DETECTION | PREVENTION | INTELLIGENCE

Invincea White Paper

"Micro-Targeted Malvertising via Real-time Ad Bidding"

UPDATED: Includes New CryptoWall Malvertising Campaign

Release date: October 27, 2014

Table of Contents

Executive Summary *2*

Introduction *3*

Operation DeathClick: Targeting the US Industrial Base **4**

Summary for Incident at Fleaflicker.com **4**

Summary for Incident at Gpokr.com **9**

Summary for Webmail.earthlink.net **11**

Summary of Incidents in Operation DeathClick **13**

Real-Time Bidding Networks: How it works *13*

Malvertisers have Weaponized RTB **16**

Competitive Service Offerings for RTB **16**

Major Players in RTB **20**

How Malvertisers Get $$ to Bid on RTB **21**

Where Malvertisers Host Exploits **22**

Real World Examples of RTB Malvertising Captured by Invincea **23**

Ransomware Campaign via Malvertising *26*

Analysis of CryptoWall Malvertising Infections **27**

Central Hosting of Clean Content *30*

How to Protect Yourself from Micro-targeted Malvertising *31*

Release Notes *32*

Executive Summary

Most targeted attacks against organizations originate as spear-phish campaigns or watering hole style web driveby attacks. Within the last six months, Invincea has discovered and stopped ***targeted*** malvertizing attacks against specific companies -- particularly those in the Defense Industrial Base. The combination of traditional cyber crime methods (malvertising) with targeted attacks against Defense industrials for theft of IP represents another development in the on-going blending of techniques from cyber crime and advanced threat actors with nation state agendas. We are tracking an on-going campaign against US Defense companies under the code name **Operation DeathClick**.

Traditional malvertizing has been an effective but indiscriminate method cyber crime gangs use to compromise endpoints to perpetrate ad fraud, identity fraud, and banking credential theft. In this new **targeted** variation of malvertizing, the perpetrators are attacking specific organizations by leveraging real-time ad bidding networks and micro-targeting techniques developed over the last decade in online advertising. The objective of these micro-targeted attacks against the Defense sector is likely theft of Intellectual Property more than ad fraud and indicates motive and sophistication characteristic of advanced threat actors. Since these attacks were blocked by Invincea prior to compromise of the machine or network, we cannot confirm the specific IP the perpetrators are after – only the Tactics, Techniques, and Protocols (TTPs) used which we describe herein, similar to methods used to provide backdoor access and command and control over compromised networks.

While we discovered these attacks across multiple Defense companies, we expect it will not be long, if not already, before other highly targeted segments including Federal, Financial Services, Manufacturing, and HealthCare are victimized with the same micro-targeted malvertising. The campaign described here does not represent a single flaw, 0-day, or unpatched bug, but rather a significant development in the adversary's capabilities and strategy to leverage legitimate online advertising platforms on well-known ad supported websites via a technique called Real-Time Ad Bidding. In other words, **this problem will not be patched on Tuesday.**

UPDATE: We have updated this document to include a new section on a campaign of distributing CryptoWall ransomware via malvertising. While the attack vector is the same, we believe this to be motivated by cybercrime rather than theft of IP from Defense companies.

Introduction

Malvertising has seen meteoric rise in 2014. Threat actors create a corporate front, advertise on commonly visited sites, then later switch out the landing pages for their ads to pages that host exploit kits, or simply create a temporary redirection from their usual content to the malicious landing page. These exploit kits are hosted on compromised web servers across the world. In other words, they leverage legitimate ad-supported popular websites together with compromised websites for hosting exploit landing pages, defeating black-listing techniques. The lifetime of these ads and landing pages are measured in hours.

In the campaign described here, **Operation DeathClick**, traditional malvertising has been armed with a micro-targeting system using IP address ranges, geographically narrowed down to zip codes, and interests of the user (recorded in cookies) to target specific companies, company types, and user interests/preferences. They are employing the tactics of real-time ad bidding to guarantee malicious ad delivery to intended targets of the campaign – building on a decade of work in real-time analytics for online ad placement, but for nefarious purposes.

The threat actors redirect their ads for just minutes at a time and then abandon their exploit kit pages forever. This means that list-based threat intelligence feeds are rendered ineffective. The domains used do not appear in any proxy blacklist, and the malware droppers delivered by the exploit pages always employ different signatures, evading traditional network and endpoint detection technology.

Ad delivery networks today are not incentivized to address the problem in a credible manner as they derive revenue from the criminal enterprise, while not being held accountable. Turning a blind eye to the problem is rewarded economically. Meanwhile the perpetrators are able to use traditional malvertising and ad fraud bots to fund the criminal enterprise.

Without cooperation of ad networks to vet the advertisers working through front companies, this attack vector will go unchecked. And now, with the advent of real-time ad bidding, these threat actors have weaponized ad delivery networks to target victims based on:

- User-Agent strings (versions of flash, OS, java and browser)
- Interest-related content (click bait articles, industry specific software or hardware, like medical supplies, radar mapping software, ammunition sales, stocks forums)
- Advertising Profiles derived from cookies (someone with specific tastes, may shop for shoes, handbags, cars, luxury vacations)
- Geographic region (malvertisers can target specific neighborhoods or states via geoip direct advertising)
- **Specific corporate IP ranges** (targeted malvertising can target the public IP space of your network or an Industrial Vertical)

Real-time ad bidding allows advertisers, and by extension, adversaries, to micro-target ad delivery on an extremely granular basis. For example, oppressive regimes trying to gather intelligence on activist protests can deliver ads to people getting email from within a specific locality where they are protesting. Today, it is commonplace for micro-targeting techniques to be used as part of the toolset in legitimate online advertising. For instance, a defense contractor, trying to win a new omnibus contract, can deliver targeted ads to online news sites frequented by Government program personnel. The latest software product release can be delivered to Windows users visiting PC Magazine's website. A local car dealership can sense when someone is in the market for a new car and can deliver advertising to those users, based solely on browsing history.

Now advanced threat actors are able to target an organization directly via micro-targeted malvertising, based solely on their corporate network IP range. Thus, it doesn't matter where in the world you point your web browser -- an online video poker room, a fantasy football club homepage, a Pakistani news homepage, or even checking your own webmail at a trusted email provider. Those ad windows can and are being used to deliver malware if the bidding price is right.

Operation DeathClick: Targeting the US Industrial Base

Recently, multiple US Defense/Aerospace contractors were targeted by a malvertising campaign. These contractors had deployed world-class enterprise security defense in depth approaches to protect their intellectual property. They had next generation firewalls that relied on threat intelligence feeds to do auto-blocking of known malicious sites. They had malware interception technology that relied on known bad hashes to prevent malicious downloads. The multiple proxies in place subscribed to real time feeds of known bad URLs. They deployed AV at the gateways and on the endpoints.

But in a two week period, these organizations were hit with dozens of micro-targeted malvertising attacks, each of which would have provided a beachhead for the threat actors from which to compromise the network, if successful. In each instance, the attacks were carried out by targeting these Defense contractors directly via real-time ad bidding. Once targeted, an end user only needed to browse to any website, anywhere in the world, which contained a DoubleClick ad-partner embedded window. Invincea stopped these attacks on the endpoints by containing the delivered exploits in secure virtual containers, while producing the forensics that led to this discovery.

Next we go in some detail about example attacks perpetrated against the defense firms.

It is important to note that the websites we show next that served up targeted malvertising were victims of malvertising campaigns with no knowledge of the malicious ads they were serving up. These malicious ads were served up by 3rd party networks, who are unwittingly sourcing malicious content. As we will discuss later, the 3rd party ad networks themselves are falling victim to malicious content campaigns.

Summary for Incident at Fleaflicker.com

A user visited his online fantasy football league homepage at Fleaflicker.com. As soon as the page loaded, a malicious ad delivered a backdoor Trojan via a Java-based exploit.

Figure 1 shows a screenshot of the page that was visited. You will notice the two inline ad placements for DoubleClick ad delivery. The malware delivered came from a compromised Polish website, and would have installed a generic backdoor Trojan.

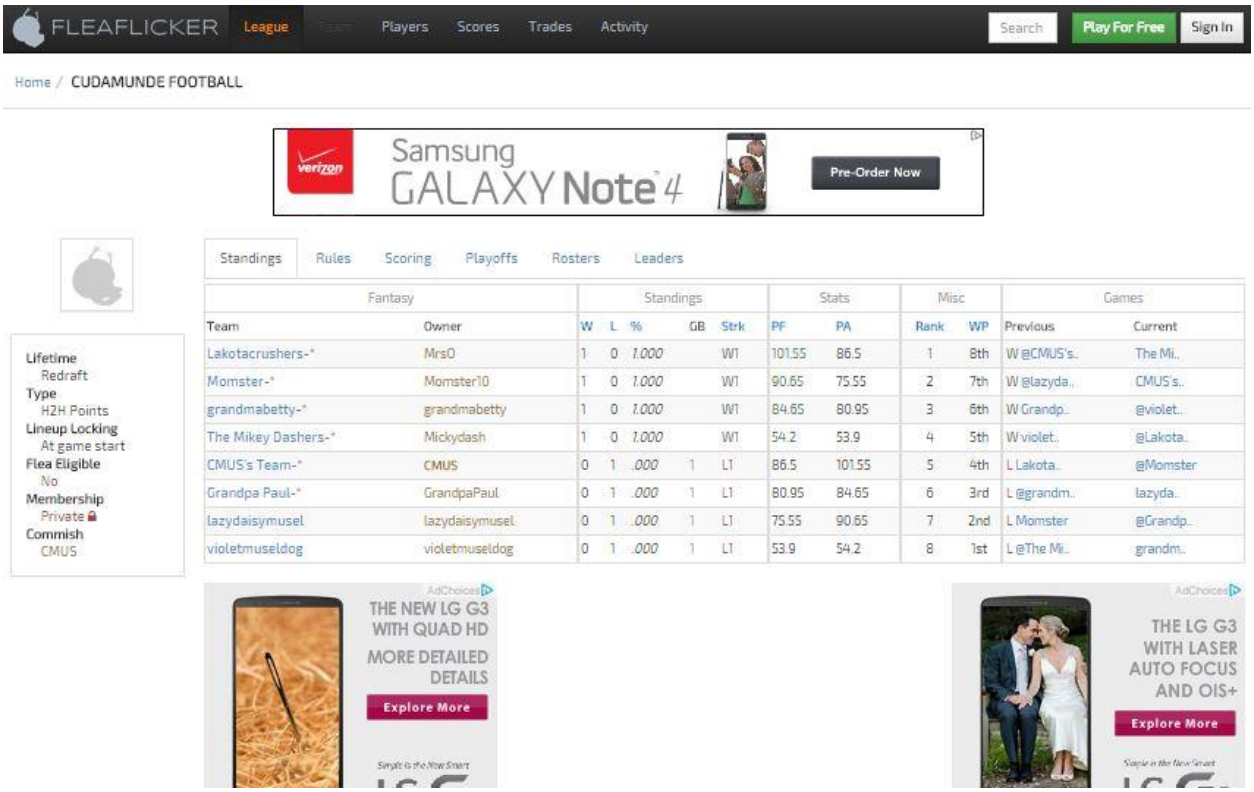


Figure 1: Fleaflicker.com website

Note the prominent ad placements by AdChoice, a DoubleClick affiliate. Figure 2 shows an event tree of the exploit and malware delivered from an ad by visiting Fleaflicker.com.

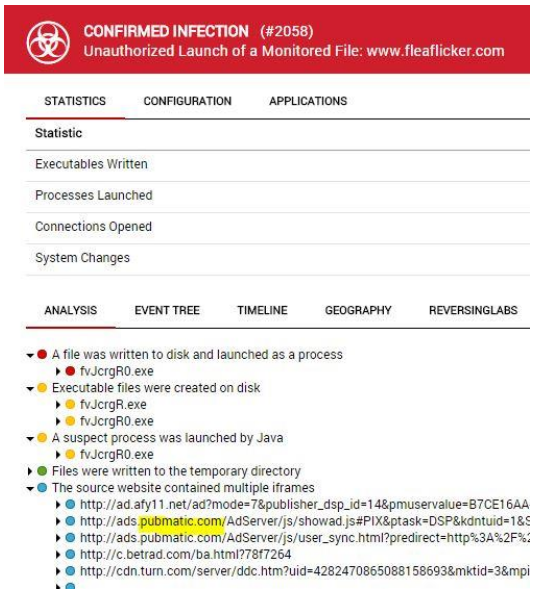


Figure 2: Event tree for infection from Fleaflicker.com Incident

The event tree in Figure 2 taken from Invincea's Threat Management Console shows the exploited Java process dropped a file called fvJcrgR0.exe, and that it likely came from Pubmatic, an ad delivery network that allows for real time bidding to deliver ads. In this instance, the Pubmatic server redirected to a Web server in Poland that dropped the malware. The timeline below shows the exact times and URLs visited.

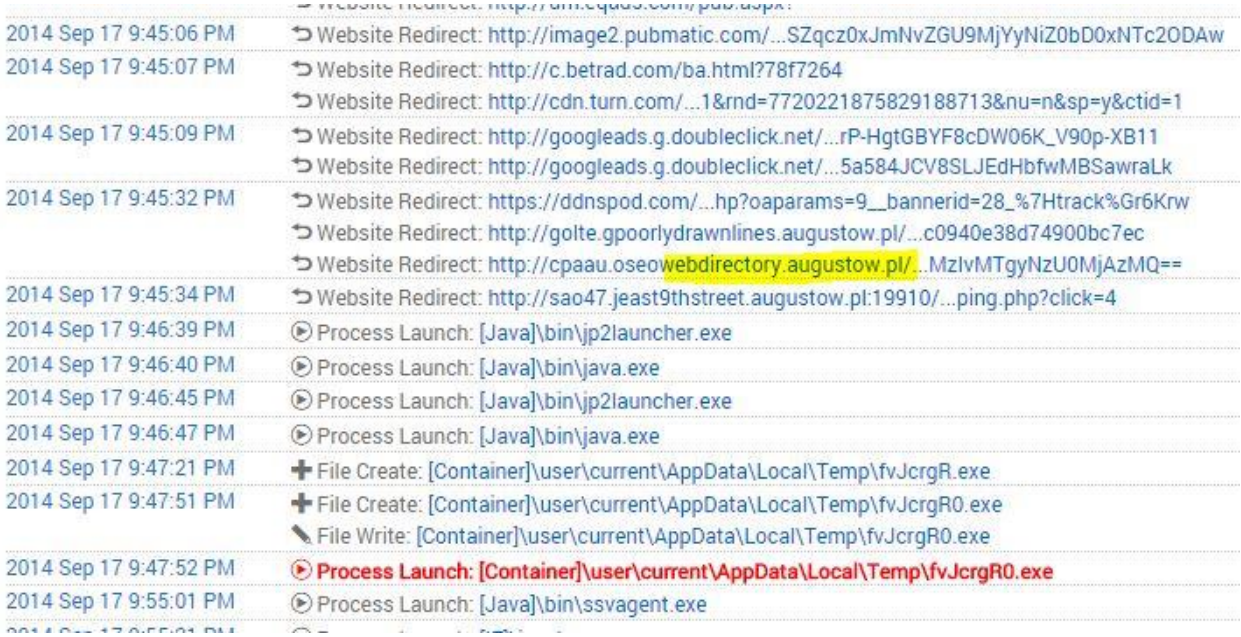


Figure 3: Timeline for Fleaflicker.com Incident

Note the number of re-directs from Fleaflicker.com to different outside properties in Figure 3.

PROCESS LAUNCH

Property	Value
Parent	[Java]\bin\java.exe (5844)
Time	2014 Sep 17 9:47:52 PM
Path	[Container]\user\current\AppData\Local\Temp\fvJcrgR0.exe
PID	7588
Trust Level	suspect
MD5	C546D1052BA65AECC68A67BB8A4A3F9D Search on iSIGHTPartners Search on Reversing Labs Search MD5 on Google Search MD5 on VirusTotal

Figure 4: Process Launch for Malware fvJcrgR0.exe from Fleaflicker.com Incident

Invincea Threat Management provides a quick way to search for an MD5 hash on third party sites (see Figure 4). By clicking the VirusTotal link, the analyst will see the following VirusTotal report in Figure 5:

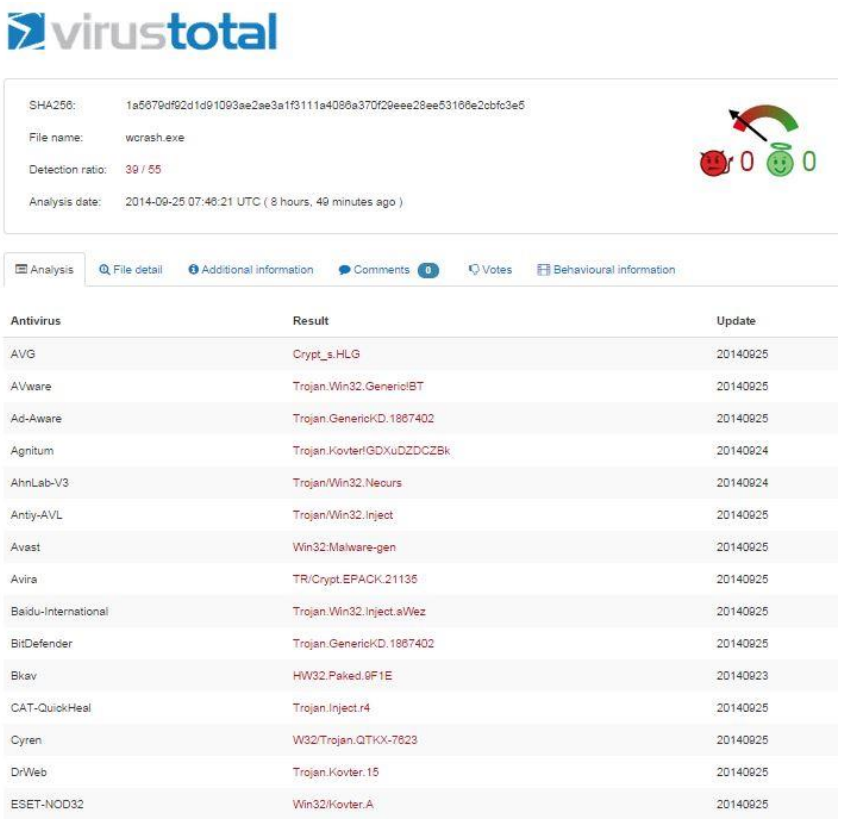


Figure 5: VirusTotal Report for Malware fvJcrgR0.exe from Fleaflicker.com Incident

From the VirusTotal report in Figure 5, you will see that this malware is a Trojan backdoor that would likely be used to download additional malware or to provide remote persistent access to the attacker.

Summary for Incident at Gpokr.com

An employee at a defense contractor visited a free Texas Poker online game. The Poker site had advertisements on the page, one of which launched a similar attack as seen in before on other websites visited by employees at this firm.

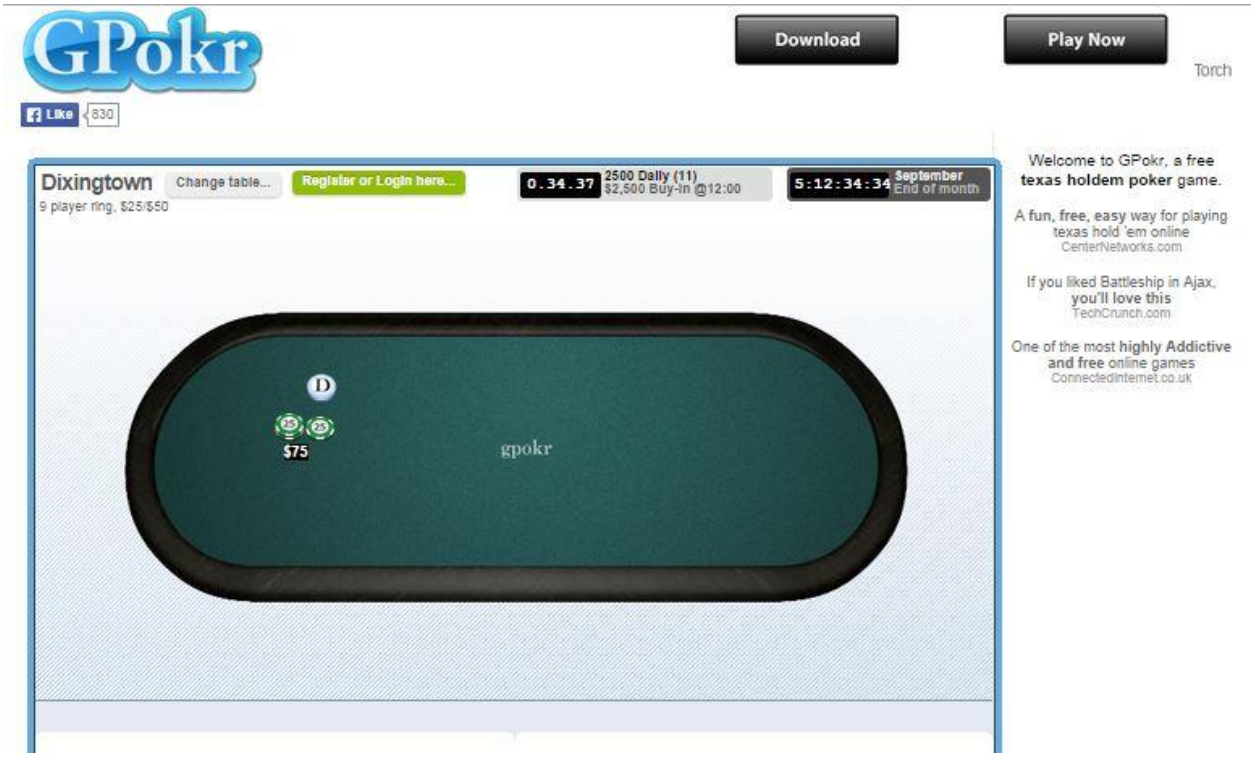


Figure 6: Screenshot of Gpokr.com

It should be noted that Gpokr.com no longer appears to be serving advertisements from their site. At the time of the incident, as seen in the logs below, an ad window was previously present. In the event tree shown in Figure 7, you will see that the winning bid redirected to a direct-to-IP site instead of a site via domain name. Also, above is the first indication of specific executable DLL files. Searches for these filenames returned zero results on VirusTotal.

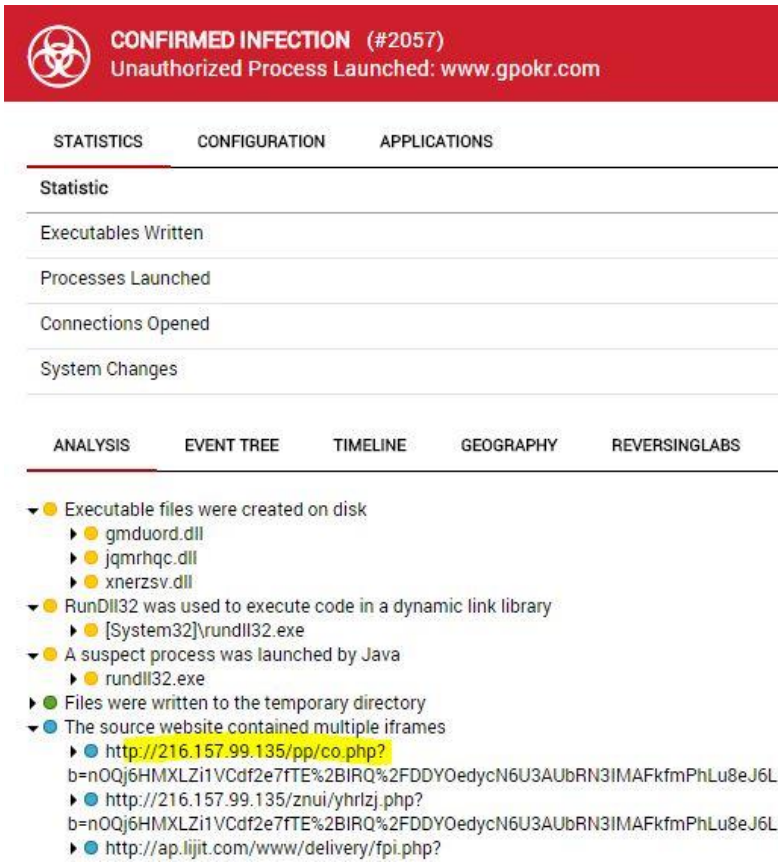


Figure 7: Event Tree for Gpokr.com

This event on September 14 (Figure 8) shows that delivery.first-impression.com redirected directly to an IP address, not a domain name to deliver its malicious payload. Note the multiple DLL files written to disk and the spawning of rundll32.exe. At this point, the Invincea-protected host recognized the unauthorized process and reverted itself to a clean state.

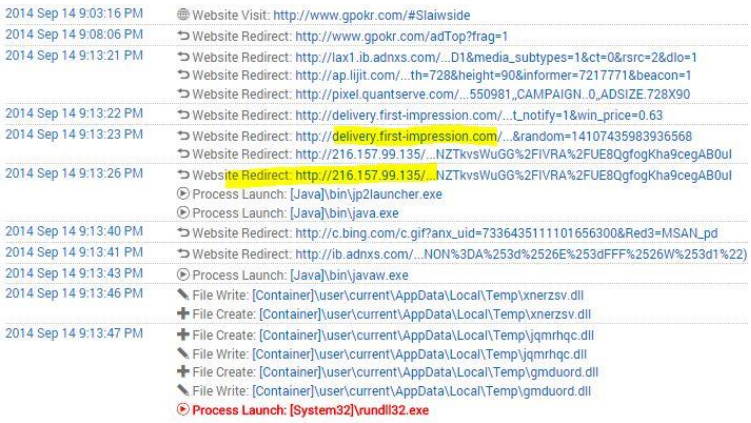


Figure 8: Timeline View for Event 5 – Gpokr.com

Summary for Webmail.earthlink.net

In another incident an employee checked their online Earthlink account. When they replied to an email, a new ad was loaded on a page that attempted to exploit Java. This malvertising was from the same IP address seen in other incidents.

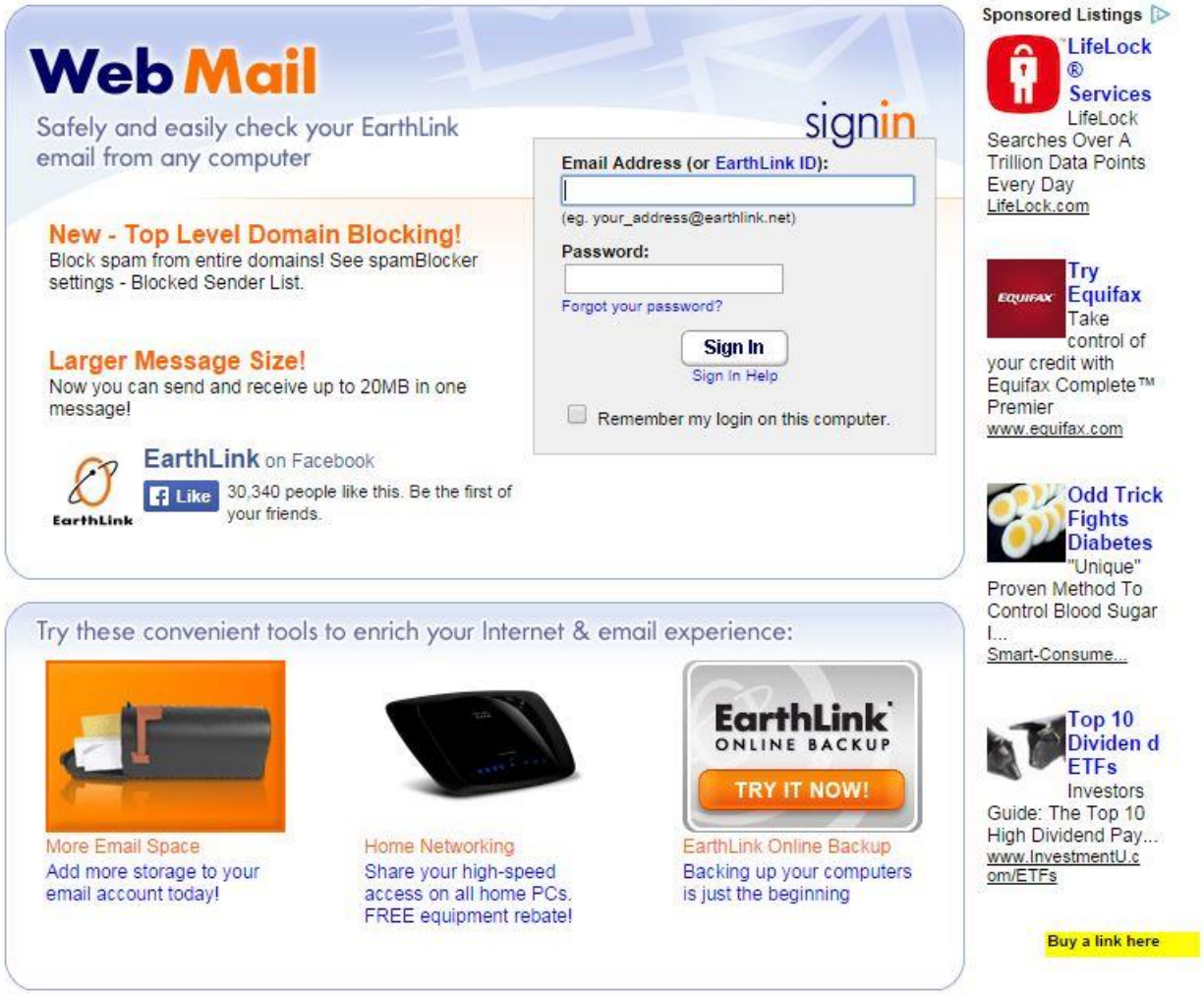


Figure 9: Screenshot of Webmail.earthlink.net

You will notice the inline advertisements on this page in Figure 9. The event tree in Figure 10 notes that this was likely a spear-phish attack. The timeline will show that when the user replied to an email, the ads on the Earthlink page refreshed, dropping the exploit code via Java.

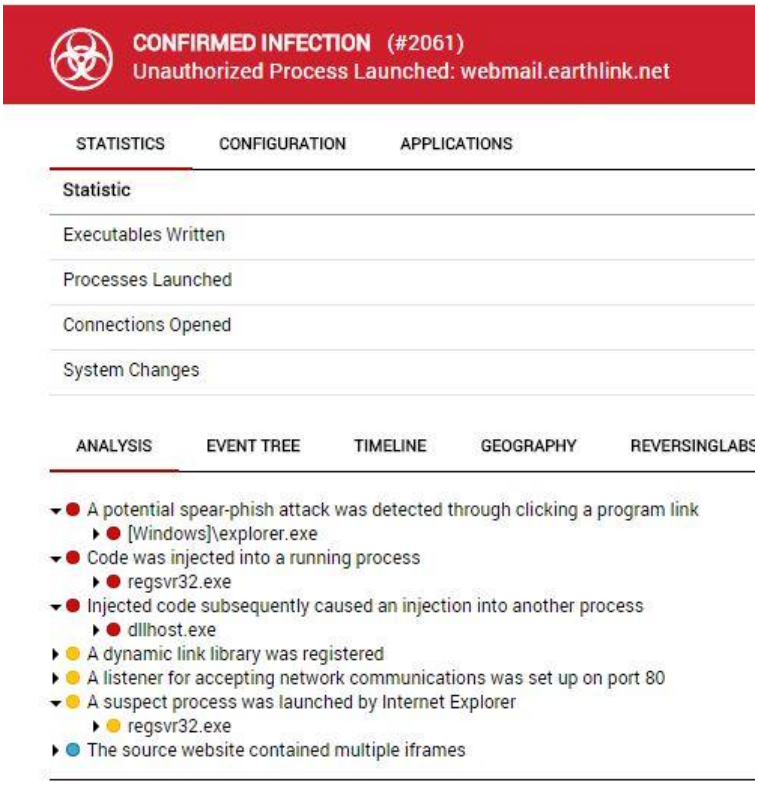


Figure 10: Event Tree for Incident 6 Webmail.earthlink.net

Note in the timeline in Figure 11, how there was a 7 minute gap between the DoubleClick ad redirect and the delivery.first-impression.com ad. This is an indication that the page was refreshed or the ad was refreshed on the page. The same exploit IP address from the Gpokr event is present. This event is the oldest, happening on September 11.

Figure 11: Timeline for Incident 6 Webmail.earthlink.net

Summary of Incidents in Operation DeathClick

The three examples above are samples of the more than two dozen micro-targeted attacks we have witnessed and blocked as part of Operation DeathClick since mid-September. Defense Industrial Base customers witnessed micro-targeted malvertising at a rate six times that of comparable private sector companies with similar defense-in-depth capabilities.

Real-Time Bidding Networks: How it works

We observed in Operation DeathClick that real-time ad bidding networks are being used by criminal enterprise to target companies with malicious content in order to gain persistent remote access. In these third-party arrangements, the content is frequently not vetted because billions of impressions are rendered in real-time. Most of the content is legitimate ads. A small fraction is malicious content linking to landing pages that infect users. *Real-time ad networks are being used, often unwittingly, and some have taken steps to try and combat malicious use of their networks. The Online Trust Alliance is one such industry group comprised of major software companies and ad networks working together to try and address this problem. Our goal in this paper is to shed light on the micro-targeting of companies by criminal enterprise employing real-time ad networks, and to aid the industry in collectively addressing this problem.*

Real-time ad bidding networks have evolved over the last ten years as a means of micro-targeting customers with advertising content they are more likely to click-on.

From Wikipedia:

> ***Real-time bidding** (**RTB**) refers to the means by which ad inventory is bought and sold on a per-impression basis, via programmatic instantaneous auction, similar to financial markets.[1] With real-time bidding, advertising buyers bid on an impression and, if the bid is won, the buyer's ad is instantly displayed on the publisher's site.[2] Real-time bidding lets advertisers manage and optimize ads from multiple ad-networks by granting the user access to a multitude of different networks, allowing them to create and launch advertising campaigns, prioritize networks and allocate advertising stock.*
>
> *Real-time bidding is a dynamic bidding process where each impression is bid for in (near) real time, against a static auction where the impressions are typically bundled in groups of 1,000.*
>
> *A typical transaction begins with a user visiting a website. This triggers a bid request that can include various pieces of data such as the user's demographic information, browsing history, location, and the page being loaded. The request goes from the publisher to an ad exchange, which submits it and the accompanying data to multiple advertisers who automatically submit bids in real time to place their ads. Advertisers bid on each ad impression as it is served. The*

impression goes to the highest bidder and their ad is served on the page.This process is repeated for every ad slot on the page. Real time bidding transactions typically happen within 100 milliseconds from the moment the ad exchange received the request.

The bidding happens autonomously and advertisers set maximum bids and budgets for an advertising campaign. The criteria for bidding on particular types of consumers can be very complex, taking into account everything from very detailed behavioral profiles to conversion data.

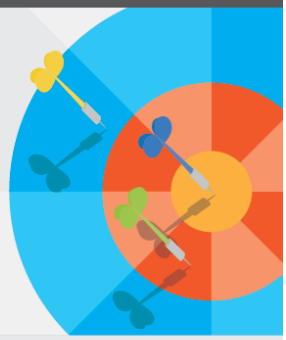
The following infographic summarizes how advanced adversaries are now micro-targeting companies using malvertising.

Malvertisers

HOW MALVERTISERS USE REAL TIME AD BIDDING TO TARGET YOU

Cyber Threat Actors have turned to targeted malvertising as a sure-fire way to bypass old-generation security controls in victim organizations. Malvertising has evolved from bulk ad purchases to using real-time Ad-bidding services to target organizations and audiences with pinpoint accuracy.

How to Discriminate Targets with Malvertising



GEOGRAPHY
Malvertisers can target specific neighborhoods or states via geoip direct advertising

CORPORATE IDENTITY
Targeted malvertising can target the public IP space of your network

USER PROFILING
Someone with specific tastes, may shop for shoes, handbags, cars, luxury vacations

CONTENT
Click bait articles, industry specific software or hardware, like medical supplies, radar mapping software, ammunition sales, stocks forums

HOW DO MALVERTISERS SETUP THEIR MALWARE DELIVERY?

STEP 1
Create corporate front to infiltrate ad networks as legitimate

STEP 2
Compromise active websites via WordPress, Apache or Ngninx vulnerabilities to host exploit landing pages and exploit kits.

STEP 3
Choose your victims from list above.

STEP 4
Use cash generated by clicks/botnets to bid up ads directed at your target.

STEP 5
Win the ad bids, deliver the exploit via ad network, compromise victim machine, drop backdoor Trojan.

STEP 6
Burn the landing page. Malvertising sites are typically online for less than 4 hours. The malicious landing pages are deleted.

STEP 7
Profit! New compromised hosts join botnets that click on ads to deliver click-fraud cash to malvertisers. Or banking credentials or passwords are stolen. **REPEAT STEPS 2-7**

Proxy blacklists can't update fast enough to catch landing pages before they disappear. Signature-based detection is bypassed because modern exploit kits use unique, changing binary payloads.

Does "**Sniper-tising**' have your organization in the crosshairs?

Only Invincea protects against all forms of malvertising and web-based threats- known, unknown, indiscriminate and targeted. Keep calm on click on!

invincea™

Malvertisers have Weaponized RTB

The marketplace and auction of ads sounds great for actual ads. But what if the landing pages that are supposed to be ads are actually malicious PHP pages with embedded malware? The bidding and ad placements work the same, but instead of seeing a flashy ad banner, the highest bidder for the placement serves malware. The price to win the bid to push malvertising to any page you happen to visit ranges from 45 to 75 cents per impression.

A malicious advertiser on a network may serve crafted, seemingly normal ads, a majority of the time. In fact, the ads are often stolen copies from legitimate advertisers. This establishes the attacker's legitimacy and trust on the ad network. Of course with real-time ad bidding, he can simply offer up low bids and his content would consistently lose in the marketplace. But it is very simple to replace the redirection code to switch from a legitimate ad banner to a drop site that hosts an exploit kit, typically based on Java, Flash, Silverlight, or all three. Once the malvertiser detects that he has several infected hosts, he removes the redirection code and goes back to serving standard ad banners. He then "burns" his temporary exploit kit drop site, moving his exploits to another location for a new campaign.

This allows the malicious advertiser to perform hit and run attacks, infect whomever he wants at whatever time he wants, and maintain his presence on the advertising marketplace without drawing undue attention to his activities.

In the sections below, we will provide highlights of the RTB industry, its targeting capabilities, and show how malvertisers have been mis-appropriating RTB networks to deliver malware.

Competitive Service Offerings for RTB

The RTB ad networks provide significant micro-targeting capabilities that have long been used to serve legitimate content to users more likely to click on them. In the following, we describe these capabilities to show the state of the art in RTB network capabilities. The quoted material below are direct quotes from Real Time Bidding service providers linked. Emphasis added by Invincea.

***Pubmatic*:**

> ***Audience Targeting***: *Bid on the audiences most valuable to you. Each impression in the PubMatic auction can be enhanced with first- and third-party data;* ***giving buyers targeting capabilities across display, mobile, tablet and video inventory. Media buyers can also cookie sync with publisher audiences to incorporate CRM, retargeting*** *and exclusion strategies in their digital advertising.*
>
> *Buyers have access to proprietary audience segments either directly through Private Marketplace deals or through the open market. With hundreds of parameters available to you, PubMatic has your best audiences waiting for you.*

*With PubMatic, buyers are able to access **pre-defined vertical or audience packages**, seasonal packages, publisher and/or site-specific inventory packages as well as pre-selected publisher packages and pricing available in Private Marketplaces.*

First-Impression.com

*"First-Impression Buy-Side offers the **granular targeting**, tracking, and reporting needed to help our clients make the most of their spend, along with an expert support team to advise when needed. By leveraging real time buying, First-Impression Buy-Side gives media buyers the full control to maximize the value of an impression."*

Could Malvertisers Track Exploits and their cost per impression? Yes. Many RTB networks provide a control panel to track advertising campaigns in real-time, along with notifications that bids have been won and who exactly was served the malware.

Below is a URL redirection log from First-Impression.com from a winning bid by a malvertiser. In the URL are parameters such as the type of ad, the type of user-agent string of the ad reader specified (which discloses browser and java versions), whether it is a retargeted ad based off of cookies (this one was not), the price paid, which is 65.4 cents, and the notification to the malvertiser that his malvertising was delivered.

```
http://delivery.first-impression.com/delivery?action=serve&ssp_id=3&ssp_wsid=2191400908&dssp_id=100&domain_id=2191400908&ad_id=748271&margin=0.4&cid=155380&bn=sj14&ip_addr=24.234.123.133&ua=1540937276&top_level_id=24.234.123.133&second_level_id=1540937276&page=thanhniennews.com&retargeted=null&height=90&width=728&idfa=null&android_id=null&android_ad_id=null&bid_price=0.654&count_notify=1&win_price=$AAABSMPg1dmFEPqXEZe5_CYviub3uOlabldGew
```

DoubleClick.net

DoubleClick discusses their targeting capabilities in online documentation. Since they specialize in knowing the location of their ad windows, they market those ad spaces to the actual advertisers and malvertisers, along with targeted demographics about the content pages, the visitors to the sites and more.

To showcase the variety of impression-level data available to buyers, consider the data made available through a connection to DoubleClick Ad Exchange's real-time bidding API. With ADX, a buyer could consider any of the following data passed from the seller with each impression:

- *Ad slot parameters: visibility (above or below the fold), size, excluded creative attributes, excluded advertiser URLs, allowed vendor or ad technology.*
- ***Geo parameters: country, region, metro, city.***
- *Content parameters: site URL, site language, seller network, **vertical** or category.*

• *User parameters**: browser, operating system, anonymous cookie (hashed), cookie age**.*

Just like when considering one type of data, by using the anonymous cookie parameter, buyers can consider first-party retargeting or third-party audience data from a data provider. However, they can go further in the evaluation by looking at more of these parameters. This helps a buyer learn much more about a particular user and a particular impression, gain a smarter answer to the three essential questions and make a more data-driven decision.

Twitter, Facebook and other RTB ads can now target mobile devices by their phone numbers.

This sounds like a great way to advertise if you are in the marketing industry. Consider how granularly a person can be targeted if this service is used maliciously. If not targeted by the desktop, how about on the mobile platform?

Twitter's Tailored Audiences just got a little more tailored.
*Advertisers can **now augment their customer data using mobile advertising IDs and mobile phone numbers** as a way to reach existing customers and increase audience size. In essence, the move is an extension of Twitter's Tailored Audiences for CRM retargeting, which allows advertisers to use hashed **non-PII email address** to retarget existing customers. **(email addresses are twitter IDs- so you could be targeted for ad delivery based on your account name or known phone number)***

*Twitter also rolled out the ability to target lookalike audiences, a function that seems pretty similar to Facebook's tool of the same name. Twitter's lookalike modeling uses a proprietary algorithm that examines modeled users looking for similarities related to behaviors, **interests, location, demographic attributes and engagement patterns**.*

Twitter described its enhanced as "part of improved targeting options to help advertisers reach additional users similar to their existing audiences."

*Tailored Audiences, Twitter's seeming answer to the Facebook Exchange (FBX), officially launched back in December after running retargeting and database matching tests in July. Twitter has appeared to follow Facebook's lead with a number of its recent roll-outs, including site retargeting, CRM targeting and now retargeting via lookalike audiences. (**Facebook also makes it possible to target users by phone numbers through Custom Audiences**.)*

Neustar.biz

Neustar does provide a real-time bidding ad exchange, but their real market is IP intelligence that they sell to other advertising networks for the purposes of better targeting specific users. In Europe, laws require that advertising networks allow people to opt out of having tracking cookies, which is how many advertisers used to rely upon for ad campaign targeting. To get around this, Neustar perfected IP based targeting, which avoids cookies. They are able to build IP specific browsing profiles based on IP subnets. In a blog post below, Neustar boasts about their direct to IP range and enterprise advertising.

How can Neustar IP Intelligence target by IP?
While IP intelligence has been around for many years, the ability to effectively target advertising by audience, based on IP is very new. Neustar IP Intelligence is currently working with select DSP platforms to buy impressions off of the exchanges based on the IP address rather than cookies. ***This has only been possible with the recent emergence of real time bidding (RTB).*** *The secret sauce is in understanding the IP and the methodology necessary for* ***targeting ads appropriately against it.***

Is an IP Address like a cookie?
No, an IP address only identifies devices on a network. The IP address does not contain any PII and does not track or store any consumer usage or behavioral information. ***(But IP ranges are registered by IANA, and you can easily know who owns the ranges)***

Product Specific Questions
Q1: How does the process work?
The process works exactly like any advertising network. Instead of buying inventory based on a cookie, Neustar is buying inventory based on an IP address. We run the targeting specifics against our proprietary database and ***create a custom IP list to target against****. Neustar has set up relationships with partners that have built the functionality for this to work end-to-end for our advertisers.*

Neustar offers a full service ad network. Brand marketers who wish to advertise using IP Audience Targeting can work directly with Neustar to determine custom IP placements, run campaigns, optimization, reporting and billing. Much like any traditional online publisher or online ad network, Neustar manages the entire process.

How does Neustar deliver its ads?
We use industry standard methods for delivering our ads, but what makes our approach special is that we bake in the IP data before delivering the inventory with our network partners, ***which allows us to target display ad campaigns to a specific business or organization****. We obtain inventory from ad exchanges, but have our own ad server.*

Zedo

Zedo, blamed for recent malvertising via DoubleClick, say they are now trying to protect against malvertisers in this blog here. Less than a week after this announcement, they published another blog post that describes how they can push advertising to specific platforms, devices, as well as specific markets and networks:

ZEDO Advertising Technology Updates – September 2014

Device Targeting
Users can now target ads to a specific device when trafficking ads. An option for "Device Targeting" is now available under "Targeting". A creative targeted to a specific Device will serve only on that Device. All major manufacturers/models are supported by this feature. If a creative is not targeted to any specific device than it will serve on all device.

Figure 13: Targeting by Device Manufacturer/Model

Apart from device, a user can target various devices based on different categories. At any given point of time, a user can target multiple manufacturers and categories.

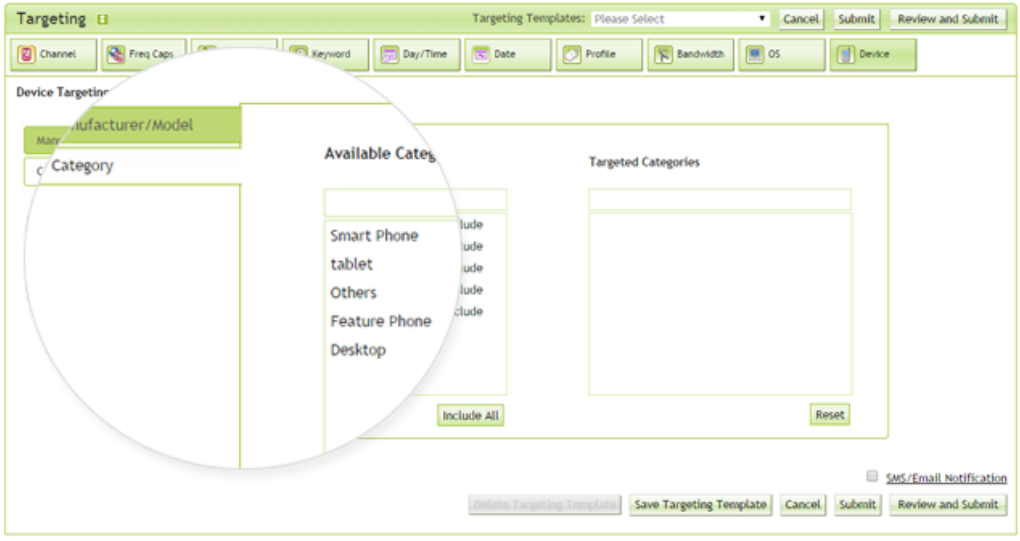


Figure 14: Targeting by Device Category

Reach Report by Creative

Apart from existing campaign reach report a user can now pull a reach report by creative. The creative reach report is available along with all the existing parameters and can be pulled by month, week or day. Creative reach report will show creative wise reach. It will help to analyze how effective the reach of a creative was.

Major Players in RTB

To be clear, RTB networks are legitimate platforms for displaying ads on ad-supported websites. They enable micro-targeting of user's interest, delivering content that a viewer would likely want to see. As we have detailed here, they can also be mis-appropriated unwittingly by malvertisers using these same tools and techniques to target companies with malware for persistent remote access in addition to traditional click fraud, phishing, and identity theft.

Below are links to RTB providers to learn more.

http://www.sovrn.com/
http://www.turn.com/
http://indexexchange.com/
https://www.dataxu.com/
http://www.sitescout.com/rtb/
http://first-impression.com/home/
http://www.zedo.com/

How Malvertisers Get $$ to Bid on RTB

Invincea has shown logs from a winning malvertising bid in the price range of 65 cents per impression. That is one ad, on one page, paid for by the malvertiser's account. This implies that malvertisers have deep pockets, spending hundreds of dollars on ad impressions. So how do they get money to spend on these malicious campaigns?

Invincea recently saw a malvertiser win a bid and delivered a Java exploit. This exploit copied a fully functional version of Chrome into the Java cache directory, and that version of Chrome launched in the background and proceeded to visit websites and click on specific ad banners. It is presumed that these ad banners paid revenue via referral bonuses to the malvertiser. By paying 65 cents to install a background web browser that does nothing but click fraud, the malvertiser is able to reap hundreds if not thousands of dollars in advertising referral income. It is a pretty good return on investment, which in turn allows the malvertiser to fund his micro-targeted malvertising attack campaign.

It is ironic, however, that click fraud is what is driving the prices of RTB advertising so high. Malvertising is not only a danger to end users, but it is a danger to the advertising industry as well. The image from Figure 14 below shows a log file of Chrome, in this instance, renamed Oajvliewxpge.exe, injected via Java to run in the background. Invincea detected this attack and killed the infection attempt. This is one instance where the malvertiser wasted his 65 cents.

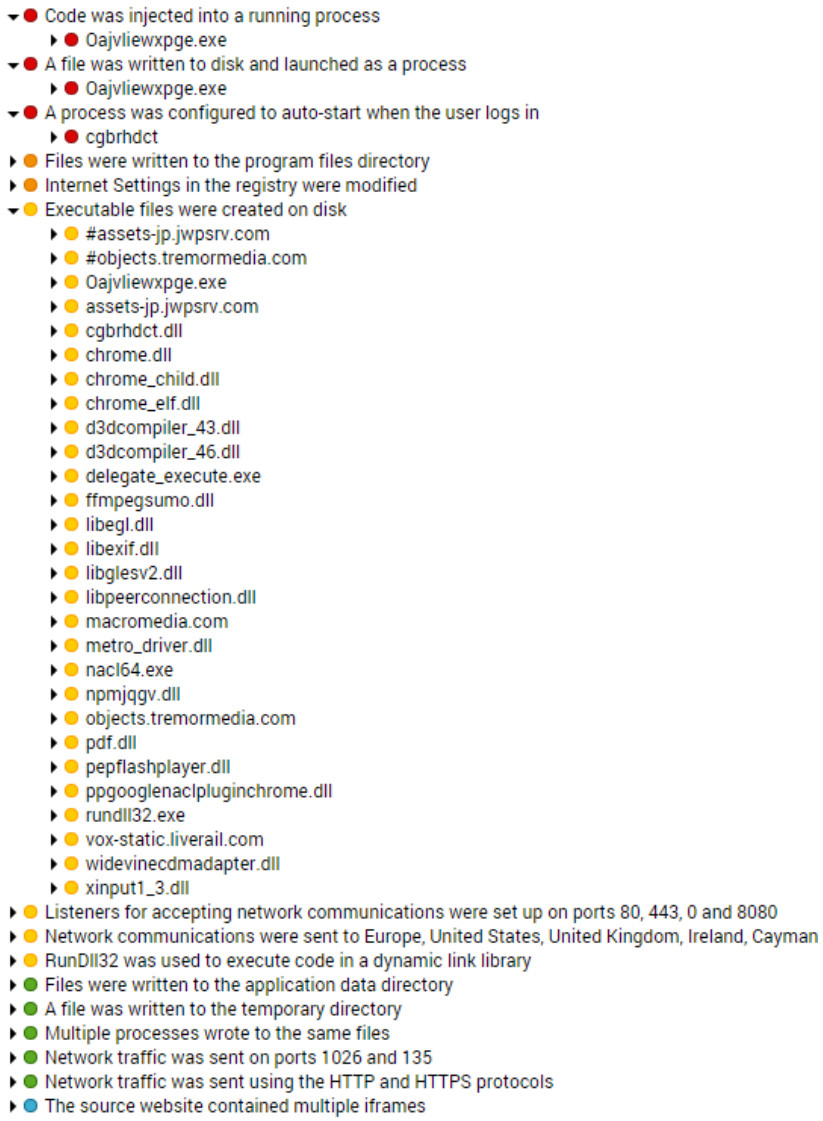


Figure 16: Event tree of click fraud malvertising exploit

It should be noted that Invincea is uniquely capable of stopping this type of attack. The introduction of Chrome as a browser, which is whitelisted by hash across the AV industry, would go unchecked by the AV and whitelisting applications industry. In this instance, the host was almost converted to a click-fraud bot. But the malware delivery could have been intended for data exfiltration, banking Trojans, or any other more insidious purpose.

Where Malvertisers Host Exploits

The ability for advertisers and malvertisers to automatically redirect to self-hosted ad content or exploit pages is driving RTB malvertising. Invincea has witnessed a rash of exploit kits and landing pages hosted on:

- Compromised WordPress Blogs

- Unconfigured Apache hosts
- Cloud-based NGINX subdirectories
- Government and News pages in Poland
- Free Hosting sites such as ua.in

In most instances, the landing pages are preconfigured with the exploit kit. The malvertiser creates the redirection in his normal ad prior to raising his bids to winning levels. Once several victims are confirmed, those malicious landing pages have the content erased, and the automatic redirection removed to serve "normal" ads again.

Real World Examples of RTB Malvertising Captured by Invincea

Figures 17 through 21 in the following are screenshots from Invincea's Threat Management console from various RTB-based malvertising incidents with highlighted URLs for malvertising delivered via RTB ad bidding.

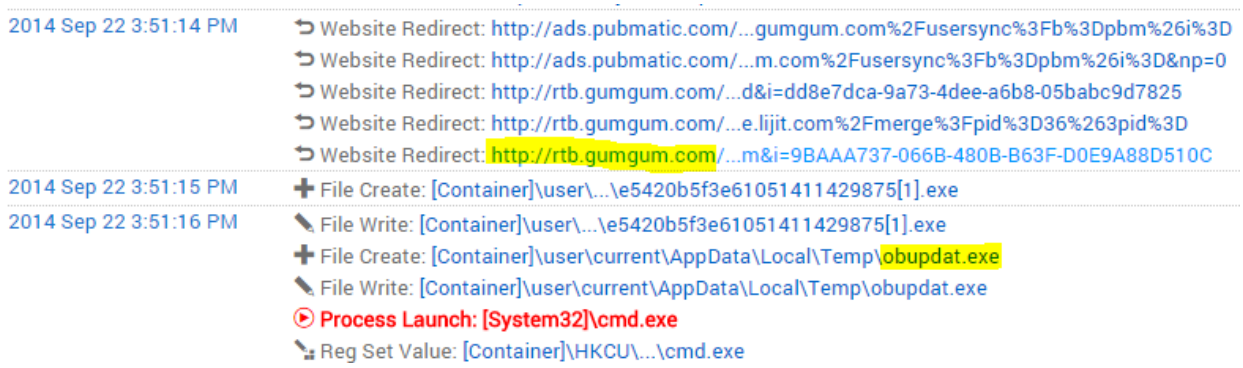


Figure 17: Recent Blaze.Com RTB Kryptik malvertising via GumGum

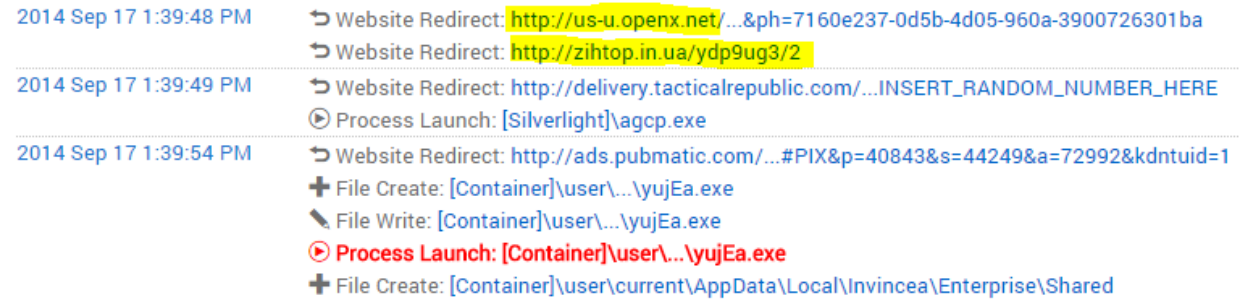


Figure 18: Online Ammunition Forum had RTB malvertising delivered. Exploit landing page in In.ua.

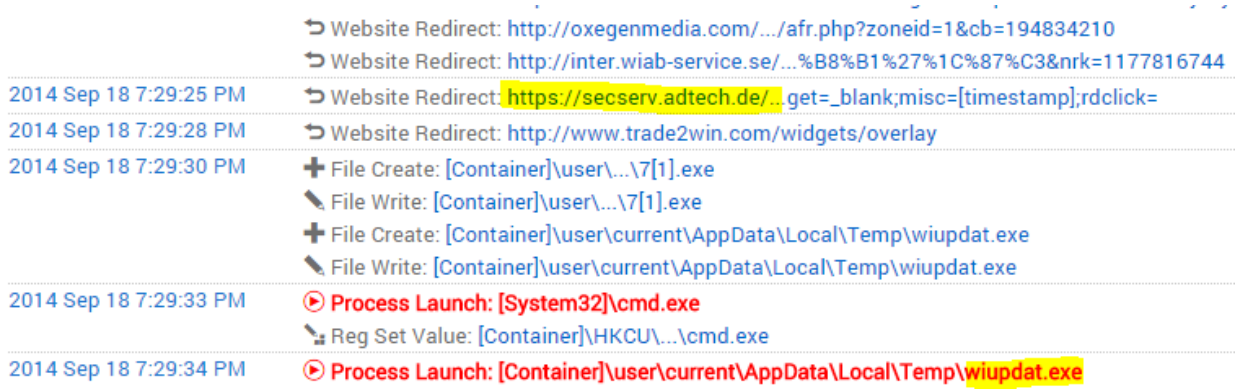


Figure 19: Largest Trading Online Forum Trade2Win.com delivered RTB malvertising via German provider:

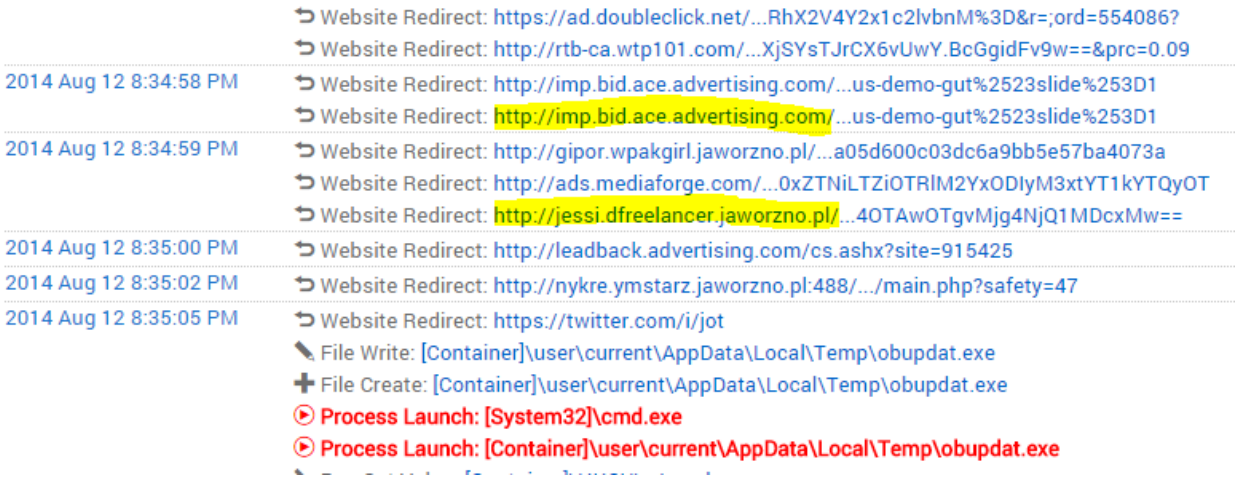


Figure 20: Answers.com click bait articles hosted winning RTB bids dropping Kryptik from Polish government landing page exploit kits.

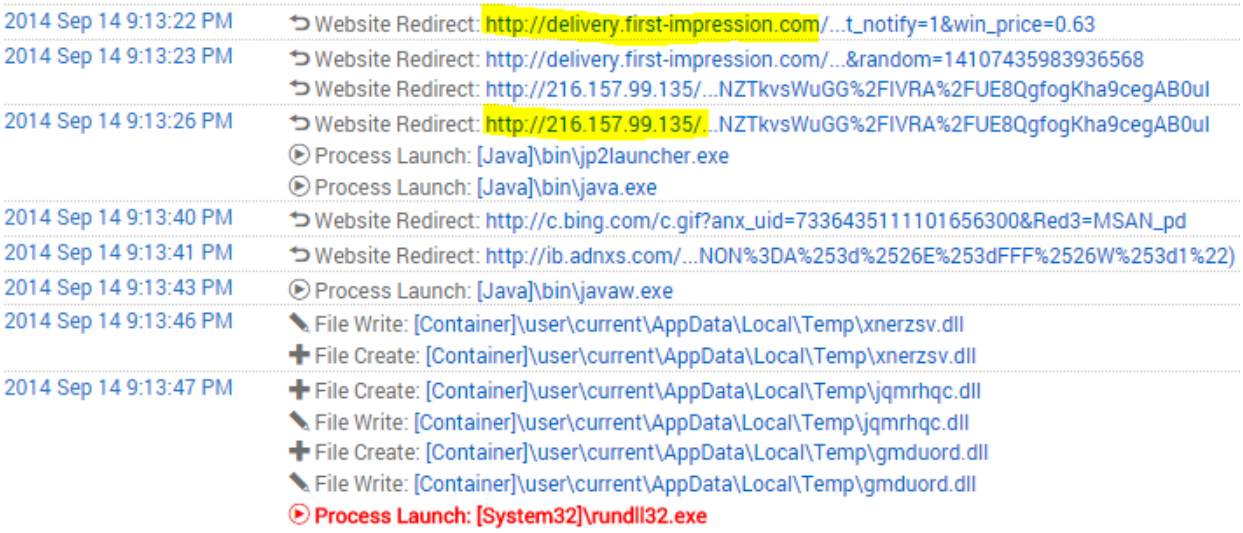


Figure 21: Online Poker Room and targeted RTB attack against Defense Contractor. Java exploit hosted at unconfigured Nginx host.

Ransomware Campaign via Malvertising

In September and October of 2014, Invincea saw a sharp spike of malvertising delivering CryptoWall ransomware attacks via Real Time Ad Bidding. We observed Real Time Ad bidding platforms, including OpenX, GoogleAds, Yahoo, AOL, and first-impression.com, fall victim to the ransomware malvertising scheme by unwittingly delivering the CryptoWall 2.0 ransomware ads.

Ransomware is a particularly pernicious form of malware that fully encrypts the victim's disk and data files, including remote storage, then demands payment of anywhere from $300 to $1000 in return for the decryption key. Users are held hostage from their own work, pictures, personal, and proprietary material. To learn more about the scourage of ransomware, see this blog.

Based on analysis of Invincea logs in would-be victims targeted by these ads, we have insight into the attacker that is delivering the malicious ads. According to Invincea analysis of ads delivered from first-impression.com, winning ad bids ranging from as low as 30 cents and as high as $1.70, were delivered by a block of unique identifiers. It is highly likely that the same attackers are using other RTB ad platforms.

This campaign matches the characteristics described by Proofpoint in its blog in terms of the exploitation methods. Legitimate ad copy is stolen, 3rd party ad networks used to distribute malware, and popular ad-supported websites displaying the malicious ads that exploit unsuspecting visitors with drive-by web exploits. Merely visiting any ad-supported site may result in a CryptoWall ransomware infection.

Cryptowall 2.0 utilizes the TOR network to hide its communications, but it quickly encrypts all local files on the disk, and demands bitcoin payment to unlock the files. Many companies have fallen prey to this attack over the past few months, making this one of the most successful Ransomware campaigns to date.

Analysis of CryptoWall Malvertising Infections

Mitigated Infection Event Sports.Yahoo.com

Below is a typical Cryptowall 2 infection as seen in the Invincea Management Server logs. This winning ad placement ran on sports.yahoo.com – an Alexa Top 4 rated site. Highlighted in order in Figure 22 is the common filename of obupdat.exe, which has ever changing hashes, followed by the TOR port, and the 3rd party ad platform of first-impression.com.

Analysis (Original report):

Figure 22: CryptoWall 2.0 infection report

Timeline Analysis (Original Report):

Below in Figure 23 is the timeline of the Tor connections and SSL connections employed by CryptoWall.

Figure 23: Network connections from CryptoWall 2.0

In addition, you can see the ransom note being written to disk on an infected machine in the audit logs in Figure 24.

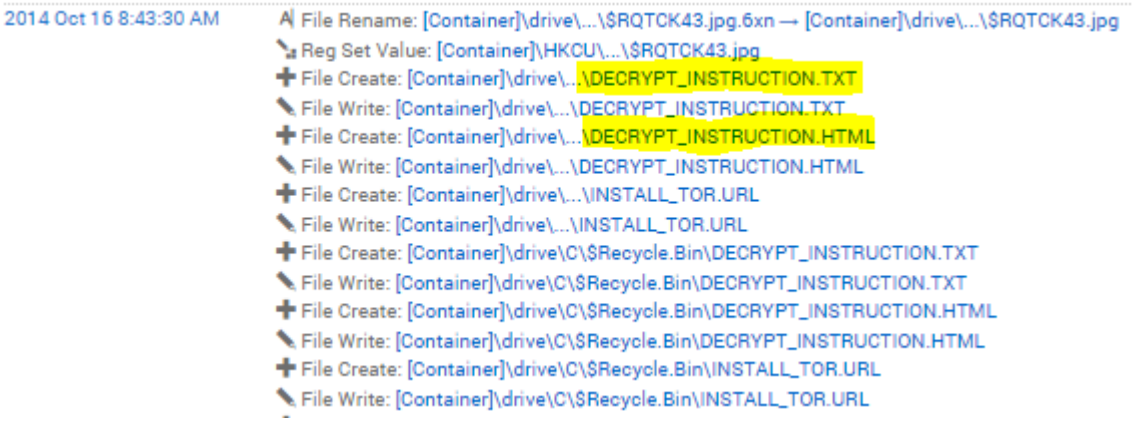


Figure 24: File writes including the ransom note from CryptoWall infection

Figure 25 shows the winning malvertising bid via RTB ad delivery from first-impression.com. Items highlighted in the URL below is userid, and the winning bid price to place malvertising of Cryptowall on sports.yahoo.com, which is 60 cents.

Figure 25: Winning malvertising bid with fields embedded in URL

In Figure 26 below, we show the unique identifiers for the userID and campaigns to deliver CryptoWall malware that were blocked and audited by Invincea, including the websites that delivered the ads via a third-party ad network over the past month.

userID, CampaignID and CommonName	Website Delivering Malvertising
748568&margin=0.4&cid=155493&bn=wheelie	Hotair.com
748568&margin=0.4&cid=155493&bn=wheeljack	webmail comcast
748163&margin=0.4&cid=155330&bn=wheeljack	theblaze.com
748566&margin=0.4&cid=155493&bn=redalert	sports.yahoo.com
746705&margin=0.4&cid=154897&bn=dc16 (unknown)	www.searchtempest.com
748480&margin=0.4&cid=155474&bn=redalert	viewmixed.com
748600&margin=0.4&cid=155528&bn=inferno	rr webmail
748418&margin=0.4&cid=155453&bn=inferno	lucianne.com
748270&margin=0.4&cid=155380&bn=sj10 (skipjack)	thanhniennews.com
748417&margin=0.4&cid=155453&bn=wheeljack	mariowiki.com

Figure 26: Malware campaigns delivered via 3rd party ad network and the websites that hosted the ads

To reiterate, neither the websites listed here, nor the 3rd party ad network, necessarily was aware of the malicious ads they were serving to the website visitors. It is likely they were not aware without ad screening technology.

In each event above, Invincea blocked an attempt to infect an endpoint with Cryptowall 2.0 and prevented CryptoWall from encrypting the user's file system and holding it hostage. Had the user not been running Invincea, the attack would likely have been successful, and the only way the user would have had to recover the encrypted files would be to pay the attacker the ransom. This is an effective ransom technique, and one that is paying off well for the attackers, who use the income from the attacks to purchase Real Time Ad Bids on RTB networks to infect more users.

Central Hosting of Clean Content

Most RTB ad providers allow for advertisers to host their own ad content. This allows advertisers to directly collect web impression data of who is hitting which ads, from where, by which IPs, which user-agent strings, and just about anything else you could log about a website visit. In addition, the advertising network doesn't have to utilize their own disk space to host the image files, the flash videos or other online content. RTB networks simply do the auctioneering and redirection to the winning content.

It is this weakness in security that malvertisers are taking advantage of. If ad networks were to switch to a model where all content is actually hosted by them (1st party hosting), in a cloud, then the risk of malvertising would drop dramatically.

The RubiconProject has a Seller's Cloud, which could be a security model for the RTB industry. It is inherently more secure way of hosting ad content.

How to Protect Yourself from Micro-targeted Malvertising

Operation DeathClick is an active campaign to micro-target companies via malvertising in order to compromise their networks. Unfortunately, the micro-targeting malvertising technique evades almost all network controls and traditional endpoint anti-virus solutions. Invincea can protect users from this attack type among other targeted and opportunistic web-based threats. For half the price of a candy bar, attackers have the unprecedented ability to deliver malware to you through your web browser simply because of your IP address space and your industry vertical. Most of the attacks featured here were not detected by standard Anti-Virus because the malware hashes constantly change.

Web proxy blocking updates, even in real time, will not stop new malvertising landing pages that appear and disappear within minutes.

Intelligence feeds from the premier intelligence providers, based on hostname, IP, URL or domain will not be able to block malicious malvertisers quickly enough.

Invincea protected users can simply browse and click anything online without fear of compromise or targeted malvertising attacks.

Non-Invincea users can attempt to OptOut of directed targeting where you can. European privacy laws for forcing most ad providers to offer the opt-out service; however, you often have to visit each ad provider individually to choose to opt out.

Note, that opting out merely places a blocking cookie in your browser. This means that ad providers will not target or retarget based on cookies. But as shown above, the new targeted advertising is via IP intelligence.

http://www.rubiconproject.com/privacy/consumer-online-profile-and-opt-out/
http://preferences-mgr.truste.com/
http://www.ghosteryenterprise.com/global-opt-out/

Release Notes

10/27: For clarification, Invincea has added additional notes in this version that the websites shown here and the 3rd party real-time ad networks are being used unwittingly and their resources misappropriated by malvertisers to target companies for persistent remote access, click fraud, and other nefarious activities. This is not a reflection on these companies, nor the services they provide. This paper highlights the problem for greater awareness so the industry collectively can combat this problem perhaps with more effective screening at the source prior to displaying ads.