Article

Modern Cyber Attacks on the Web

Anastasiia Tilniak, Antónia Zsófia Márton, Khalil Abdellah Lemtaffah, Richard Faragó and [redacted]

Abstract: In today's digital world, malefactors' illegal actions are aimed at financial, legal, healthcare, retail, as well as biopharmaceutical and biotechnology organizations. The purpose of the study was to identify existing shortcomings in the level of web security and form recommendations for eliminating users risks. This paper describes the use of distant cyberattacks in order to obtain data for logging into people's accounts or organizations on various platforms by using popular social networks or mail. This is considered one of the smartest phishing methods to date, which creates a window inside the browser frame that is indistinguishable from a fake one. The difference can be seen by a cybersecurity professional, but not by the average user or office worker. To deal with the Browser In The Browser (BITB) Attack, the research has created a tool that looks for the script used for the attack, if any, and only blocks it so that websites can continue to function correctly. The research also conducted an anonymous survey in which 4,000 people took part. From the survey, it was concluded that the method created as a result of this investigation is the best measure to counter attacks on the web and prevented (88.37%) attacks.

Keywords: Cybercrime, Cyber-attacks, Cybersecurity, Web Services Security, Web-attacks, BITB

1. Introduction

This paper elaborates a new web-based attack and propose a potential countermeasure. The effectiveness of countermeasures through surveys is also analyzed.

Phishing is the most impactful attack in the cybersecurity world, it can make big organizations and companies pay a lot of money in return. Advanced attacks and malwares rely on sophisticated phishing techniques to succeed. In addition, ransomware is often used to block confidential documents and files of the entire organization, demanding a large amount of money as a ransom, all hacked in case of non-payment.

Modern cyber attacks on the web use various methods and forms to achieve the goal of making the victim fall into the attacker's trap. Mentioning "modern attacks" means judicious use of web programming languages. Javascript combined with some CSS styling and html injections can be used as a great way to perform attacking techniques and phishing methods. After falling into the trap, the next step which is controlled by the attacker's algorithm is going to be executed, either the victim's system is going to be infected by a certain harmful malware, or his credentials are going to be sent to the hacker in either ways, where the latter one can use them to takeover the victim's account or impersonate his privileges.

This paper covers one of the smartest phishing techniques to date, which is the creation of a window inside the browser's frame to make it look like another legitimate window, where the user cannot distinguish the difference between a fake window and a regular one. Definitely, someone who is a professional in their field can notice the difference, but not the average user or everyday employee.

The research relied on the work of S. William, M. Baykara, Z. Gurel, E. O. Yeboah-Boateng, P. M. Amanor, etc. The investigation has shown that cybercrime is also rapidly evolving, and presents scientists with new challenges and problems. As a result, a “manual approach” was used to identify vulnerabilities, and also relied on expert analysis. To deal with the Browser In The Browser (BITB) Attack, the research has created a tool that looks for the script used in the attack, if any, and only blocks it so that website can continue to function correctly.

2. The reason behind the attack

In this section describes what is the motive and purpose of cybercrime, and also considers the legal aspects of preventing such crimes.

2.1. What is an attacker target?

According to data provided by the Atlas VPN team, "86% of hacked Google Cloud accounts are used for illegal mining"[1]. This is more than half of all remaining cases, including malicious port scanning, cyberattacks, malware hosting and others.

Nowadays, malefactors' illegal actions are aimed at financial, legal, healthcare, retail, as well as biopharmaceutical and biotechnology organizations. This paper considers the use of cyberattacks in the web in order to obtain data for logging into the accounts of people or organizations.

2.2. What is the intention?

Having gained access to the data, an attacker can use it for any illegal purposes: from damage to the reputation of a person/organization, to obtaining benefits by debiting funds from accounts or for ransom. Summing up, we understand that attackers can have two goals of attacks: damage to the reputation of a person or organization, and also for the purpose of illegal enrichment. Attacks for the purpose of illicit enrichment are among the mass hacker attacks, when many people or organizations are attacked at the same time, and the least protected users become victims. At the same time, attacks aimed at damaging the reputation of a person or organization are targeted attacks, which are usually well planned and include several stages: from reconnaissance and infiltration to the destruction of traces of presence.

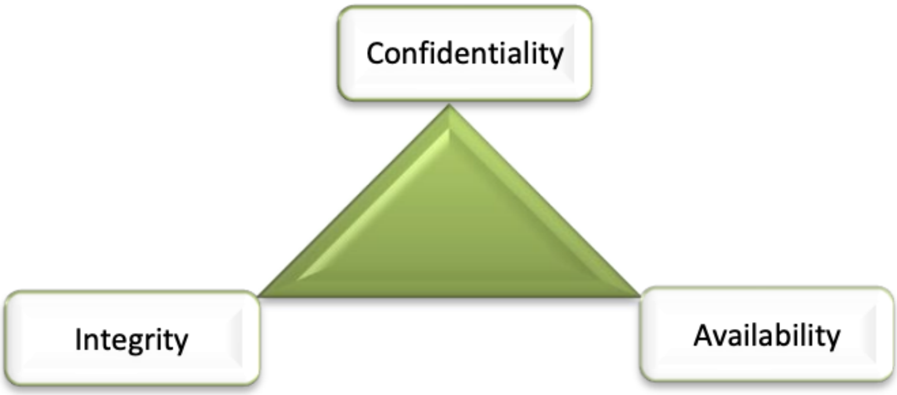


Figure 1. The triad model of the United Nations system organizations[1]

2.3. *What is known about cybercrime today?*

In today's digital world, cybersecurity has become an important issue for international organizations. Many scientists and experts in the field of cybersecurity devote hundreds of scientific papers to preventing all kinds of attacks. Today we have unlimited access to all sorts of resources that explain in a structured way any processes in the field of information security. These include data from the United Nations, the Cybercrime Prevention Act of 2012, International covenants in Financial, Corporate and Criminal law. But we also need to understand that at the moment there is no single international treaty prohibiting cyberattacks.

For example, the National Institute of Standards and Technology of the United States of America created the information security triad model [1], which is considered a reference model, designed to regulate and evaluate how an organization handles data when it is stored, transmitted or processed.

According to the United Nations, in today's reality, no organization in the system can claim that it has not been subjected to some form of cyberattack of greater or lesser severity. Malicious actions directed against users of information systems (such as phishing, identity theft, interception of a communication channel, etc.) or infrastructure (malware, distributed denial of service attacks, etc.) are currently the most common source of known threats.

By the end of this part, it should be concluded that a cyberattack is a clear threat not only to any corporations, but also to individuals. Threat trends vary by environment, so it's important to be aware of changes in information technology, services, controls, and behavior over time. In this article, we will consider an example of a modern cyberattack on the web, which can be a victim of any of us.

3. Initialization

This section introduces ways cybercriminals can succeed in deceiving or luring victims in the online world. These ways represent the initial steps of a BITB attack, which mainly consists of redirecting the user to a clone of a legitimate website or other fabricated platforms that involve shopping deals, job opportunities or news, that might appear interesting to the public.

3.1. *Methods*

Along with the modern frameworks and libraries, the bugs on the other hand arise to appear with those changes, the famous quote of "everything is vulnerable" applies 100% to this area. Vulnerability

[1] Source: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

databses such as Snyk[2], which is a great updated database for vulnerabilities in most updated libraries and packages.

The Figure 2 shows a code snippet of how BITB (Browser In The Browser) redirects the victim to a phishing window and takes control of his SSO (Single Sign On) credentials, or anything else.

In this code snippet, the `return false` will make sure that when the user hovers over the infected button, he will not have an idea about which link he is going to be redirected to after clicking on it. And indeed this is considered advanced technique to trick the user and do not give him a hint about the phishing trap.

The first approach is called Spear Phishing [2] [3], which is a targeted phishing method. This requires prior knowledge of the target, such as personal information and contact details, which are freely available on the internet, mostly on social media websites. After a significant portion of data is obtained the fraudster can tailor a personalized email, which improves the probability of the user falling into the trap of clicking the malicious link provided inside the email.

The second practice is called Smishing [4], which is really similar to the first method, except it uses SMS instead of email as its communication channel, which makes people more likely to trust the content they receive.

The third technique is connected to content injection regarding websites that are vulnerable to SQL injection and XSS[3] [5]. The attacker changes the content of the reliable web page using the aforementioned vulnerabilities by inputting harmful JavaScript code with additional HTML and CSS elements to make it look legitimate.

The last two methods are known as link manipulation and web push technology [6]. The former incorporates a deceptive link, which name does not match the website it opens. The only way to check its legitimateness, other than clicking it, is hovering the mouse over it to view the real address. Finally, the latter method allows using modern web browser notifications to trick the users.

3.2. The flow of the attack

A person wants to login to his account using a SSO service, say Google for example. Suppose the victim fell into the trap and he clicked on a malicious button, that will show the browser in the browser (BITB) dialogue. Here the attacker already got all the details of the victim including his IP address, his user agent, which browser he is using and so on... So even if the victim does not enter his details into the phising form, targeting him in the future will be a piece of cake to the attacker.

The next step is to show the tricky browser, and here it depends on many factors such as which operating system the user is running, or which mode is used (dark/light), which browser, etc. But this can be concluded on previous assessments. Now the victim will see a pop up inside the frame of the infected website, which appears exactly like another window from the browser, in fact, it is not. It is just another frame inside the website, made using some JavaScript lines and decorated using HTML and CSS.

[2] Source: https://security.snyk.io/
[3] Cross-Site Scripting

```
<a href="https://gmail.com" onclick="return launchWindow();">Google</a>

function launchWindow(){
    // Launch the fake authentication window
    return false; // This will make sure the href attribute is ignored
}
```

Figure 2. Code snippet of how BITB redirects the victim to a fishing windows.

Depending on the victim, most of the times it is very hard to notice the difference, and there is a high chance the user will then enter his credentials just like it is Google who is asking for it. Hiding evidence that this is an attack is much easier to do by returning a False statement at the end of the JavaScript function, in order to hide the URL name of the `href` attribute, while hovering over the malicious button, as was demonstrated in the introduction's code snippet.

Now all the attacker has to do is wait for the victim to enter his credentials and click on the login button, then he will get the information of the user in plain text.

If it is a campaign then the attacker can setup a server in the cloud to collect each pingback from the victims that received the link.

In the end, everyone can avoid this by not clicking on questionable links, and by setting up two-factor authentication for all accounts to add an extra layer of security. These actions ensure that you do not lose access to your account, even if you have previously been phished or leaked.

4. Implementation

In this section describes how this type of attack is implemented.

4.1. How to setup the server?

In order to receive all the callbacks from the affected victims, the attacker needs to have a running server to collect the information. There are many ways to perform this, one of them are:

- Setting up a VPS server in one of the cloud providers
- Building a local server and exposing it to the internet
- Setting up a local server in a private network (wifi, vpn...)
- Building a Raspberry pi architecture

As part of the study, a local server was created inside a virtual machine on which an instance of Kali Linux will be launched. To speed things up, the research used an automated phishing tool with 30+ templates from Github, called Zphisher[4], to spin up a web server and build a phishing page.

4.2. How to develop the phishing page?

There are many resources on the Internet on how to create a web page, but for this paper, but this research does not require any knowledge of programming to create a web page that looks like the one we want to model. For example, the Zphisher tool comes with a set of login pages and other interfaces that can be included in an investigative phishing campaign. BITB focuses mainly on the use of single sign-on technology, so the priority of this article will be on the login pages of mainly well-known companies such as Google, Microsoft, Apple and Facebook.

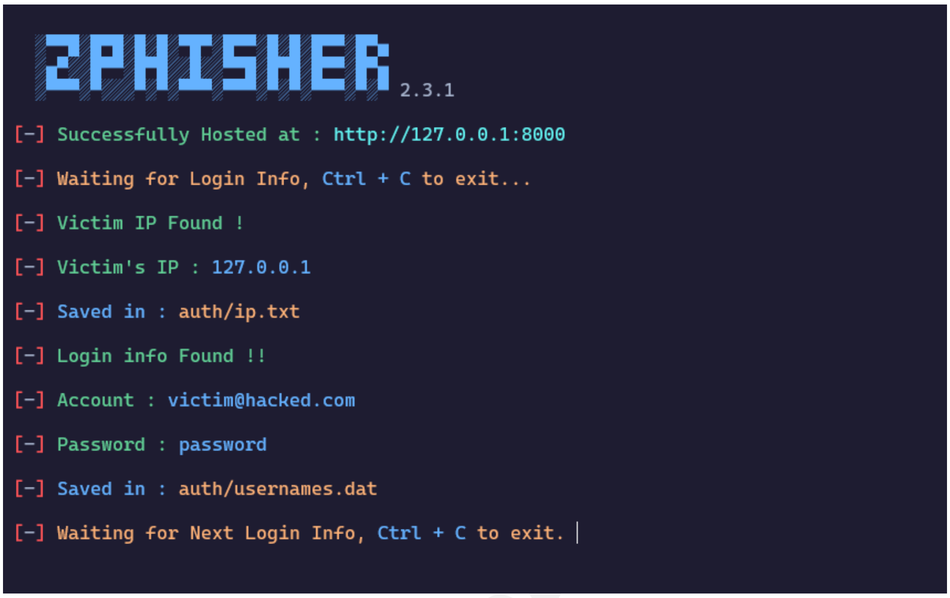
In the other hand, for advanced red teaming operations, will require some advanced techniques so that the victim will not have any chance to make a difference between a real and a fake SSO page. Most of the cases, the red teamers or black hat hackers assign this task to an experienced person who knows how to build a proper webpage.

4.3. How to get the information from the browser?

The first thing an attacker need to know about his victim is the environment he is using. The attacker should ask himself the following questions:

- Is the victim connected from a laptop or a smartphone?
- What is his Operating System?
- Is he using dark or light mode?

[4] Source: https://github.com/htr-tech/zphisher



```
ZPHISHER 2.3.1
[-] Successfully Hosted at : http://127.0.0.1:8000
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : victim@hacked.com
[-] Password : password
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. |
```

Figure 3. Commandline prompt of the Zphisher tool shows the start-up of the server and every victim's detail, who connects to the phishing server.

- Which browser he is surfing on?

These are the most important questions the attacker needs in order to perform a proper Browser In The Browser attack. Luckily again, Zphisher comes with a handy utility (see Figure 3.) that fetches the victim's information and stores it in a file, such as the IP address and the User-Agent of the browser. This will let the attacker know whether he should send the Windows or the MacOS version of the browser, and whether he should include the light or dark mode version of it. This is useful for the window header so that the victim will not notice that it is a fake one or not.

5. Defense

Effective procedures need to be known that can be used to detect and avoid an attack so that adequate protection can be developed to protect sensitive data.

5.1. Detection of BITB attack

The Browser In The Browser (BITB) Attack is almost impossible to detect for a poorly educated user in the field of IT.

So far phishing attacks begin with an email that contains a link to a fake website. This website looks almost the same as a real site, however, by looking at the site's URL it can be detected as fraudulent. The web addresses used for phishing websites may appear the same as the web address of a real site at first glance, but those do not hold up under scrutiny.

With this new BITB method, the generated fake browser window (see Figure 4.) can contain the exact web address of a legitimate website. After examining the URL, the user cannot be convinced whether we are under attack or not, which is why this type of attack is so hard to detect.

Now the question is how a user can notice the attack or see the difference between real and fake pages. Users can detect fraud by moving the window because the generated fake window is not as interactive as the real one. Unfortunately, with some JavaScript and JQuery skills, the attacker can create a sufficiently interactive, demonstrative interface for the average user. Therefore, this is not a suitable solution either.

Until now, the only effective solution to avoid the attack was to disable JavaScript, but in today's world, their use is indispensable for the operation of most websites.

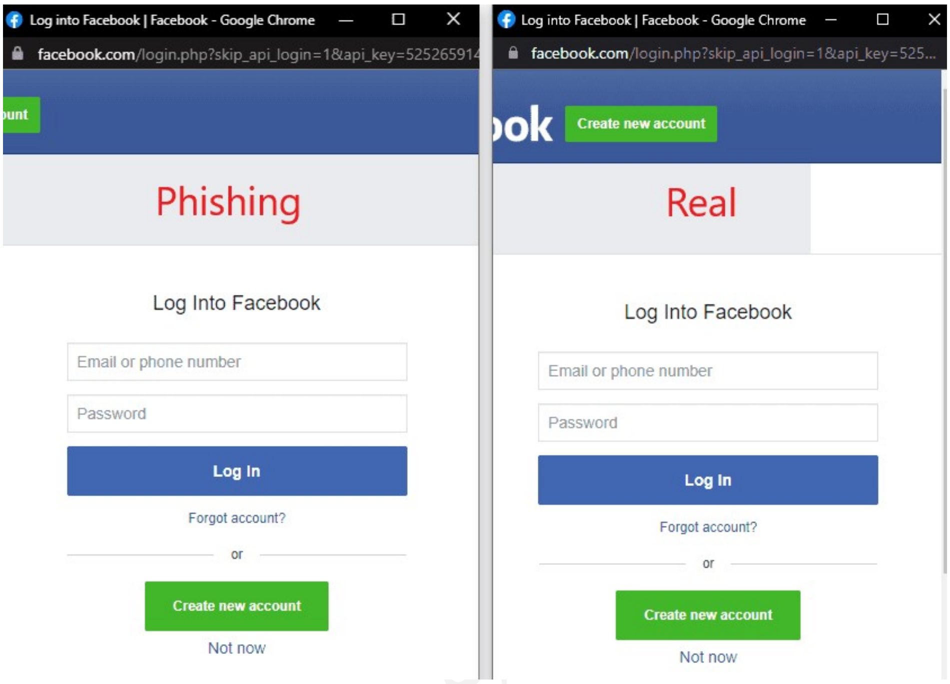


Figure 4. The figure illustrates a fake and a real Facebook SSO login page.

Algorithm 1: Algorithm `detectBITB` implemented in the browser extension. It is for finding malicious HTML and JavaScript code in the source of the web page which could be a potential BITB attack component. The `hasMaliciousPattern` function checks whether the source code of the given element matches potential patterns or not.

```
function detectBITB ($htmlDocument$);
Input  :Source code of the web page $htmlDocument$
Output:True - detected malicious pattern, False - no detection of malicious pattern
for $element$ in $htmlDocument.listOfElements$ do
    if $hasChildren(element)$ then
        return $detectBITB(element)$;
    end
    return $hasMaliciousPattern(element)$
end
```

5.2. *New user-friendly browser extension solution*

The existing tools were combined and improved to achieve the most user-friendly defense. This browser extension solution applies the option of partially disabling JavaScript. It can be easily used from reliable sources by any user so they do not have to install packages on their computers from unknown sites. Installation packages can also contain computer viruses.

There is already an existing add-on Extension for Firefox called Disable JavaScript, but it provides only ability to disable JavaScript for specific sites or specific tabs. This extension was improved by a searching function, which uses the Algorithm 1 to identify malicious code, so the new defense method can find the script used for the attack, if there is any, it blocks JavaScript only in the specific part of the web page so the website can continue functioning properly.

6. Survey

To compare the effectiveness of the proposed protections, it is worth analyzing the result obtained in the form of anonymous surveys. The surveys are aimed at employees of an international company. The name of the company is not disclosed by mutual agreement.

4,000 employees selected for the experiment, which consists of approximately 10% of the total number of employees in the company. All selected employees have been asked to fill out a form to agree with taking the survey (phrased as a non-intrusive internal testing of cybersecurity). If an employee declined the survey, another employee was randomly selected to accept the role. Then these 4,000 employees are randomly distributed into four groups, where each group has 1,000 employees.

- Group A is the control group. The SSO browser presented to employees in group A is benign.
- Group B is presented with a malicious SSO browser without any defense mechanism.
- Group C is also presented with a malicious SSO browser. However, group C is informed of the existence of such attack methods.
- Group D is also presented with a malicious SSO browser. However, group D is informed of the new browser extension defense method one week before the attack.

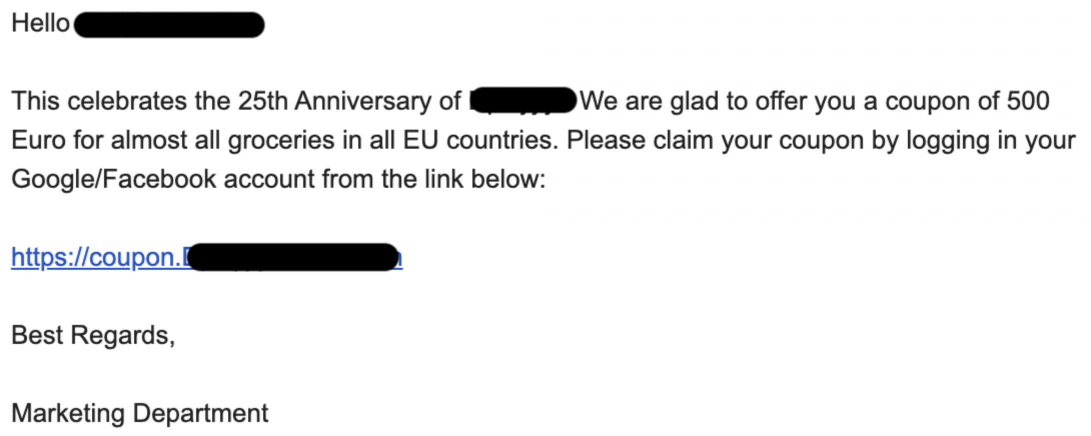
The SSO login screen is prepared as in the above description. The attack initiates as an email, sent from the company's marketing department. The sample email can be seen on Figure 5.

Masqueraded as a grocery coupon, by clicking the link, the user is prompted to a website of coupon claiming, with only two SSO login options: Google and Facebook. After clicking the SSO login button, the user is prompted to the SSO screen (either benign or malicious).

The attack is successful if the user enters their username and password and clicks the login button. The following table shows the number of successful attacks. The poll only records whether the attack was successful or not. The survey never records actual user inputs, which is in line with respect for privacy.

Group A	Group B	Group C	Group D
789	765	567	89

The result of the survey clearly reflects the effectiveness of each defense method. The number of successful attacks was reduced by $1 - 567/765 \approx 25.88\%$ by informing the users of the BITB attack. Using the browser extension solution as the defense method, the number of successful attacks was reduced by $1 - 89/765 \approx 88.37\%$. There is no significant difference between a benign SSO and a malicious SSO when no defense measure is imposed.



Hello [redacted]

This celebrates the 25th Anniversary of [redacted] We are glad to offer you a coupon of 500 Euro for almost all groceries in all EU countries. Please claim your coupon by logging in your Google/Facebook account from the link below:

https://coupon.[redacted]

Best Regards,

Marketing Department

Figure 5. The figure shows a phishing email with a fake website link.

7. Conclusion

Cybercrime has become more sophisticated, and security has become synonymous with reputation. After all, if personal data gets to the offender, the most unpleasant consequences can be expected. In research, a new way was found to protect the data of ordinary users and office workers on the network. The advantage of development is that users can get the right tool from reliable sources and do not need to install packages that can also contain computer viruses. The proposed solution looks for the script used for the attack, if any, and only blocks it so that websites can continue to function properly. The effectiveness of this method has been proven and has shown its effectiveness in blocking cyberattacks (88.37%).

In conclusion, it is worth noting that at present there is no way that would absolutely guarantee the safety of users. That is why the modern world needs highly qualified cybersecurity specialists. It is also necessary to use information technology carefully and consciously to ensure the security and integrity of important data.

1. William, S. 86% of hacks in Google Cloud were used for illegal crypto mining. https://atlasvpn.com/blog/86-of-hacks-in-google-cloud-were-used-for-illegal-crypto-mining, 2018. Online; accessed 13-October-2022.
2. Lin, T.; Capecci, D.E.; Ellis, D.M.; Rocha, H.A.; Dommaraju, S.; Oliveira, D.S.; Ebner, N.C. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact.* **2019**, *26*. doi:10.1145/3336141.
3. Baykara, M.; Gurel, Z. Detection of phishing attacks. Detection of phishing attacks, 2018, pp. 1–5. doi:10.1109/ISDFS.2018.8355389.
4. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, 2014.
5. Kieyzun, A.; Guo, P.J.; Jayaraman, K.; Ernst, M.D. Automatic creation of SQL Injection and cross-site scripting attacks. 2009 IEEE 31st International Conference on Software Engineering, 2009, pp. 199–209. doi:10.1109/ICSE.2009.5070521.
6. Subramani, K.; Yuan, X.; Setayeshfar, O.; Vadrevu, P.; Lee, K.H.; Perdisci, R. When Push Comes to Ads: Measuring the Rise of (Malicious) Push Advertising. Proceedings of the ACM Internet Measurement Conference; Association for Computing Machinery: New York, NY, USA, 2020; IMC ’20, p. 724–737. doi:10.1145/3419394.3423631.