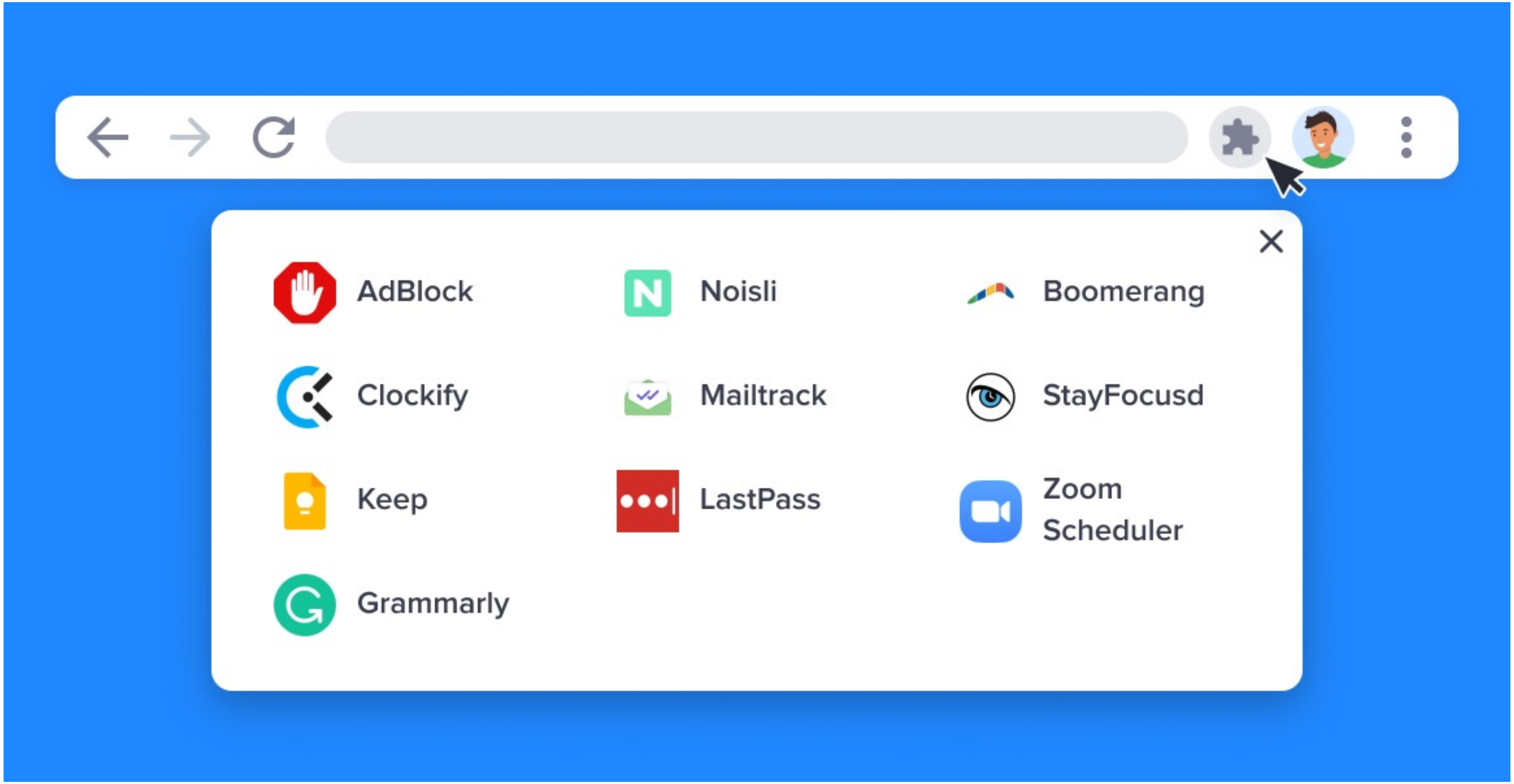
CSE610: Web Programming & Security

9. Browser Extensions & Phishing

Seongil Wi

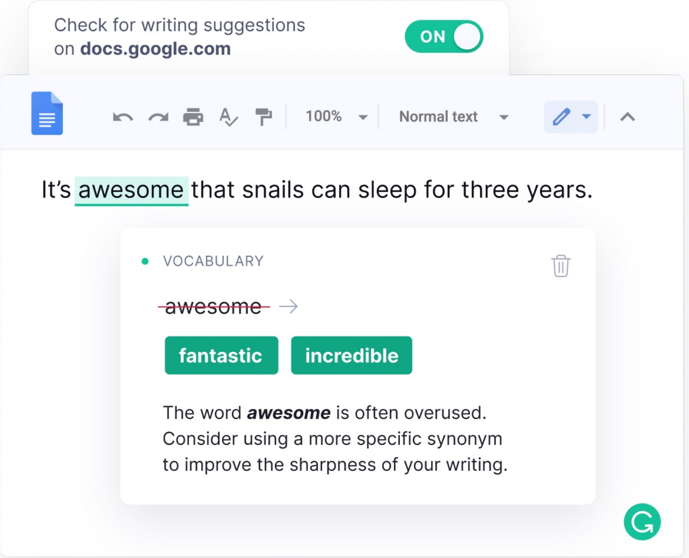
Department of Computer Science and Engineering

Browser Extension



What is a Browser Extension?

- A software that allows you to **customize your web browser/website**
  - Add extra features



Check for writing suggestions on **docs.google.com** ON

It's awesome that snails can sleep for three years.

VOCABULARY

~~awesome~~ →

fantastic incredible

The word ***awesome*** is often overused. Consider using a more specific synonym to improve the sharpness of your writing.

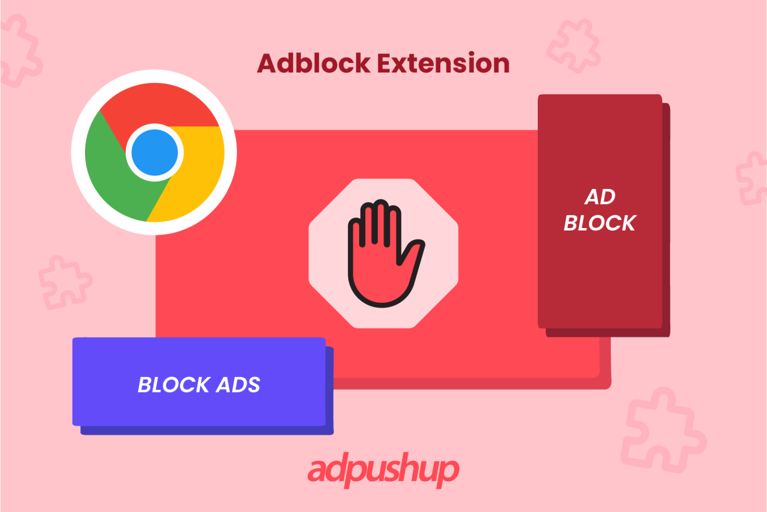


Image from https://chromewebstore.google.com/detail/custom-cursor-for-chrome/ogdlpmhglpejoiomcodnpjnfgcpmgale

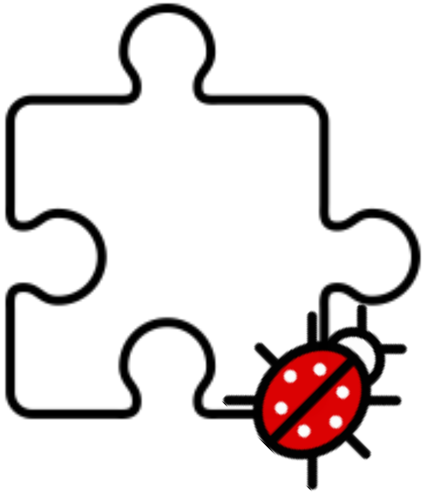
Popularity of Extensions

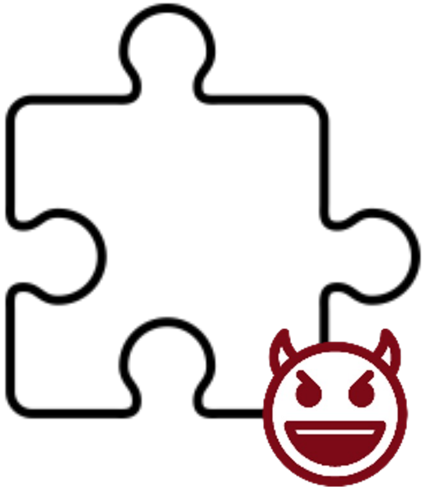
- 93% of enterprise companies use browser extensions
- 130,445 extensions are available for Chrome (2024)

https://www.pixiebrix.com/reports/state-of-browser-extensions-2023

Unfortunately…

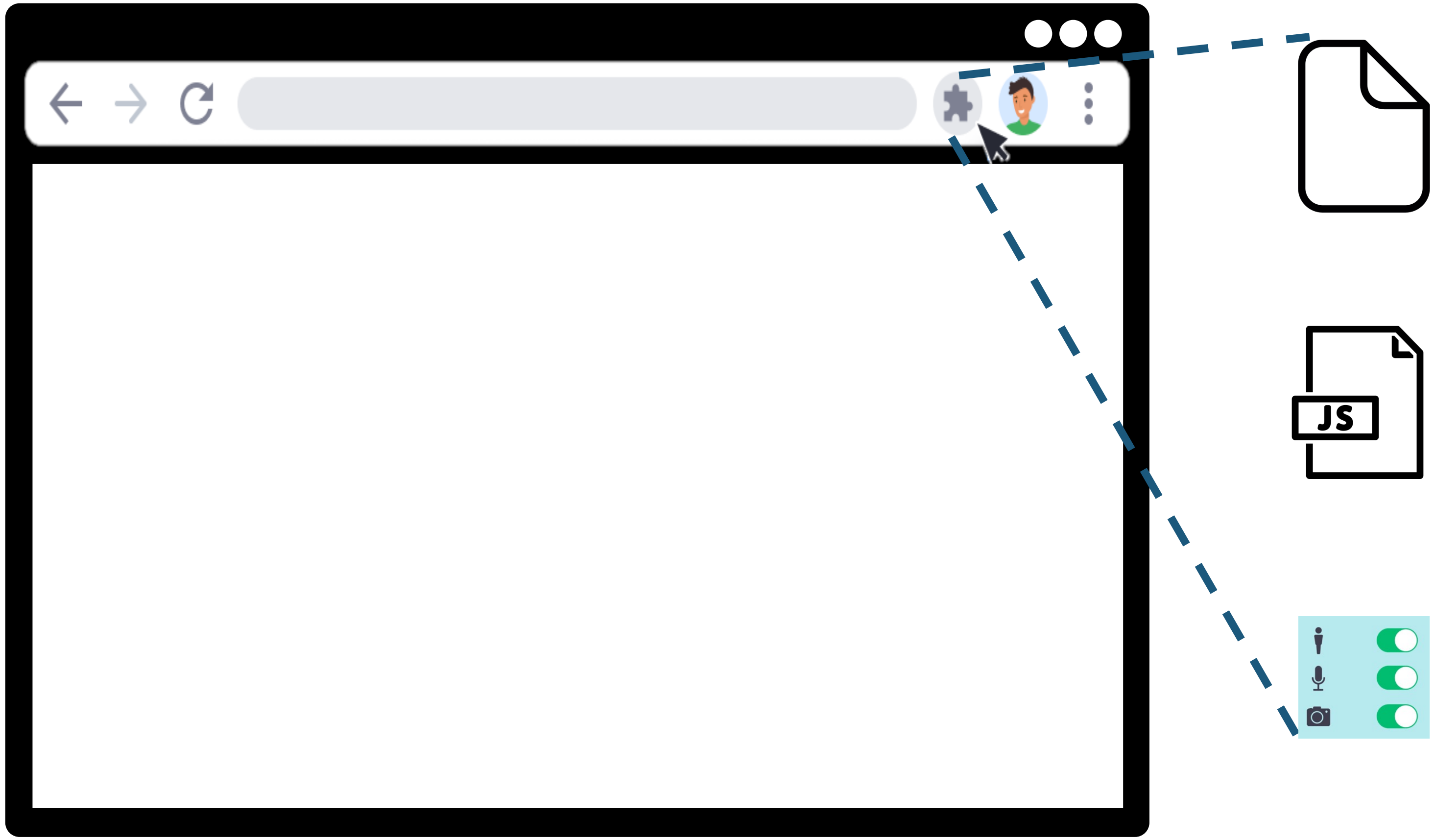
- There are lots of vulnerable or malicious extensions





Browser Extensions - Structure Overview

- A browser extension consists of three components: **background pages**, **content scripts**, and **permissions**



- **Background Pages**
- **Content Scripts**
- **Permissions**

Manifest File

Defines extension properties

```
"background": {
  "scripts": ["background.js"]
},

"content_scripts": [{
  "matches": ["http://www.google.com/*"],
  "css": ["mystyle.css"]
  "js": ["jquery.js", "myscript.js"]
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

- **Background Pages**
- **Content Scripts**
- **Permissions**

Background Pages

```
"background": {
  "scripts": ["background.js"]
},

"content_scripts": [{
  "matches": ["http://www.google.com/*"],
  "css": ["mystyle.css"]
  "js": ["jquery.js", "myscript.js"]
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**
- **Permissions**

Content Scripts

```
"background": {
  "scripts": ["background.js"]
},

"content_scripts": [{
  "matches": ["http://www.google.com/*"],
  "css": ["mystyle.css"]
  "js": ["jquery.js", "myscript.js"]
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**

Content Scripts

Two JavaScript files will be run in the page for any URLs matching the specified URL patterns

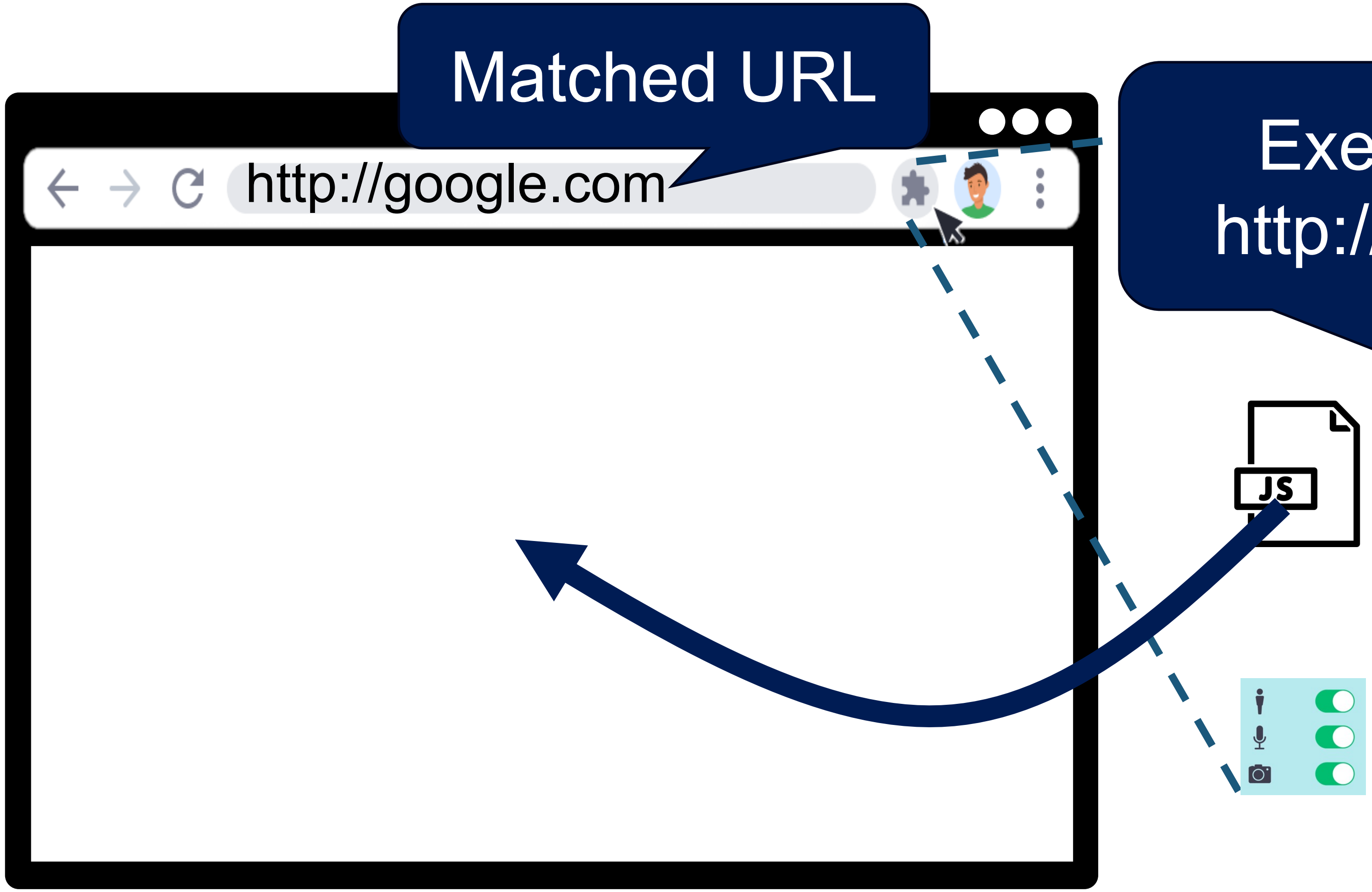
```
"background":
  "scripts": [
},

"content_scripts": [{
  "matches": ["http://www.google.com/*"],
  "css": ["mystyle.css"]
  "js": ["jquery.js", "myscript.js"]
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**

Content Scripts



Execute this JS from http://google.com origin

efine the

on

o the user

- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**

Permissions

```
"background": {
  "scripts": ["background.js"]
},

"content_scripts": [{
  "matches": ["http://www.google.com/*"],
  "css": ["mystyle.css"]
  "js": ["jquery.js", "myscript.js"]
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**

Permissions

```
"background": {
  "scripts": ["background.js"]
}
}],

"permissions": [
  "bookmakrs",
  "*://*.facebook.com/",
  "https://www.google.com/"
],
...
```

Extension API permission: tab, geolocation, bookmarks, webRequests, … (browser provided APIs)

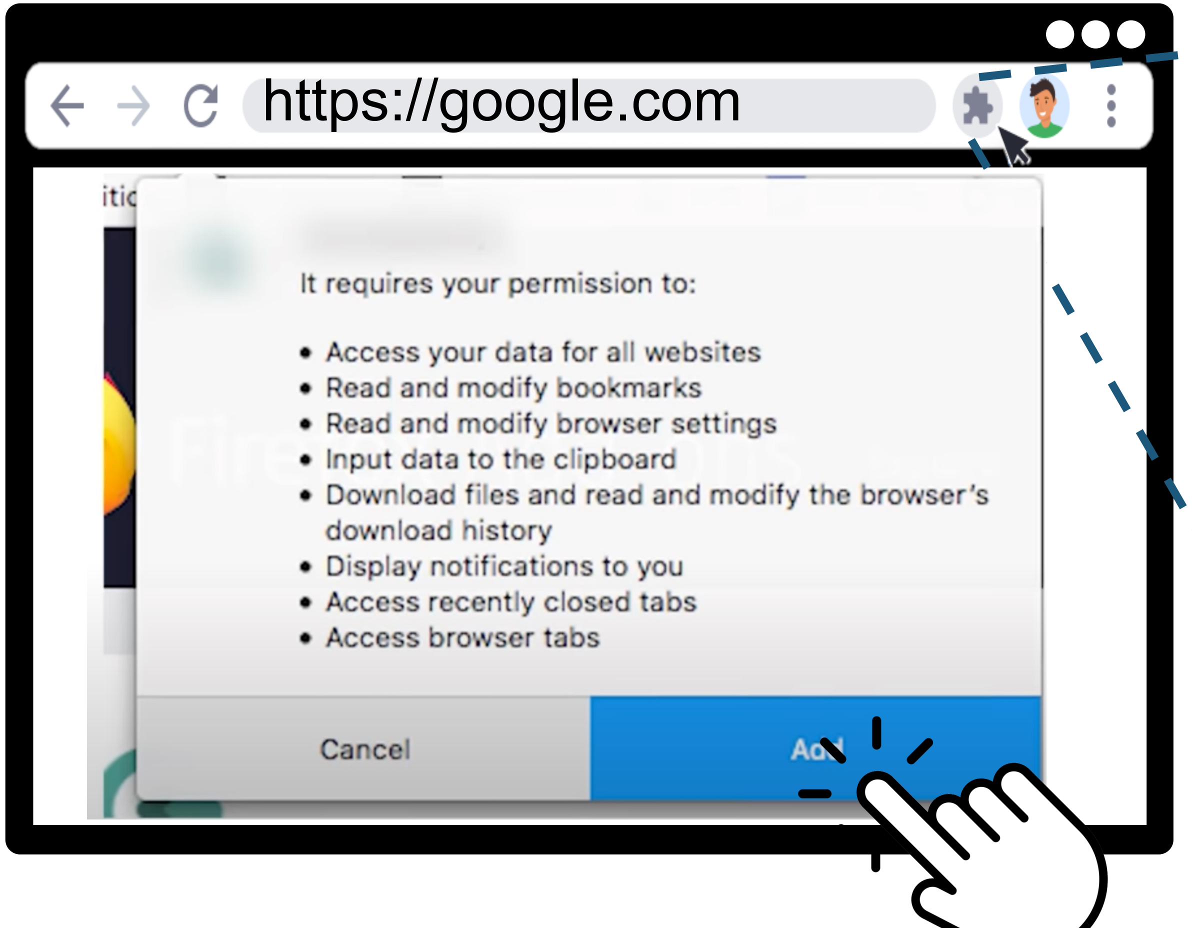
Extension API permissions operate in conjunction with the optional **host permissions**

- **Background Pages**: define the

es that runs in the context of a web page

- **Permissions**: permissions to access the different parts of the extension API

Permissions



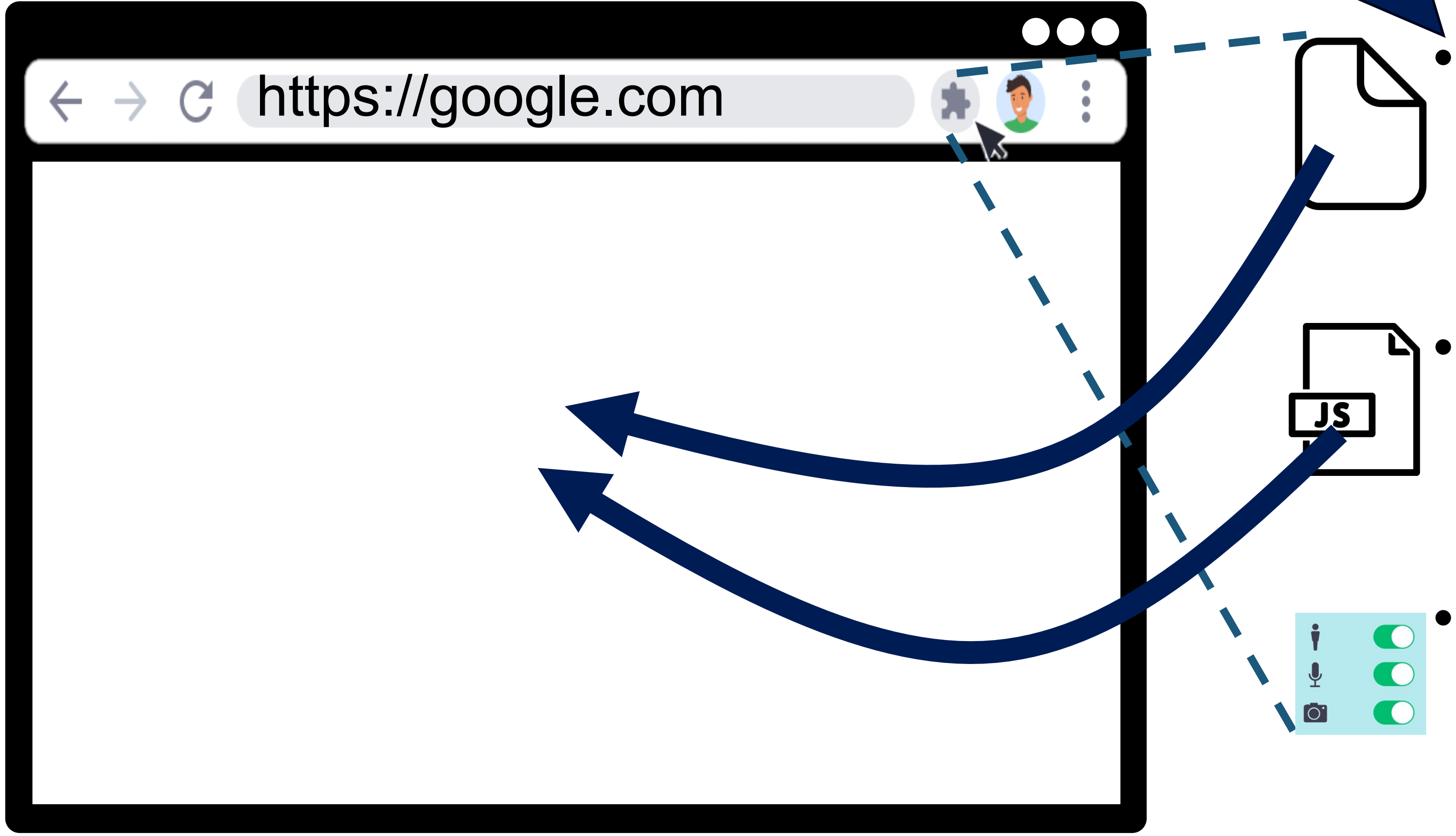
It requires your permission to:

- Access your data for all websites
- Read and modify bookmarks
- Read and modify browser settings
- Input data to the clipboard
- Download files and read and modify the browser's download history
- Display notifications to you
- Access recently closed tabs
- Access browser tabs

- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**: permissions to access the different parts of the extension API

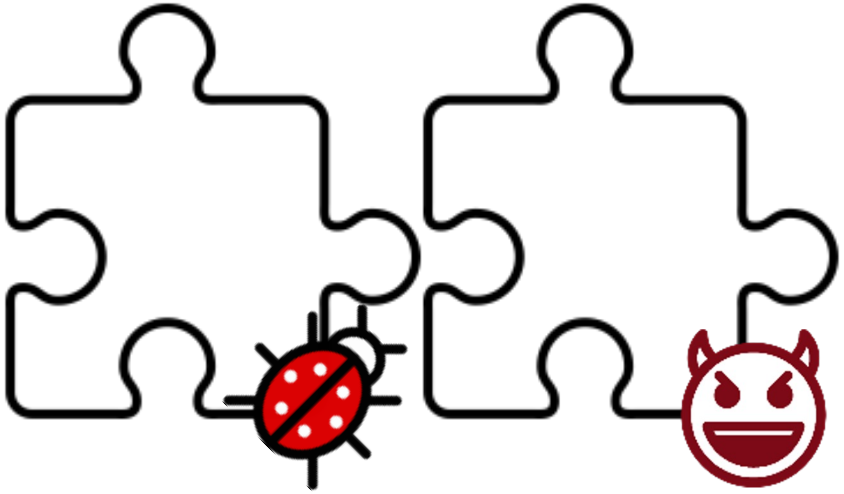
Permissions

Can execute privileged `chrome.*` APIs according to its permissions



- **Background Pages**: define the behavior of the extension
  - Do not have any visibility to the user
- **Content Scripts**: JavaScript files that runs in the context of a web page
- **Permissions**: permissions to access the different parts of the extension API

Is Your Extension Secure?



Malicious Extensions

```
"background": {
  "scripts": ["background.js"]
},

"content_scripts": [{
  "matches": ["*"],
  "js": ["attacker.js"]
}],

"permissions": [
  "bookmakrs",
  "geolocation”, …  //all permissions
  "*"
],
...
```

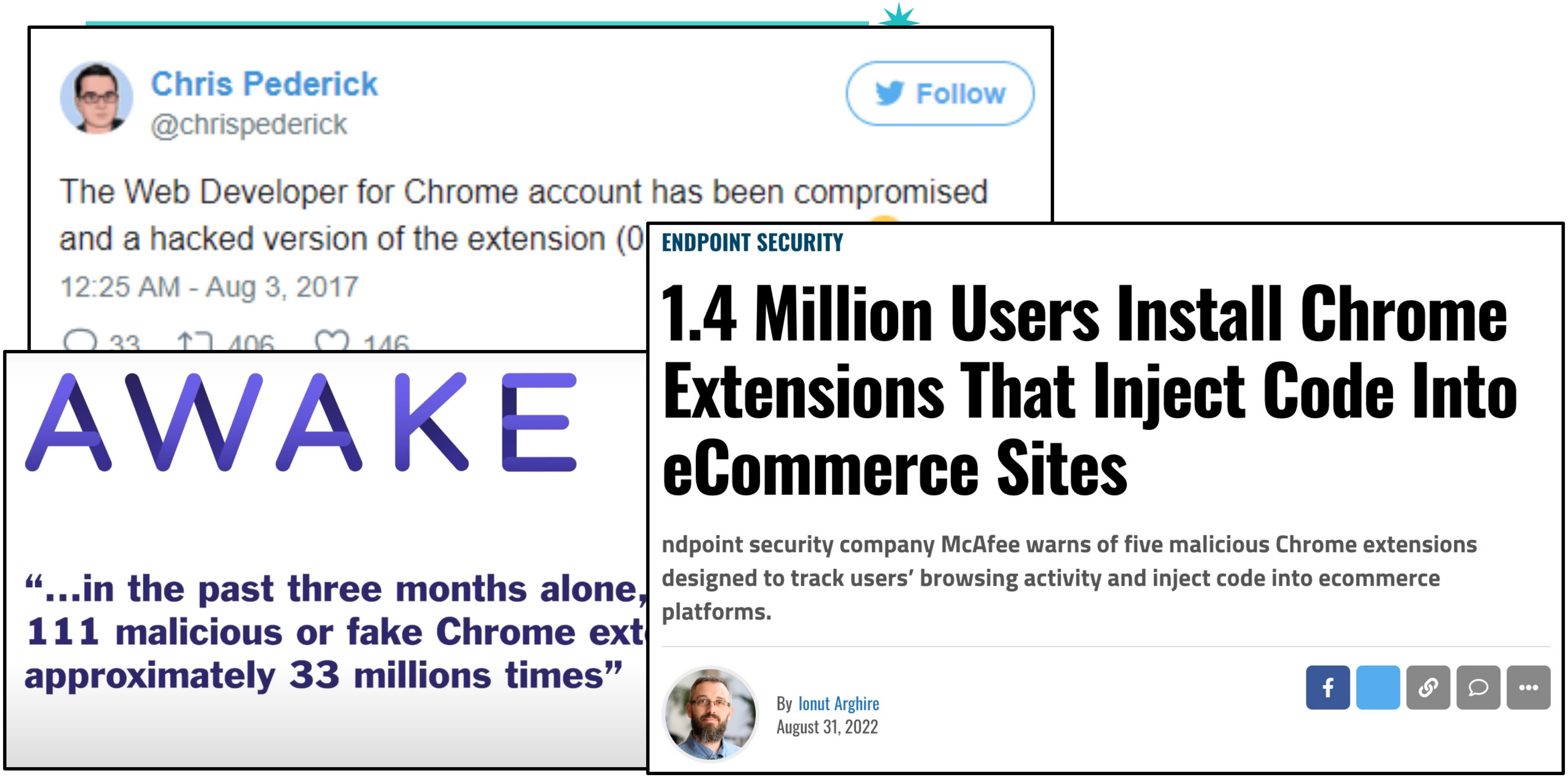
Execute arbitrary JS code in any domain

Execute arbitrary browser APIs in any domain

Malicious Extensions

- Modify page content
- Keystroke logging (steal your information)
- Steal cookies
- See browser histories
- Cryptocurrency mining
- Inject ad

Malicious Extensions



Chris Pederick
@chrispederick

Follow

The Web Developer for Chrome account has been compromised and a hacked version of the extension (0

12:25 AM - Aug 3, 2017

33 406 146

AWAKE

“...in the past three months alone,
111 malicious or fake Chrome ext
approximately 33 millions times”

ENDPOINT SECURITY

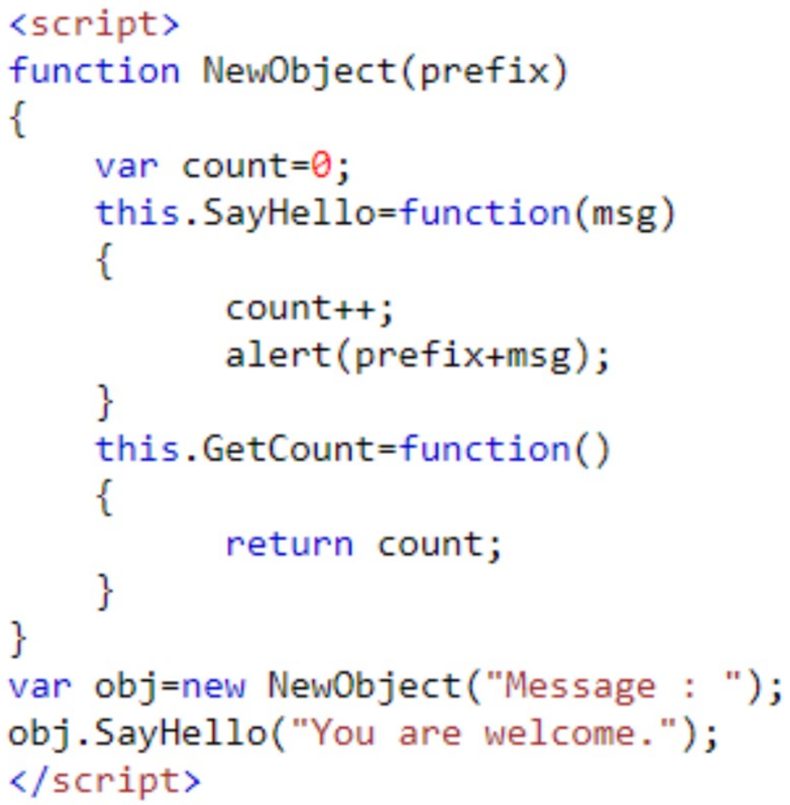
1.4 Million Users Install Chrome Extensions That Inject Code Into eCommerce Sites

ndpoint security company McAfee warns of five malicious Chrome extensions designed to track users’ browsing activity and inject code into ecommerce platforms.

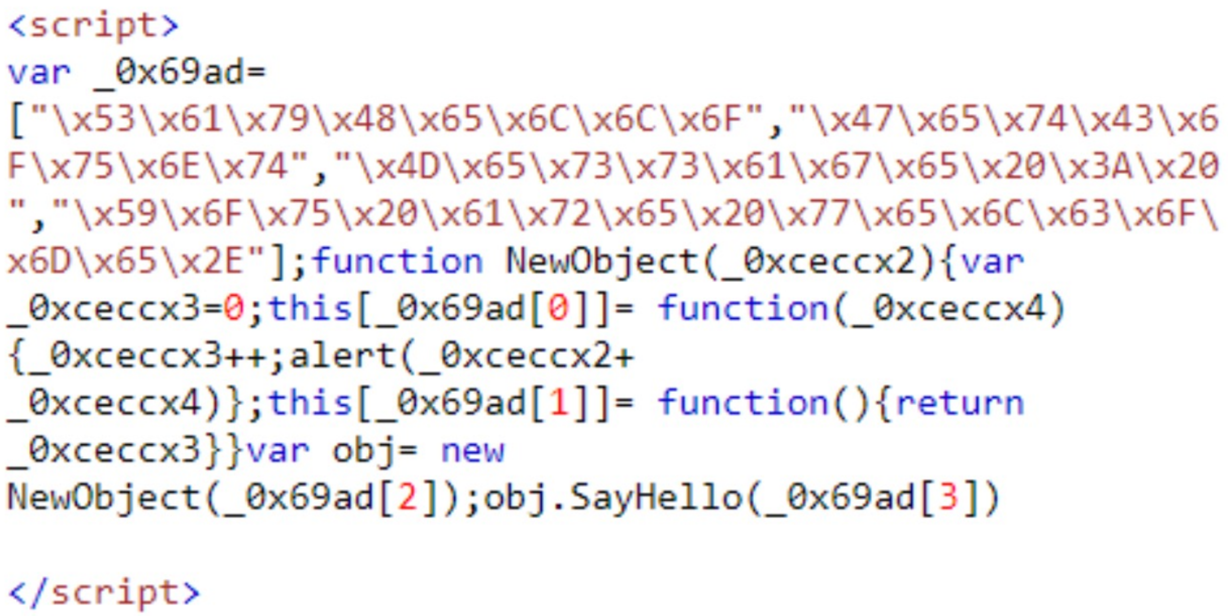
By Ionut Arghire
August 31, 2022

Difficulties in Identifying Malicious Extensions

- **JavaScript Obfuscation**



```
<script>
function NewObject(prefix)
{
    var count=0;
    this.SayHello=function(msg)
    {
          count++;
          alert(prefix+msg);
    }
    this.GetCount=function()
    {
          return count;
    }
}
var obj=new NewObject("Message : ");
obj.SayHello("You are welcome.");
</script>
```



```
<script>
var _0x69ad=
["\x53\x61\x79\x48\x65\x6C\x6C\x6F","\x47\x65\x74\x43\x6
F\x75\x6E\x74","\x4D\x65\x73\x73\x61\x67\x65\x20\x3A\x20
","\x59\x6F\x75\x20\x61\x72\x65\x20\x77\x65\x6C\x63\x6F\
x6D\x65\x2E"];function NewObject(_0xceccx2){var
_0xceccx3=0;this[_0x69ad[0]]= function(_0xceccx4)
{_0xceccx3++;alert(_0xceccx2+
_0xceccx4)};this[_0x69ad[1]]= function(){return
_0xceccx3}}var obj= new
NewObject(_0x69ad[2]);obj.SayHello(_0x69ad[3])

</script>
```

Difficulties in Identifying Malicious Extensions

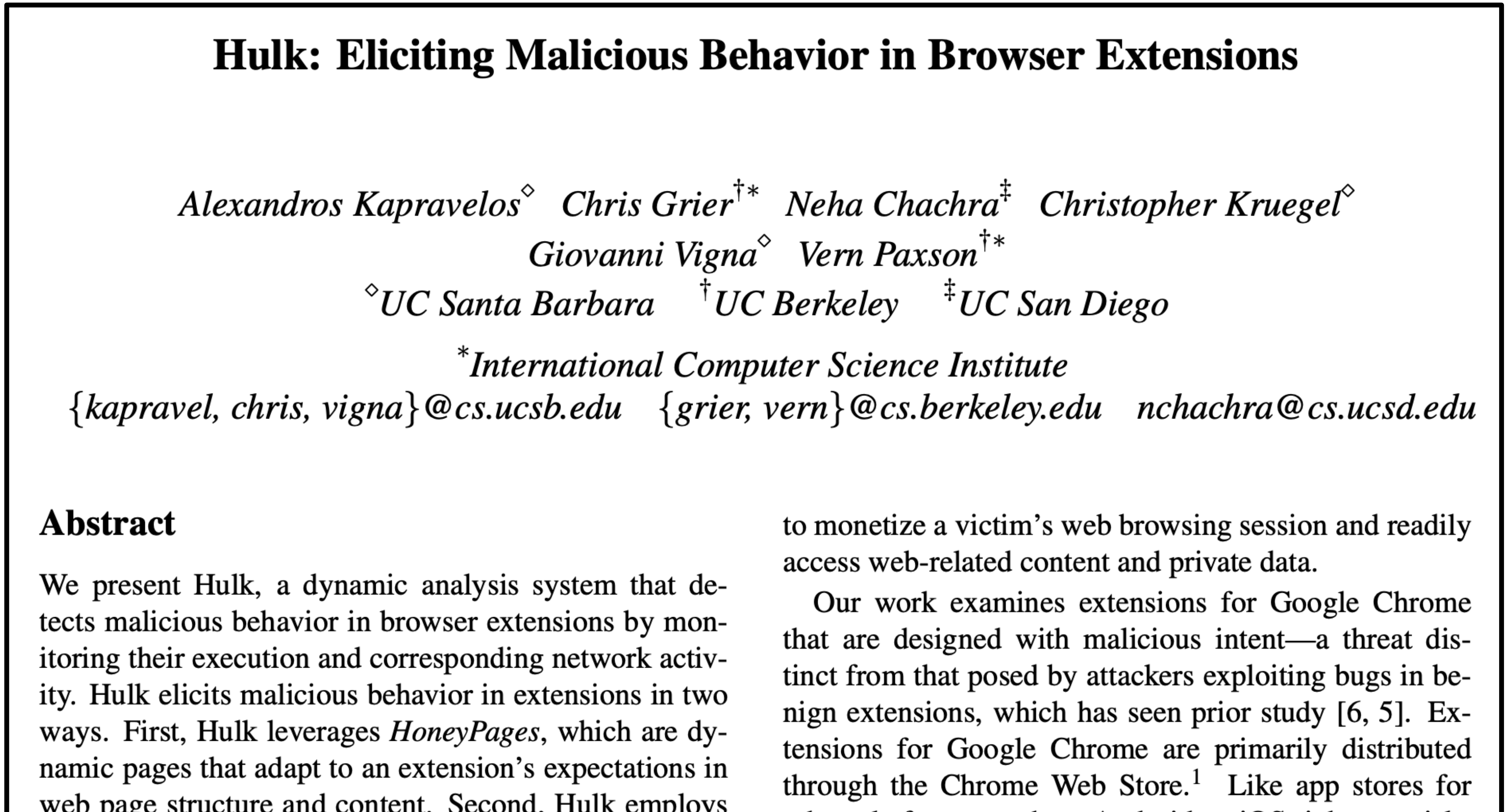
- **JavaScript Obfuscation**

- **Cloacking**: a malicious extension loads different code based on the tester’s location and IP
  - Google's IP range: loads legitimate code
  - IP range outside of Google: loads malicious code

- Its malicious behaviors can be triggered remotely
- No malicious behaviors appear until certain conditions met

Hulk, *UNISEX SEC'2014*

- Dynamically detect malicious extensions



Hulk: Eliciting Malicious Behavior in Browser Extensions

Alexandros Kapravelos[◇] *Chris Grier*[†*] *Neha Chachra*[‡] *Christopher Kruegel*[◇]
Giovanni Vigna[◇] *Vern Paxson*[†*]
[◇]*UC Santa Barbara* [†]*UC Berkeley* [‡]*UC San Diego*
[*]*International Computer Science Institute*
{*kapravel, chris, vigna*}*@cs.ucsb.edu* {*grier, vern*}*@cs.berkeley.edu* *nchachra@cs.ucsd.edu*

Abstract

We present Hulk, a dynamic analysis system that detects malicious behavior in browser extensions by monitoring their execution and corresponding network activity. Hulk elicits malicious behavior in extensions in two ways. First, Hulk leverages *HoneyPages*, which are dynamic pages that adapt to an extension's expectations in web page structure and content. Second, Hulk employs

to monetize a victim's web browsing session and readily access web-related content and private data.

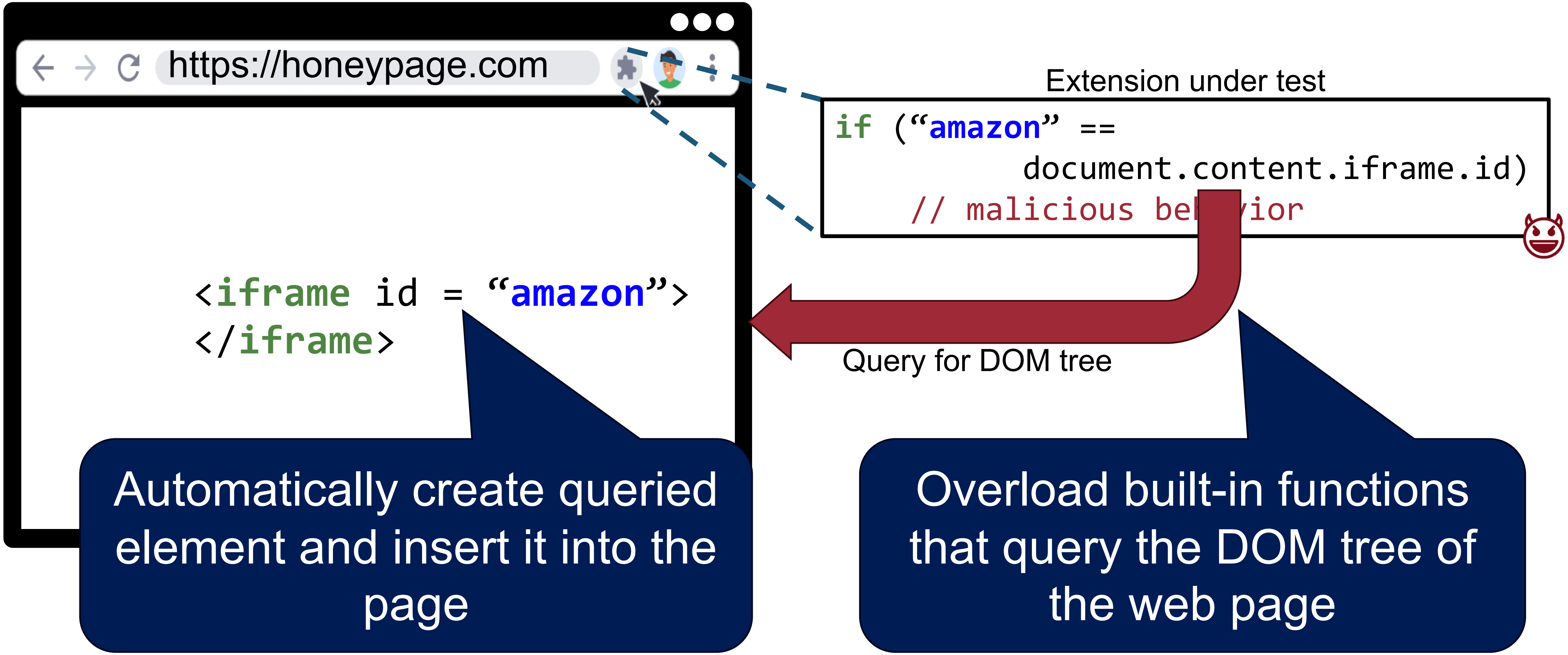
Our work examines extensions for Google Chrome that are designed with malicious intent—a threat distinct from that posed by attackers exploiting bugs in benign extensions, which has seen prior study [6, 5]. Extensions for Google Chrome are primarily distributed through the Chrome Web Store.[1] Like app stores for

Hulk, *UNISEX SEC'2014*

- Dynamically detect malicious extensions

- Let's trigger the malicious code, which is conditionally executed
  - How?
  - **Intuition**: several malicious extensions activate based on the content of a web page
  - **Idea**: Honey Page (Extension testing page)
  - Dynamically create DOM elements whenever an extension requests certain DOM elements

Honey Pages



https://honeypage.com

```
<iframe id = “amazon”>
</iframe>
```

Extension under test

```
if (“amazon” ==
            document.content.iframe.id)
    // malicious beh vior
```

Query for DOM tree

Automatically create queried element and insert it into the page

Overload built-in functions that query the DOM tree of the web page

Hulk, *UNISEX SEC'2014*

- Dynamically detect malicious extensions

- Let's trigger the malicious code, which is conditionally executed
  - How?
  - **Intuition**: several malicious extensions activate based on the content of a web page
  - **Idea**: Honey Page (Extension testing page)
  - Dynamically create DOM elements whenever an extension requests certain DOM elements

How to detect maliciousness?

Malicious Behaviors (Bug Oracle)

- Attempt to uninstall other extensions
- Make hard to be uninstalled
  - Dynamically replace or remove that tab `chrome://extensions`
- Remove security request headers
  - `X-Frame-Options` and `Content-Security-Policy`
- Inject keylogger JS code
  - Intercepting every keystroke
- Looking for DOM elements whose name is “`password`”
- Alter outgoing HTTP requests
  - For requests from Amazon pages, the extensions adds parameters that credit a particular affiliation
  - htttp://www.amazon.com/dp/096182570/?tag=affilateID

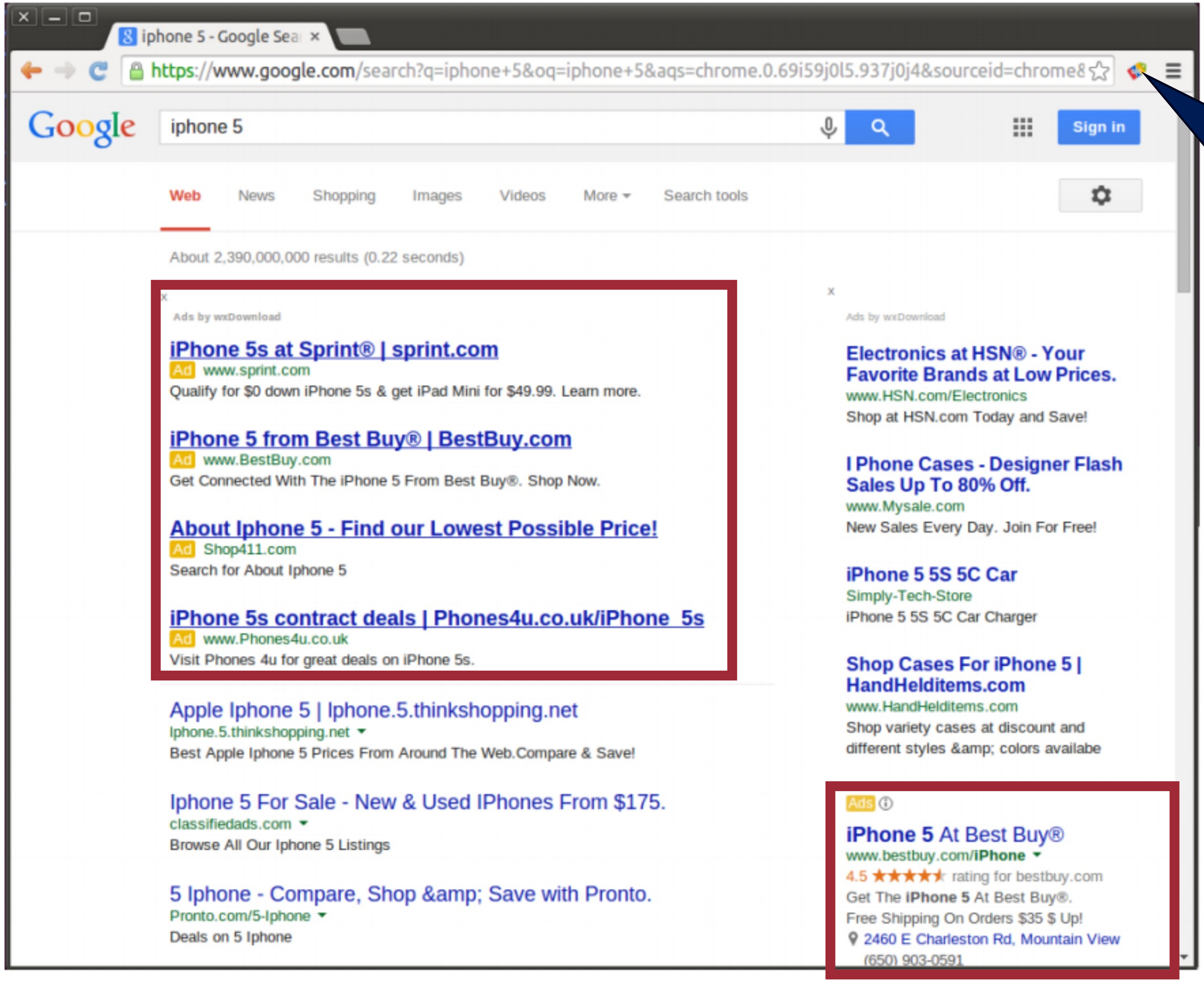
Experimental Results

- Total: 48,332
- **Benign**: 43,490
- **Suspicious**: 4,712
  - Injects dynamic JavaScript
  - Evals with input >128 long
  - Produces HTTP 4xx errors
  - Performs requests to non-existent domains (Why?)
- **Malicious**: 130
  - Ad replacement
  - Affiliate fraud
  - Keylogger
  - Online social network abuse: spams on Facebook account

Limitations

- Difficult to detect extensions that perform **cloaking**
- Searching **coverage**
  - If the extension looks for multiple structural DOM elements, Hulk failed to prepare such DOMs
- Any malicious extension can **detect** whether Hulk is in place
  - Ask for a random DOM element to the honey page
  - If it returns, Hulk is in place

Ad Injection



iphone 5 - Google Sea
https://www.google.com/search?q=iphone+5&oq=iphone+5&aqs=chrome.0.69i59j0l5.937j0j4&sourceid=chrome&
Google
iphone 5
Sign in
Web
News
Shopping
Images
Videos
More
Search tools

About 2,390,000,000 results (0.22 seconds)

x

Ads by wxDownload

iPhone 5s at Sprint® | sprint.com
Ad www.sprint.com
Qualify for $0 down iPhone 5s & get iPad Mini for $49.99. Learn more.

iPhone 5 from Best Buy® | BestBuy.com
Ad www.BestBuy.com
Get Connected With The iPhone 5 From Best Buy®. Shop Now.

About Iphone 5 - Find our Lowest Possible Price!
Ad Shop411.com
Search for About Iphone 5

iPhone 5s contract deals | Phones4u.co.uk/iPhone_5s
Ad www.Phones4u.co.uk
Visit Phones 4u for great deals on iPhone 5s.

Apple Iphone 5 | Iphone.5.thinkshopping.net
Iphone.5.thinkshopping.net
Best Apple Iphone 5 Prices From Around The Web.Compare & Save!

Iphone 5 For Sale - New & Used IPhones From $175.
classifiedads.com
Browse All Our Iphone 5 Listings

5 Iphone - Compare, Shop &amp; Save with Pronto.
Pronto.com/5-Iphone
Deals on 5 Iphone

x

Ads by wxDownload

Electronics at HSN® - Your Favorite Brands at Low Prices.
www.HSN.com/Electronics
Shop at HSN.com Today and Save!

I Phone Cases - Designer Flash Sales Up To 80% Off.
www.Mysale.com
New Sales Every Day. Join For Free!

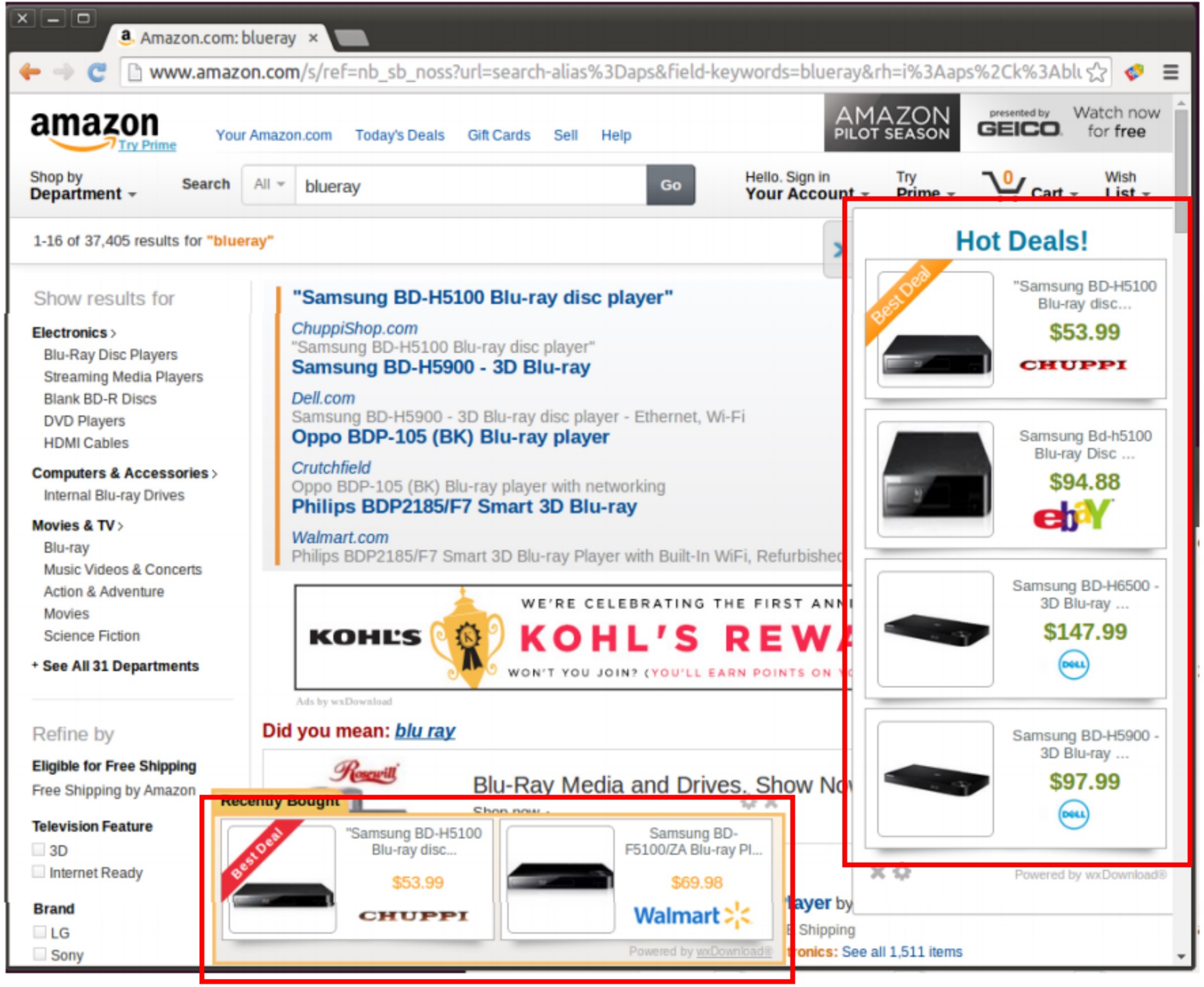
iPhone 5 5S 5C Car
Simply-Tech-Store
iPhone 5 5S 5C Car Charger

Shop Cases For iPhone 5 | HandHelditems.com
www.HandHelditems.com
Shop variety cases at discount and different styles &amp; colors availabe

Ads
iPhone 5 At Best Buy®
www.bestbuy.com/**iPhone**
4.5 ★★★★★ rating for bestbuy.com
Get The **iPhone 5** At Best Buy®.
Free Shipping On Orders $35 $ Up!
2460 E Charleston Rd, Mountain View
(650) 903-0591

Ad injector: Modify a page's content to insert or replace advertisements

Ad Injection



1-16 of 37,405 results for "blueray"

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

KOHL'S
WE'RE CELEBRATING THE FIRST ANN
KOHL'S REWA
WON'T YOU JOIN? (YOU'LL EARN POINTS ON Y

Ads by wxDownload

Did you mean: *blu ray*

Blu-Ray Media and Drives. Show No
Shop now .

Hot Deals!

Best Deal	"Samsung BD-H5100 Blu-ray disc... $53.99 CHUPPI
	Samsung Bd-h5100 Blu-ray Disc ... $94.88 ebY
	Samsung BD-H6500 - 3D Blu-ray ... $147.99 DELL
	Samsung BD-H5900 - 3D Blu-ray ... $97.99 DELL

Powered by wxDownload®

Recently Bought

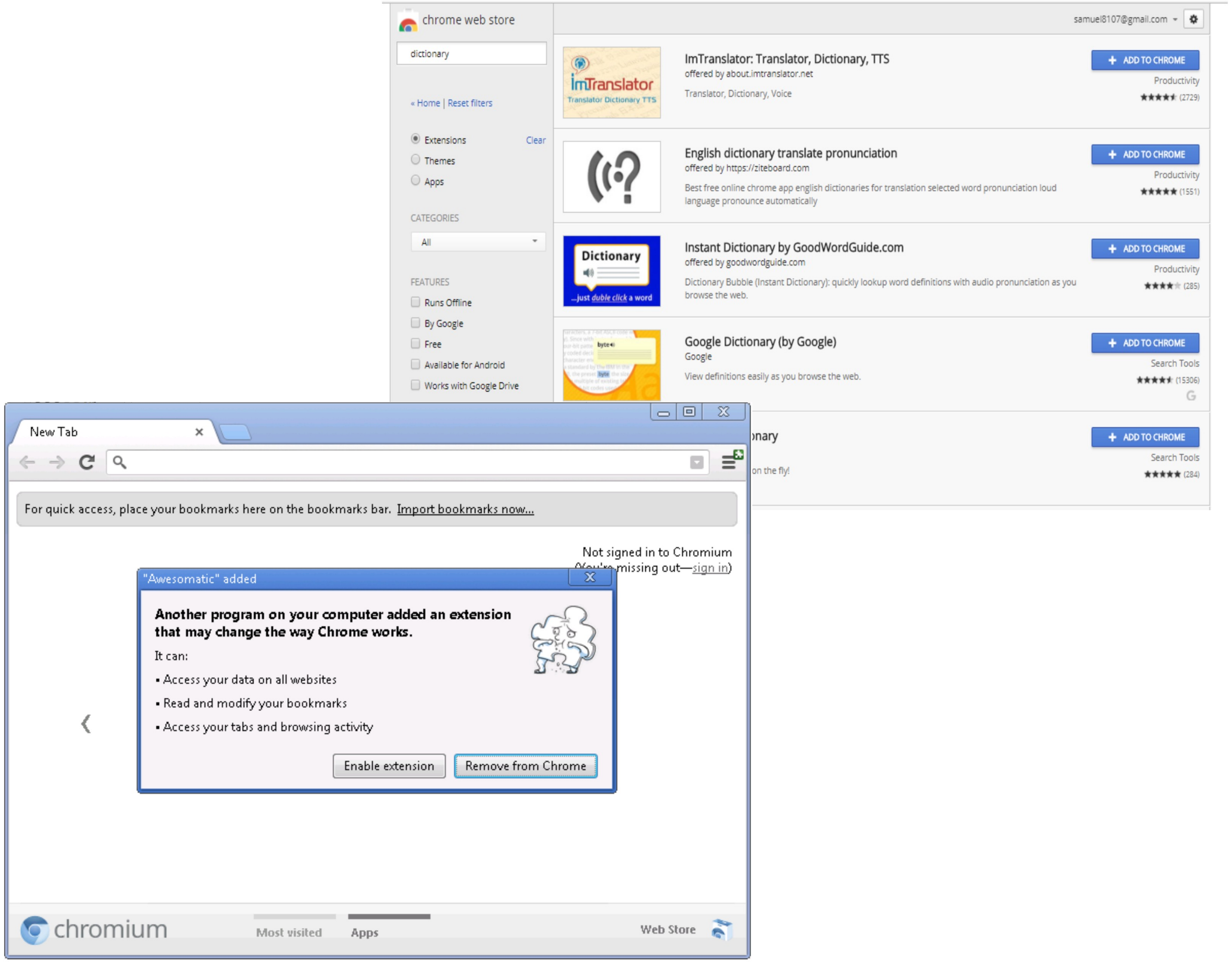
Best Deal	"Samsung BD-H5100 Blu-ray disc... $53.99 CHUPPI
	Samsung BD-F5100/ZA Blu-ray Pl... $69.98 Walmart

Powered by wxDownload®

ayer by
Shipping
ronics: See all 1,511 items

How Are Users Exposed to Ad Injectors?

- Chrome web store
- Sideloading extension
- Malware infection



chrome web store

dictionary

samuel8107@gmail.com

« Home | Reset filters

● Extensions Clear
○ Themes
○ Apps

CATEGORIES

All

FEATURES

□ Runs Offline
□ By Google
□ Free
□ Available for Android
□ Works with Google Drive

ImTranslator: Translator, Dictionary, TTS
offered by about.imtranslator.net
Translator, Dictionary, Voice
Productivity ★★★★★ (2729)

English dictionary translate pronunciation
offered by https://ziteboard.com
Best free online chrome app english dictionaries for translation selected word pronunciation loud language pronounce automatically
Productivity ★★★★★ (1551)

Instant Dictionary by GoodWordGuide.com
offered by goodwordguide.com
Dictionary Bubble (Instant Dictionary): quickly lookup word definitions with audio pronunciation as you browse the web.
Productivity ★★★★☆ (285)

Google Dictionary (by Google)
Google
View definitions easily as you browse the web.
Search Tools ★★★★★ (15306)

nary
on the fly!
Search Tools ★★★★★ (284)

New Tab

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Not signed in to Chromium
(You're missing out—sign in)

"Awesomatic" added

Another program on your computer added an extension that may change the way Chrome works.

It can:

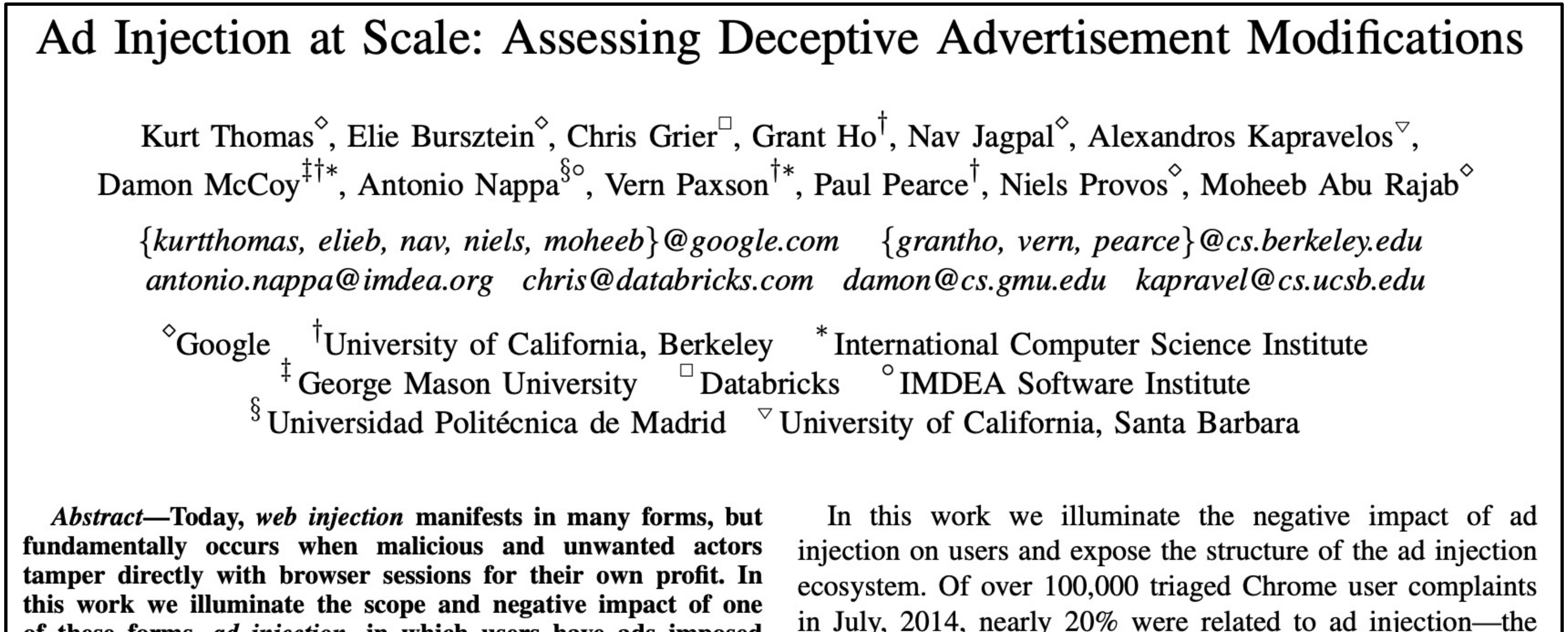
- Access your data on all websites
- Read and modify your bookmarks
- Access your tabs and browsing activity

Is Ad Injector Malicious?

- Why?
  - (**Privacy**) Monitor user’s browser activities for tracking and advertisement selection
  - (**User experience**) Increases page load latency
  - (**User experience**) Overwhelm the original content (spurious “search results” and fly-in banners)
  - (**Security**) Serve spam, malware, phishing
- Who can be damaged from ad injections?
  - **End users**

Ad Injection at Scale, *S&P'2015*

- Identifies ad injection in the wild
- Found 50,870 ad injector extensions, 38% of which are explicitly malicious



Ad Injection at Scale: Assessing Deceptive Advertisement Modifications

Kurt Thomas[◇], Elie Bursztein[◇], Chris Grier[□], Grant Ho[†], Nav Jagpal[◇], Alexandros Kapravelos[▽],
Damon McCoy[‡†*], Antonio Nappa[§○], Vern Paxson[†*], Paul Pearce[†], Niels Provos[◇], Moheeb Abu Rajab[◇]

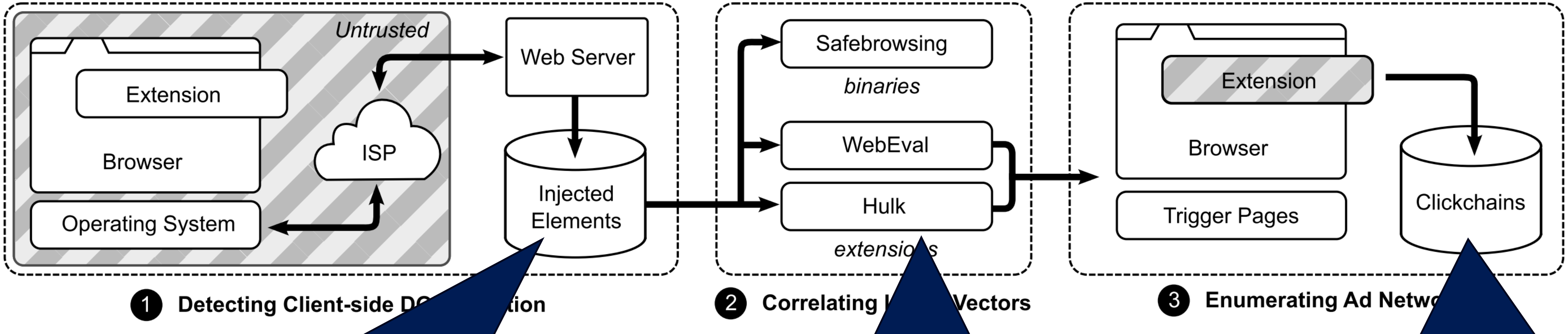
{kurtthomas, elieb, nav, niels, moheeb}@google.com *{grantho, vern, pearce}@cs.berkeley.edu*
antonio.nappa@imdea.org *chris@databricks.com* *damon@cs.gmu.edu* *kapravel@cs.ucsb.edu*

[◇]Google [†]University of California, Berkeley [*]International Computer Science Institute
[‡]George Mason University [□]Databricks [○]IMDEA Software Institute
[§]Universidad Politécnica de Madrid [▽]University of California, Santa Barbara

***Abstract*—Today, *web injection* manifests in many forms, but fundamentally occurs when malicious and unwanted actors tamper directly with browser sessions for their own profit. In this work we illuminate the scope and negative impact of one of these forms, *ad injection*, in which users have ads imposed**

In this work we illuminate the negative impact of ad injection on users and expose the structure of the ad injection ecosystem. Of over 100,000 triaged Chrome user complaints in July, 2014, nearly 20% were related to ad injection—the

Large-scale Ad Injection Investigation, *S&P'2015*



Identify injected DOM elements by JS

- Compare between Injected VS. untampered version

Identify extensions

- Static Analysis
  - Manifest permissions, Access to Cookie, Age of the extension, Developer reputation, …
- Dynamic Analysis
  - Capture all Chrome API calls, DOM method calls, network requests, …

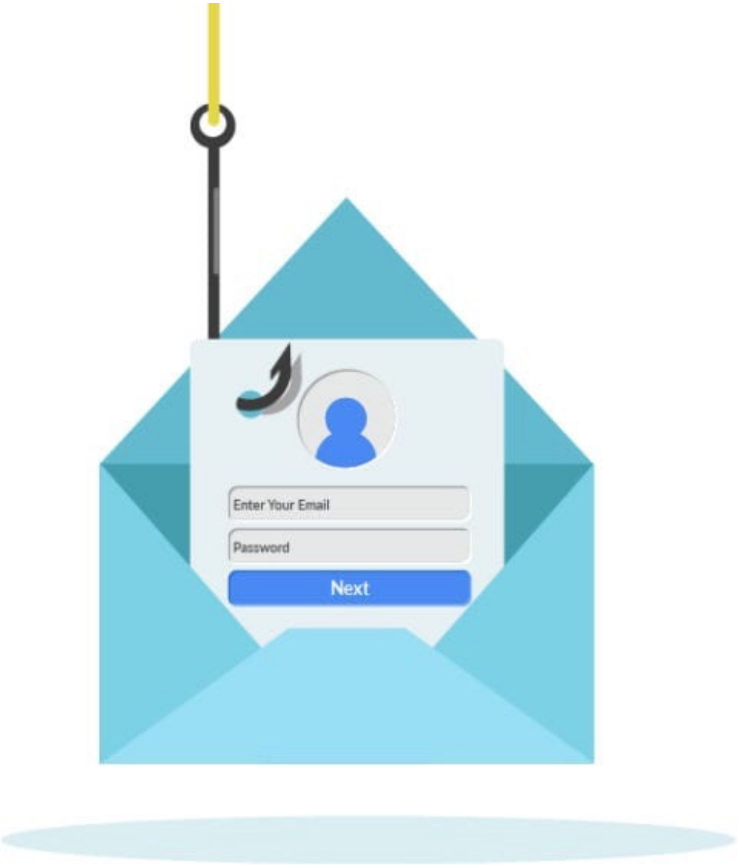
Execute them to click on the injected ad

- Harvest advertisement revenue clickchains

Limitations

- The data is only from Google website
- Cloacking

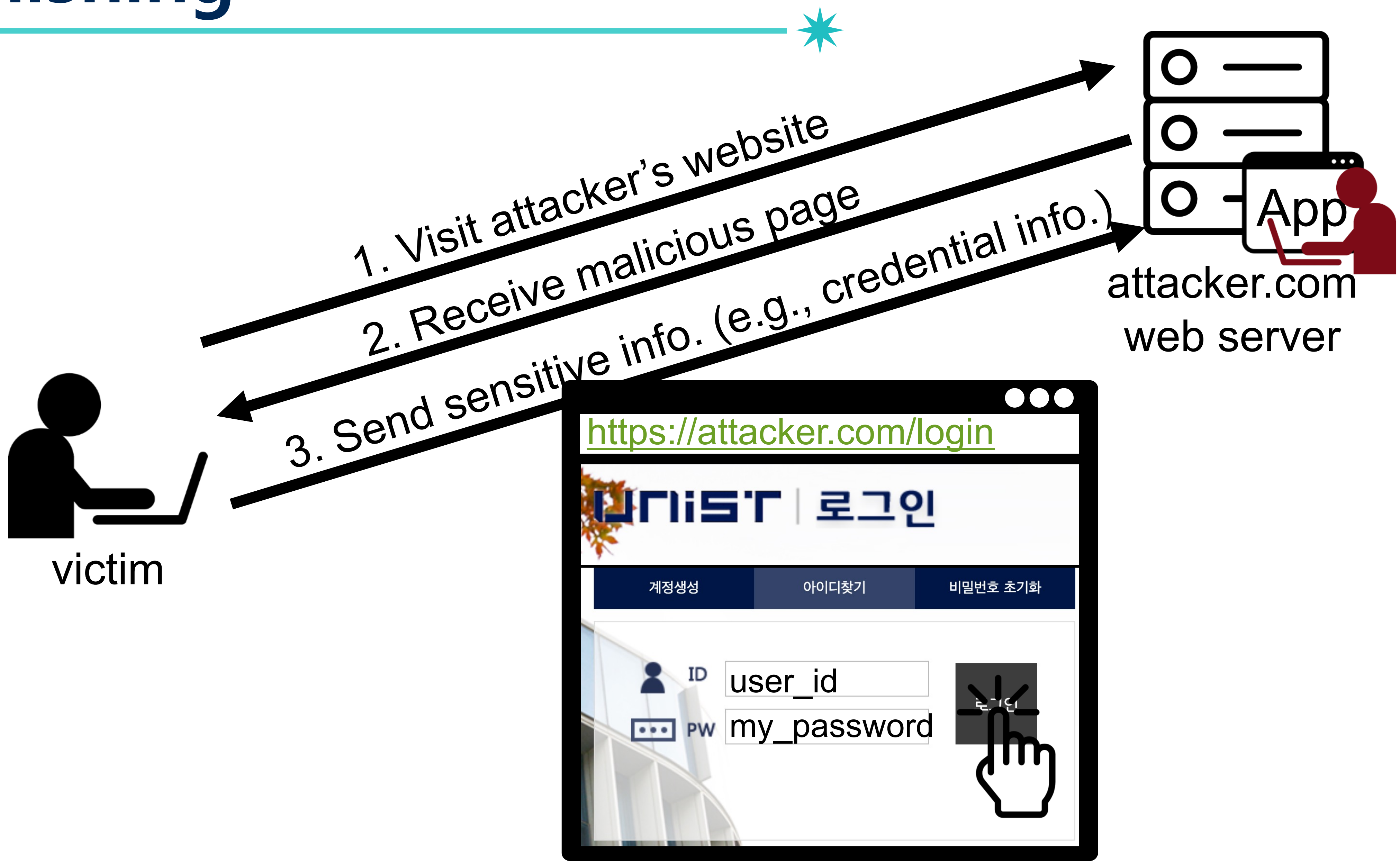
Phishing



Phishing

- Disguising as a trustworthy entity, and obtain private information
  - Login credentials
  - Financial records

Phishing


1. Visit attacker's website
2. Receive malicious page
3. Send sensitive info. (e.g., credential info.)
victim
App
attacker.com
web server
UNIST | 로그인
계정생성
아이디찾기
비밀번호 초기화
로그인

https://attacker.com/login

ID user_id

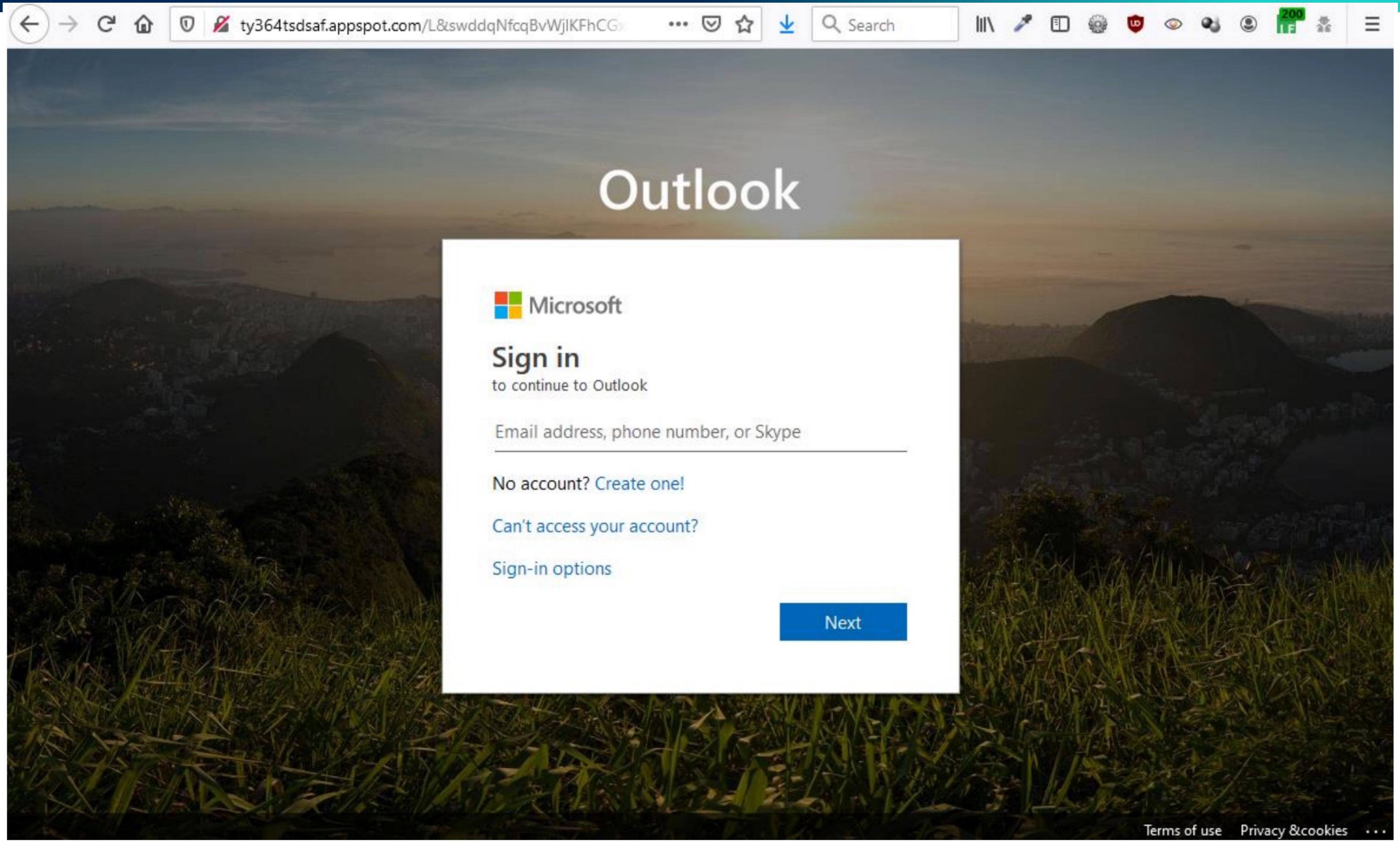
PW my_password

Phishing

- Disguising as a trustworthy entity, and obtain private information
  - Login credentials
  - Financial records

- Links to phishing webpages dispatched to victims through email or SMS

- According to a report from the FBI, it received 800,944 reports of phishing, with losses exceeding $10.3 billion in 2022



Outlook

Microsoft

Sign in

to continue to Outlook

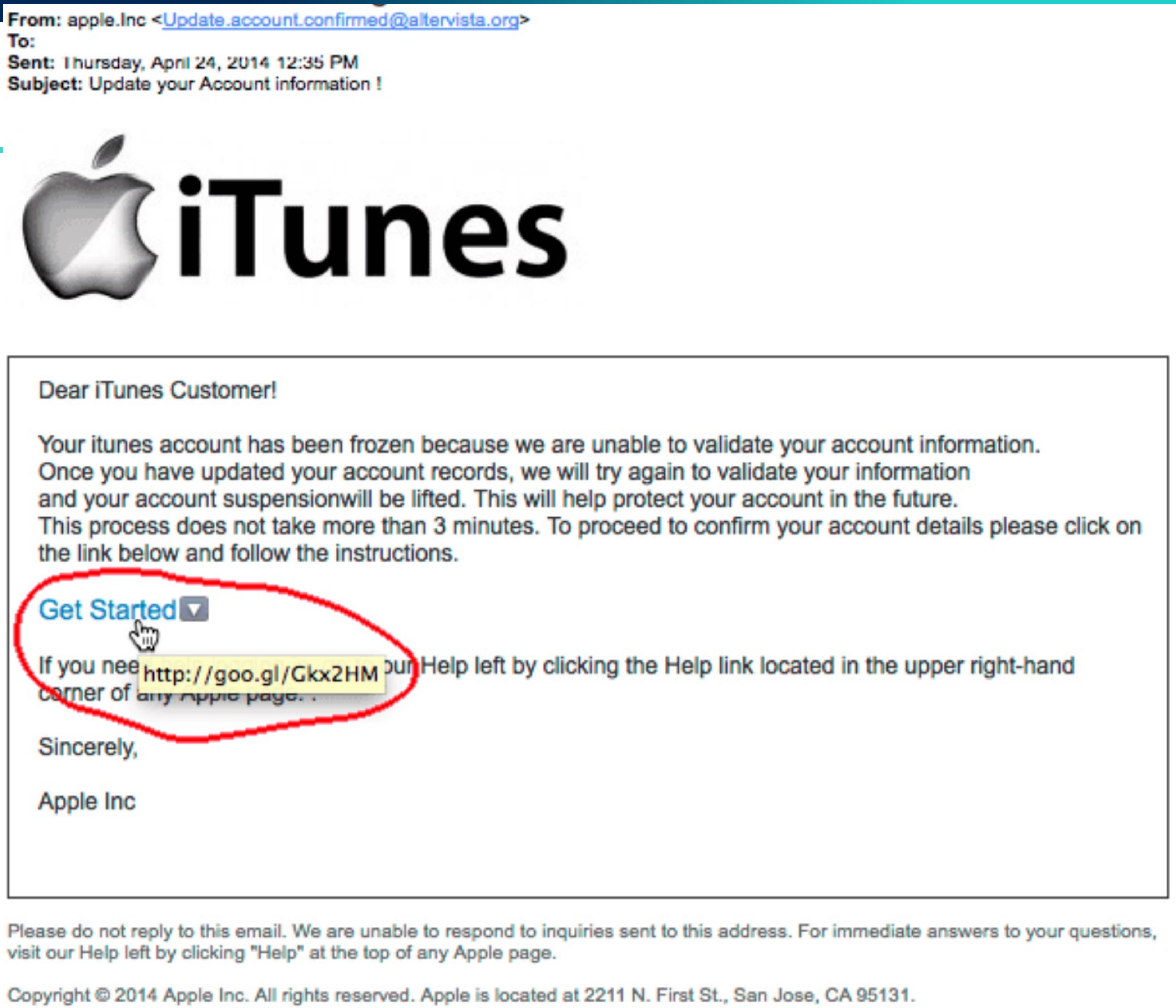
Email address, phone number, or Skype

No account? Create one!

Can't access your account?

Sign-in options

Phishing



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information.
Once you have updated your account records, we will try again to validate your information
and your account suspensionwill be lifted. This will help protect your account in the future.
This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

http://goo.gl/Gkx2HM

If you nee our Help left by clicking the Help link located in the upper right-hand corner of

Sincerely,

Apple Inc

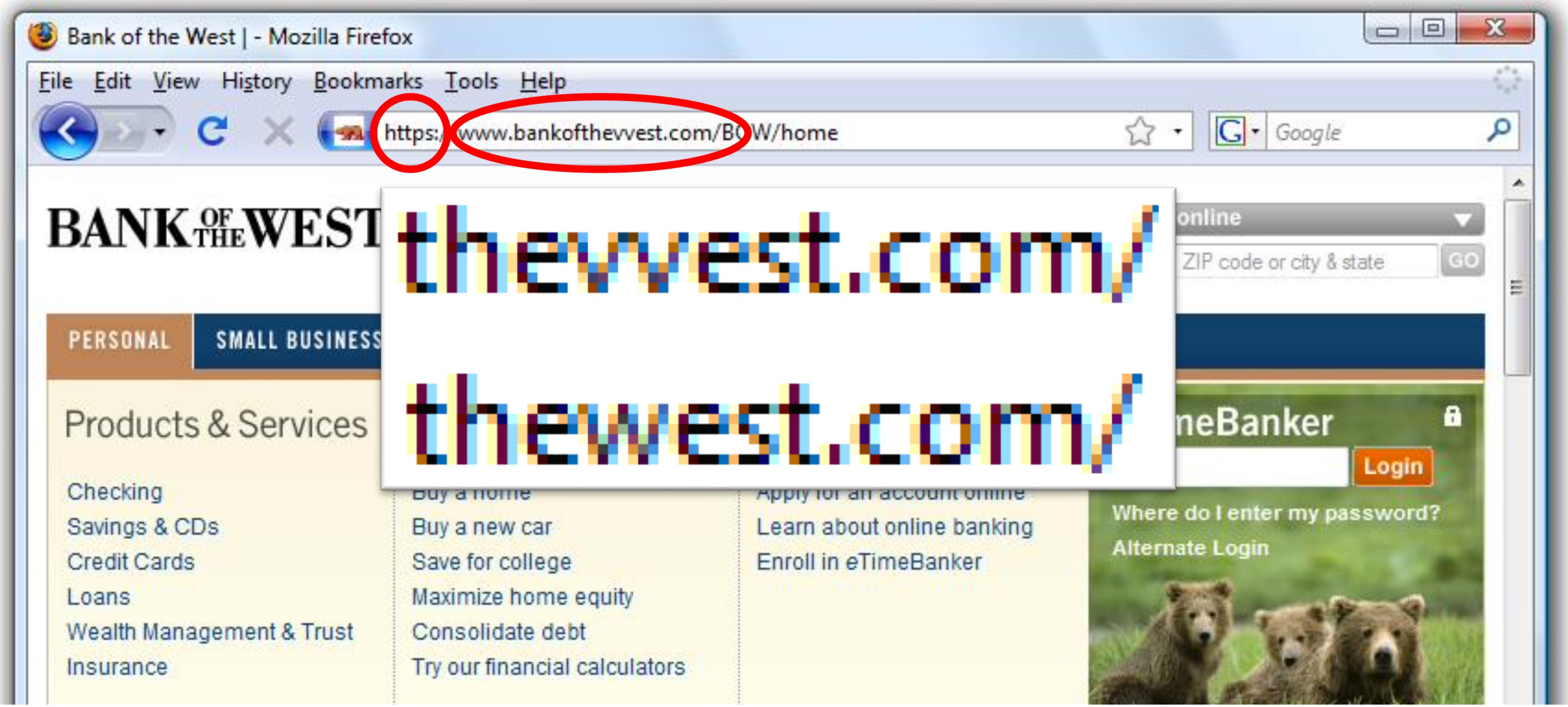
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

Typical Properties of Spoofed Sites

- Attackers manually copy/recreate web content from target website
  - Show logos found on the honest site
- Have suspicious URLs: mostly, being camouflaged as a URL that looks familiar to people
  - E.g., umist.ac.kr
- Ask for user input
  - Debit card number, username, password, …
- Phishing content served from attacker-owned web server
  - Or a compromised web server

Safe to Type Your Password?



Bank of the West | - Mozilla Firefox

Products & Services

Checking
Savings & CDs
Credit Cards
Loans
Wealth Management & Trust
Insurance

Buy a home
Buy a new car
Save for college
Maximize home equity
Consolidate debt
Try our financial calculators

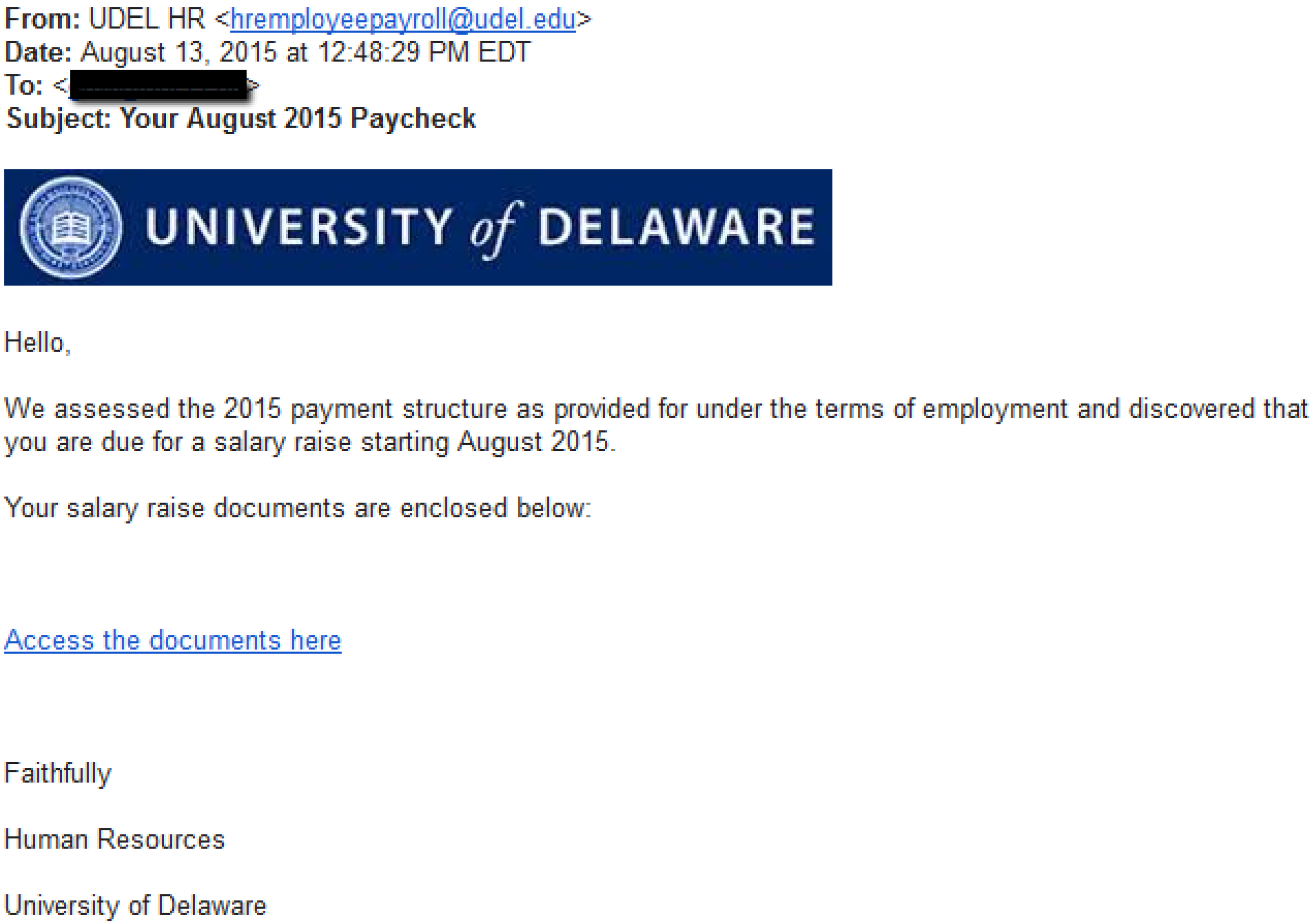
Apply for an account online
Learn about online banking
Enroll in eTimeBanker

Where do I enter my password?
Alternate Login

Spear Phishing

- Phishing attempts directed **at specific individuals**
- This can increase the likelihood of success, as the sender appears more credible and informed

Spear Phishing



From: UDEL HR <hremployeepayroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: <[redacted]>
Subject: Your August 2015 Paycheck

UNIVERSITY *of* DELAWARE

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

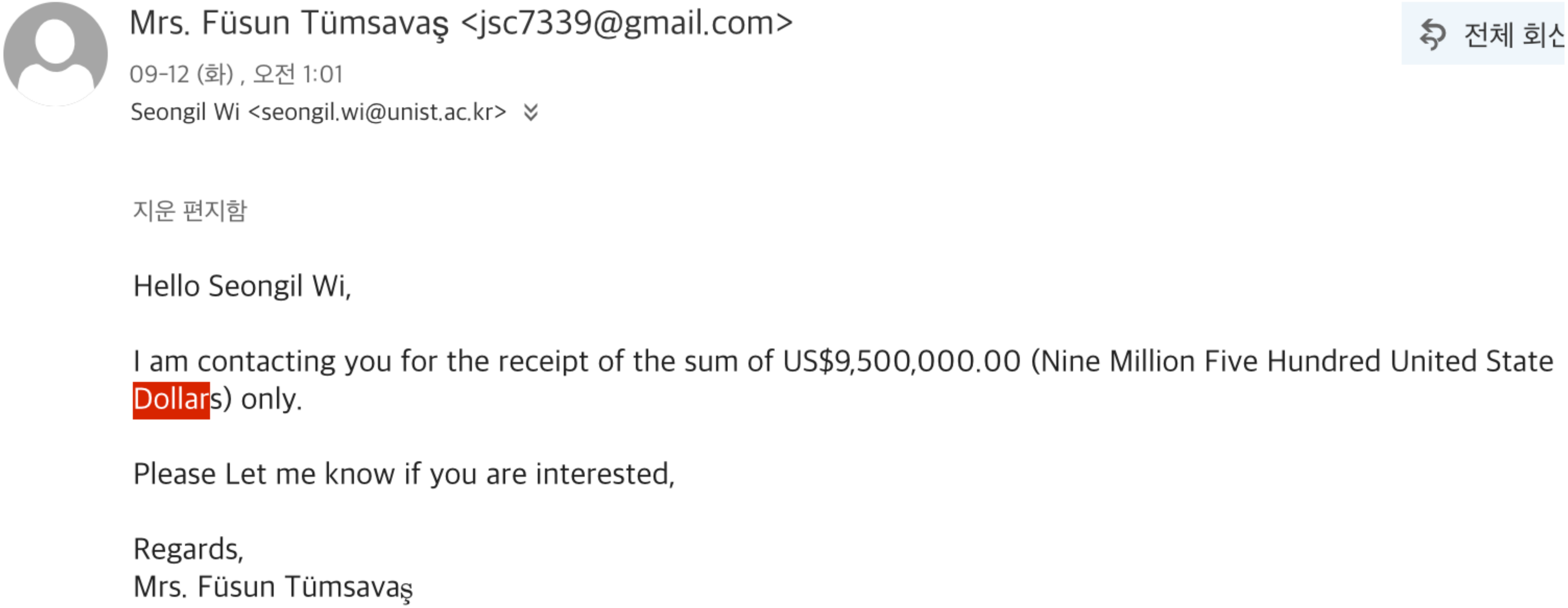
Access the documents here

Faithfully

Human Resources

University of Delaware

Spear Phishing



Mrs. Füsun Tümsavaş <jsc7339@gmail.com>

09-12 (화) , 오전 1:01

Seongil Wi <seongil.wi@unist.ac.kr>

지운 편지함

Hello Seongil Wi,

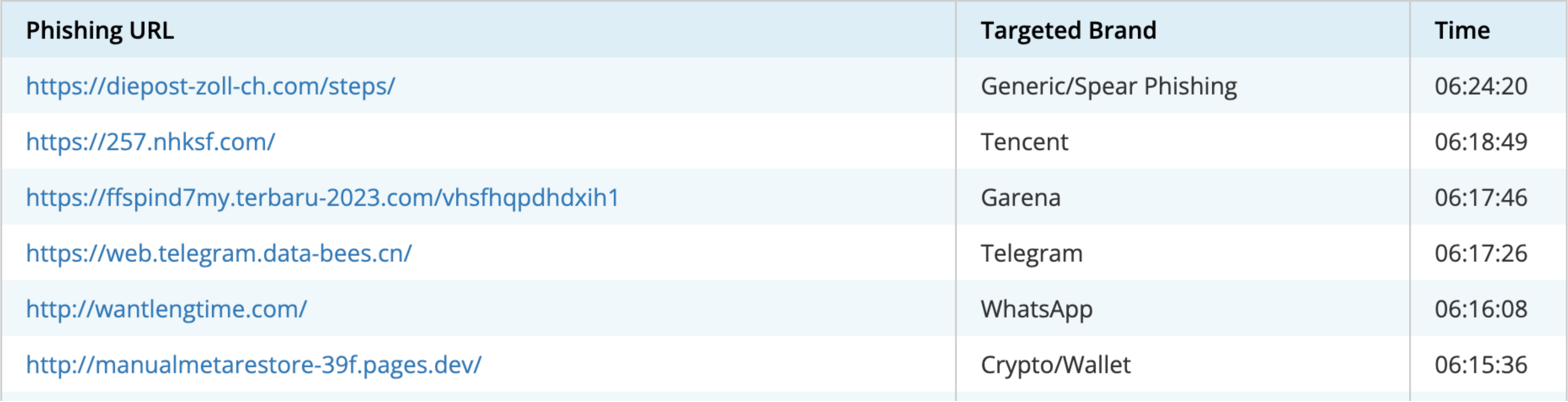
I am contacting you for the receipt of the sum of US$9,500,000.00 (Nine Million Five Hundred United State Dollars) only.

Please Let me know if you are interested,

Regards,
Mrs. Füsun Tümsavaş

How to Detect Phishing?

- Crowdsourcing, Blacklisting
  - lists reported phishing URLs
  - E.g., https://openphish.com/



Phishing URL	Targeted Brand	Time
https://diepost-zoll-ch.com/steps/	Generic/Spear Phishing	06:24:20
https://257.nhksf.com/	Tencent	06:18:49
https://ffspind7my.terbaru-2023.com/vhsfhqpdhdxih1	Garena	06:17:46
https://web.telegram.data-bees.cn/	Telegram	06:17:26
http://wantlengtime.com/	WhatsApp	06:16:08
http://manualmetarestore-39f.pages.dev/	Crypto/Wallet	06:15:36

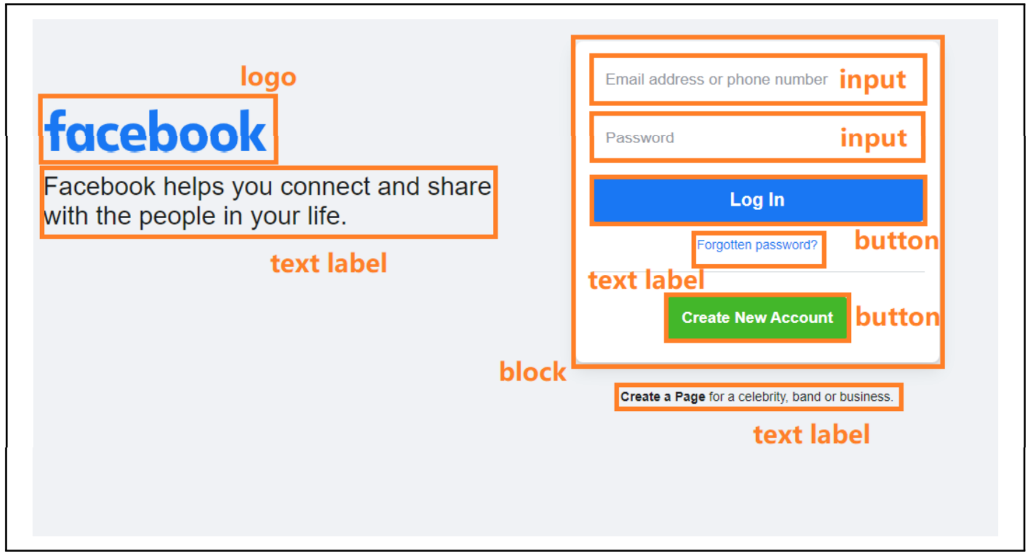
How to Detect Phishing?

- Crowdsourcing, Blacklisting
  - lists reported phishing URLs
  - E.g., https://openphish.com/

- Require human intervention and verification
- Phishers are starting to use one-time URLs

- URL-based pattern detection
  - E.g., A URL is phishy if its length ≥ 76
  - E.g., Brand name modification with ‘-’
    - youtube-x.com

- Content-based pattern detection


logo
facebook
Facebook helps you connect and share with the people in your life.
text label
Email address or phone number
input
Password
input
Log In
button
Forgotten password?
text label
Create New Account
button
block
Create a Page for a celebrity, band or business.
text label

Question?