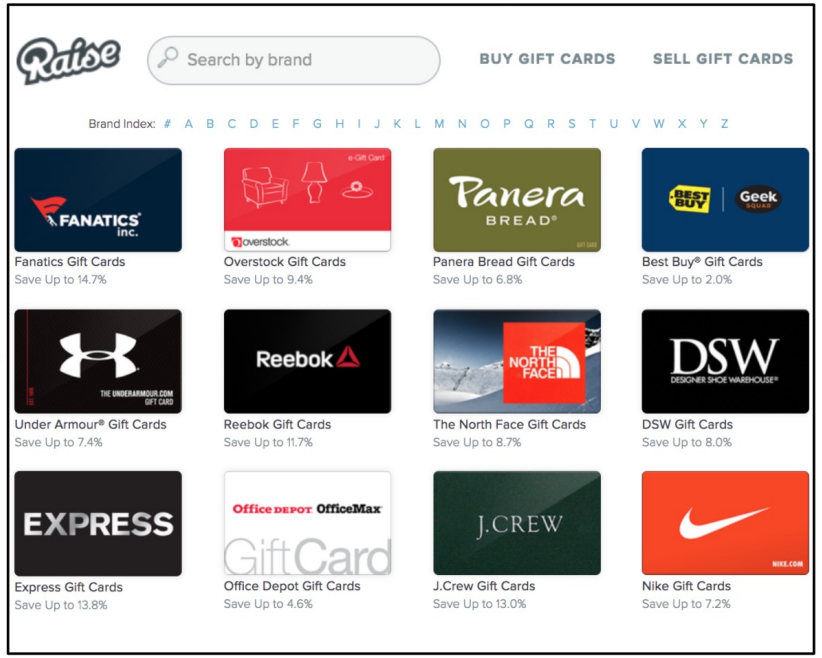
Gift card balance applications are aggressively targeted

Only card number and PIN needed to monetize

fraudster



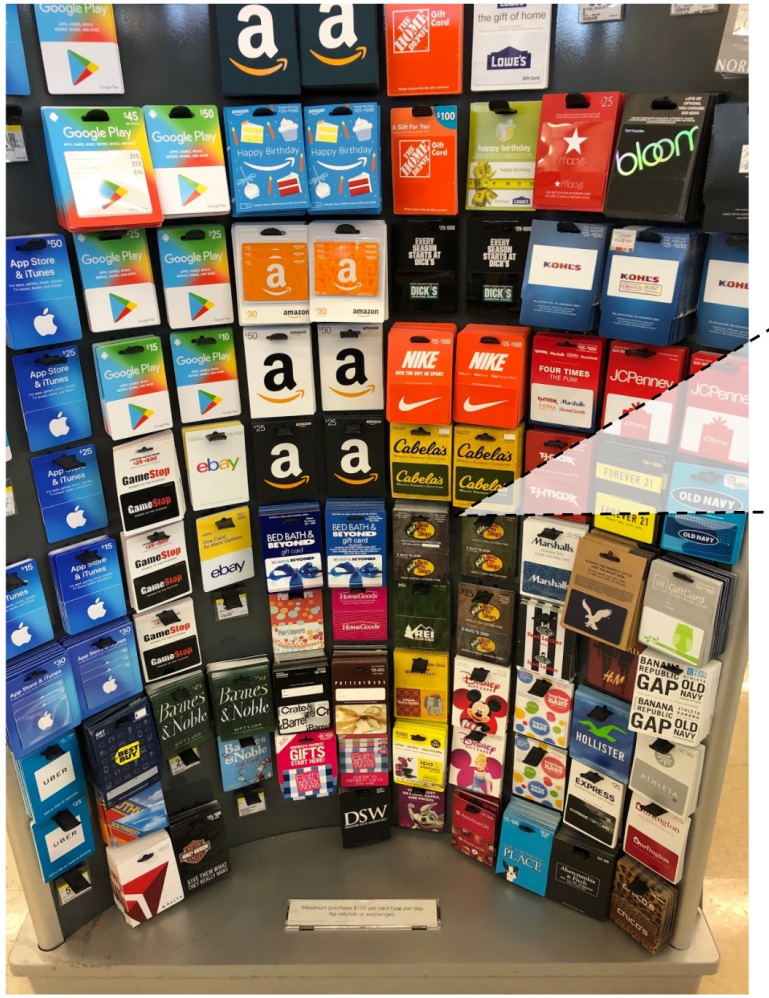
check gift card balance application

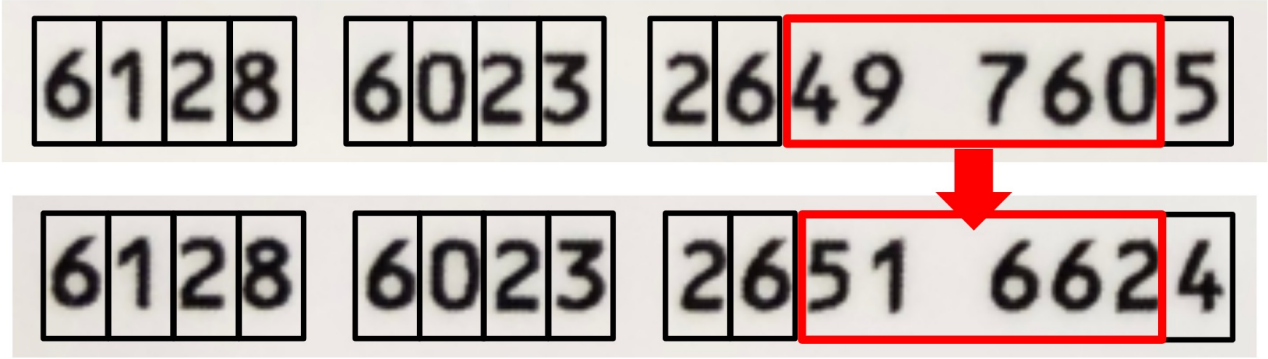


third-party gift card buyers/sellers

Might be easier than you expect

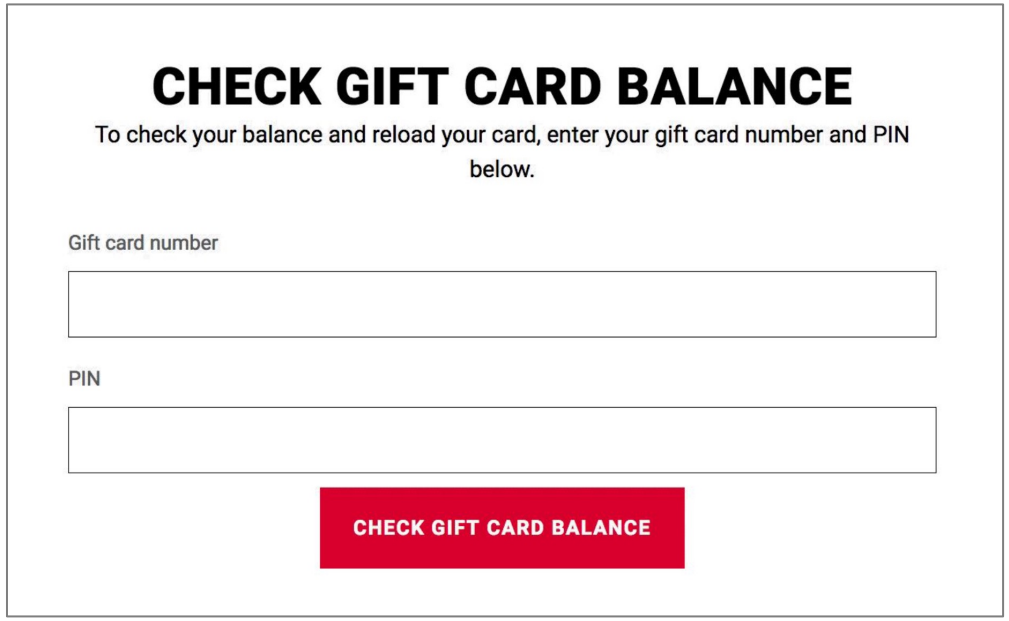
Attackers often don't need to try all possible card numbers and PINs





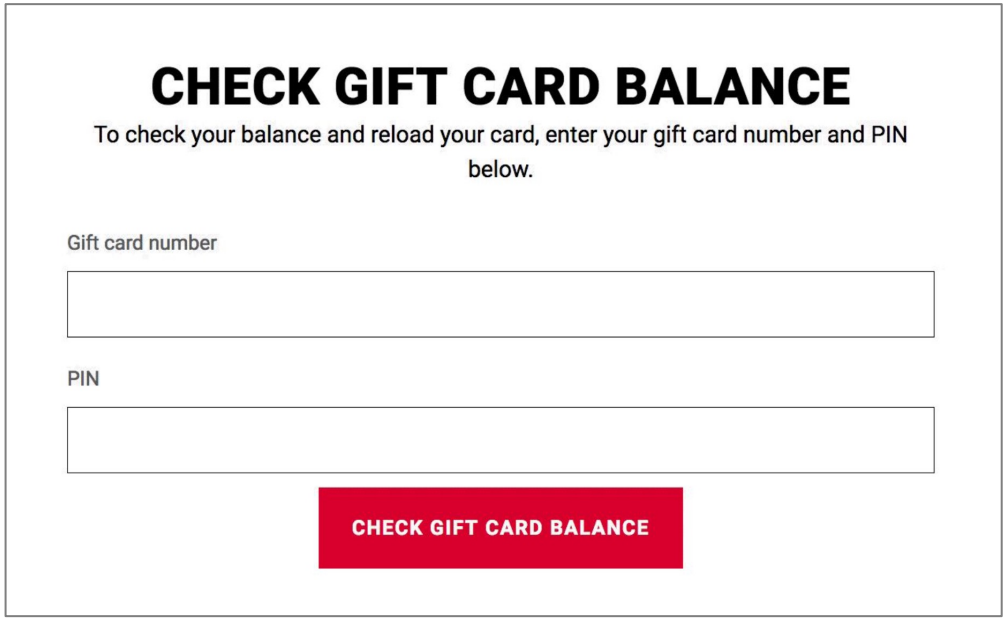
Checking gift card balance with six lines of code

```
1 from selenium import webdriver
2 browser = webdriver.Firefox()
3 browser.get("https://www.footlocker.com/giftcards/checkbalance")
4 browser.find_element_by_id('input_svcNumber').send_keys("6128602326497605")
5 browser.find_element_by_id('input_svcPIN').send_keys("05393457")
6 browser.find_element_by_css_selector('#main > div > div > div > form >
      div.row.flex-middle > button').click()
```



Considered "sophisticated"

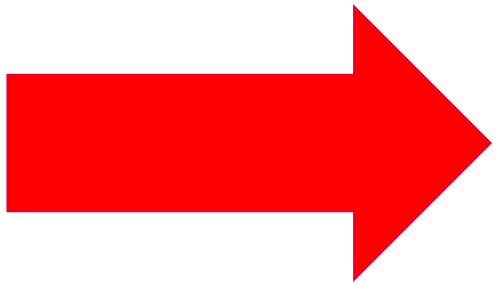
```python
import pyautogui
import pyautogui.tweens
from selenium import webdriver
from selenium.webdriver.common.keys import Keys
from time import sleep
from selenium import webdriver
browser = webdriver.Firefox()
browser.get("https://www.footlocker.com/giftcards/checkbalance")
# Card 6128602326497605
# PIN 05393457
browser.find_element_by_id('input_svcNumber').send_keys("6")
pyautogui.typewrite('12', interval=.2)
pyautogui.typewrite('860', interval=.1)
pyautogui.typewrite('23', interval=.3)
pyautogui.typewrite('2', interval=.2)
pyautogui.typewrite('64', interval=.2)
pyautogui.typewrite('976', interval=.1)
pyautogui.typewrite('05', interval=.1)
browser.find_element_by_id('input_svcPIN').send_keys("0")
pyautogui.typewrite('53', interval=.2)
pyautogui.typewrite('934', interval=.1)
pyautogui.typewrite('5', interval=.2)
pyautogui.typewrite('7', interval=.3)
pyautogui.moveTo(705, 720, .7, pyautogui.easeOutQuad)
pyautogui.click()
browser.quit()
```



Common Mitigation Methods

Deny IP and signatures

- IP denylist
- geoblocking
- IP rate limits
- Useragent
- other signatures



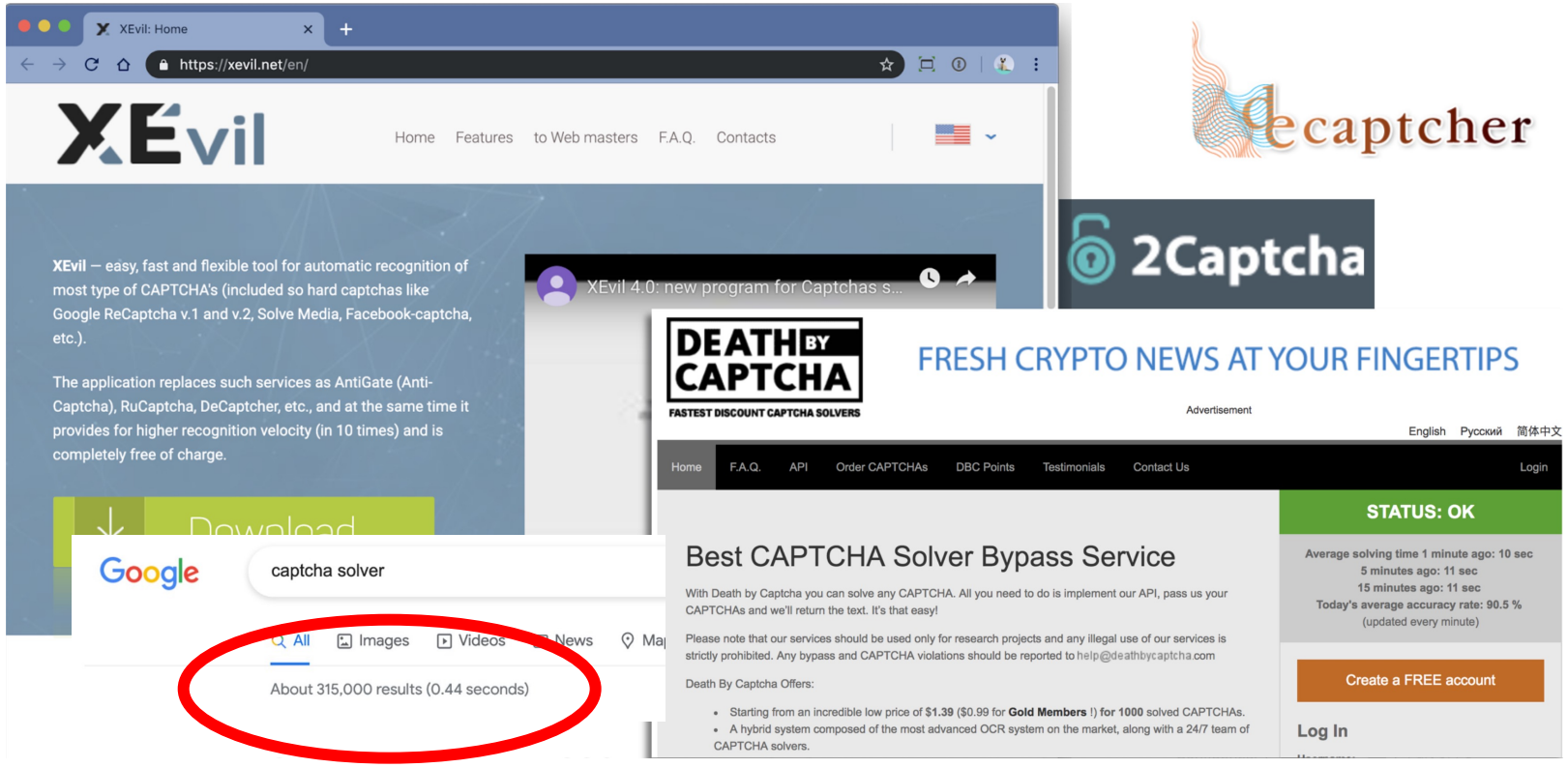
bypass with

proxynet

low volume

spoofing & diversification

CAPTCHA



decaptcher

2Captcha

CAPTCHA solvers are cheap and plentiful

Attackers solve CAPTCHA more effectively than humans !

MFA

amazon.com.au Hello Select your address All Hello, Sign in Account Returns & Orders

All Best Sellers Prime New Releases Customer Service Fashion Today's Deals Kindle Books Books Electronics Gift Ideas

Help & Customer Service

‹ All Help Topics

Account Settings

- About Creating an Account
- About Signing In and Signing Out
- About Closing Your Account
- About Mobile Phone Number Accounts
- About SMS Verification for Mobile Phone Number Accounts
- About Two-Step Verification
- **Turning on Two-Step Verification**
- Changing Two-Step Verification Settings
- Disabling Two-Step Verification
- Two-Step Verification Account Recovery
- Notifications & E-mail Subscriptions

Find more solutions

Managing Your Account › Account Settings ›

Turning on Two-Step Verification

Here's how to enable Amazon's Two-Step Verification, a feature that adds an extra layer of security by asking you to enter a unique security code in addition to your password on computers and devices that you haven't designated as trusted.

To enable Two-Step Verification:

1. Go to **Your Account** and select **Login & Security Settings**.
2. Click **Edit** in the **Advanced Security Settings** section.
3. Click **Enable** to set-up Two-Step Verification.
4. Add your primary phone number (this phone must be able to receive text messages) or download

Why is 2FA optional at Amazon ?

A = $$$

Can you achieve the same outcome without user friction?

EXAMPLE ATTACK

MFA Bypass

EDITION: AU

ZDNet

MOBILITY SECURITY NBN CXO HARDWARE MORE NEWSLETTERS ALL WRITERS

MUST READ: What is cyber insurance? Everything you need to know

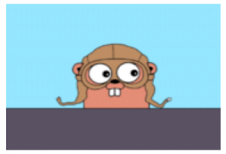
FBI warns about attacks that bypass multi-factor authentication (MFA)

FBI warns about SIM swapping and tools like Muraen and NecroBrowser.

By Catalin Cimpanu for Zero Day | October 7, 2019 -- 12:15 GMT (23:15 AEDT) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Chrome will soon try HTTPS first when you type an incomplete URL



Security
Go malware is now common, having been adopted by both APTs and e-crime groups

Security
Chinese cyberspies targeted Tibetans with a malicious

MFA works but it does have limits

MFA bypass – low effort

Call tech support - "*I've lost my token/device/etc !*"

Phishing site - "*please enter credentials and token*"

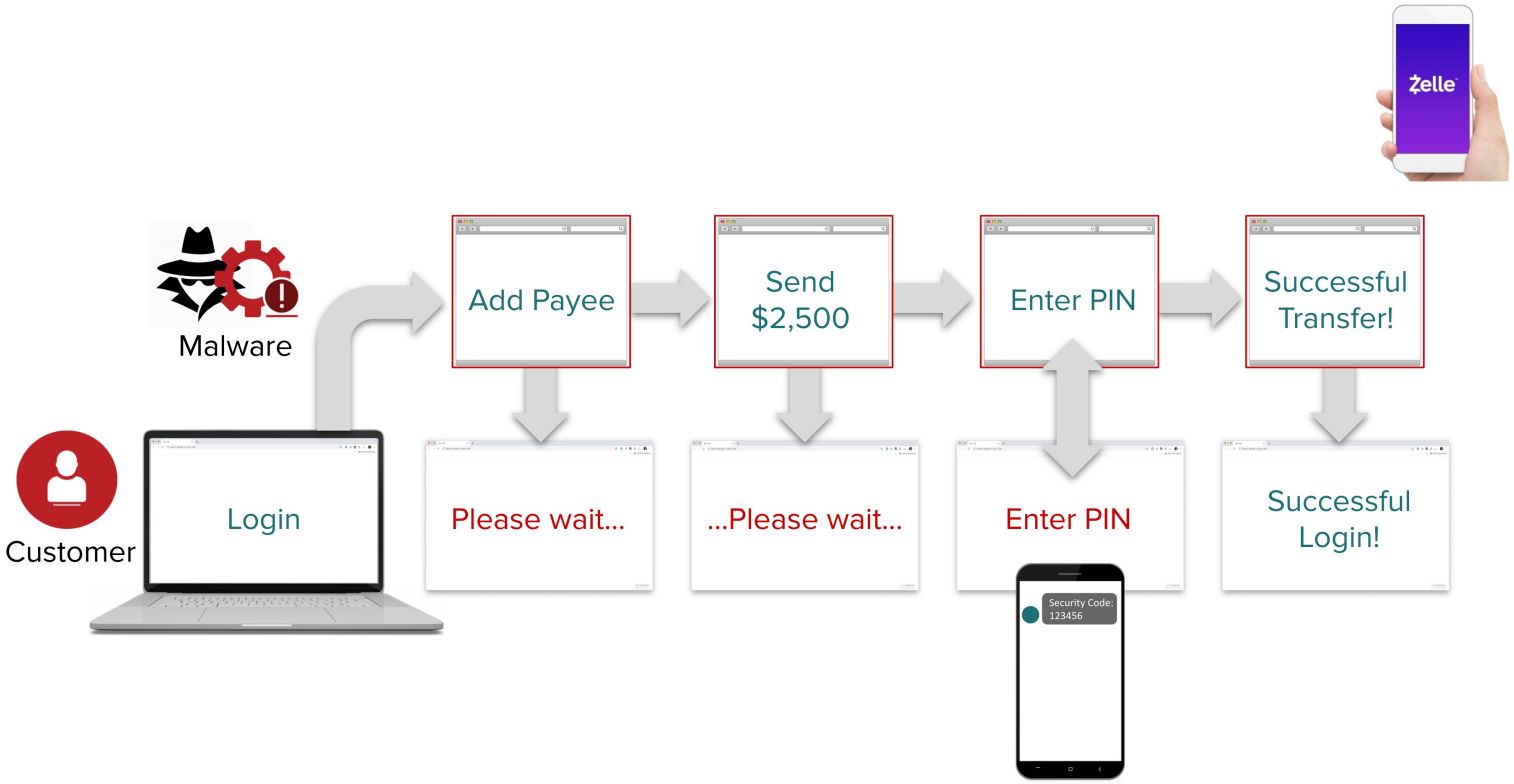
Pretence – "*Hi I'm from your bank, trust me*"

And more ...

Social engineering

https://www.enzoic.com/social-engineering-tactics/

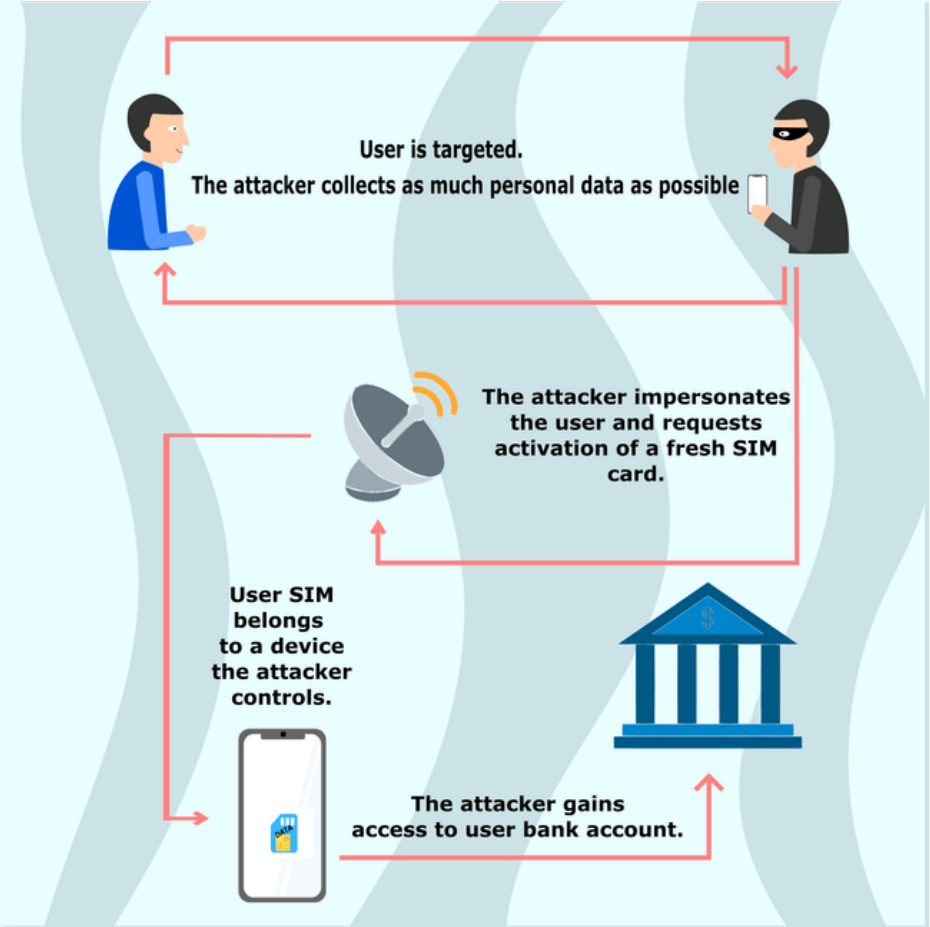
MFA bypass – medium effort



Man-in-the-browser malware can bypass MFA

Lower volume of attempts is balanced by a much higher rate of success

MFA bypass – medium effort



SIM Swap FRAUD

MFA bypass – (very) advanced

SolarWinds hackers have a clever way to bypass multi-factor authentication

*Volexity's investigation into this incident determined the attacker had accessed the Duo integration secret key (**akey**) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account. It should be noted this is not a vulnerability with the MFA provider*

hack the target
bypass MFA

next level pwnage

Reference : https://www.schneier.com/blog/archives/2020/12/how-the-solarwinds-hackers-bypassed-duo-multi-factor-authentication.html

Where to next?

So what to do now?

- Security team says they have things under control
- The fraud group doesn't talk to security team
- Neither talk to marketing

OWASP Automated Top Threats

Who is accountable for

customer experience
+
reducing costs (fraud)
+
effective security
+
brand reputation

?

A new way of thinking is required

Summary

- What is an Automated Threat?
- What are common tools used?
- Motivation of threat actors
- Common Mitigated Methods and their pitfalls
- Example attacks for gift card fraud and MFA bypass
- How can OWASP Automated Threats help?
- Who should care about Automated Threats?