Malvertisements

Darren Hobin and Rajdeep Nanua
University of Toronto

What are malvertisements?

- Malicious advertisements
- May contain malware
- Can affect legitimate websites
- Does not need user interaction
- Not much can be (or will be) done to prevent them
    - More on this later, can maybe be stopped by your or by ad networks

2,862,875

Malvertising incidents resulting in blacklisting in 2017 - RiskIQ

??%

Overall number of ad impressions is not publically available. Therefore, it’s unclear what percentage of ads this makes up. Fortunately, it likely to be very small.

Phishing

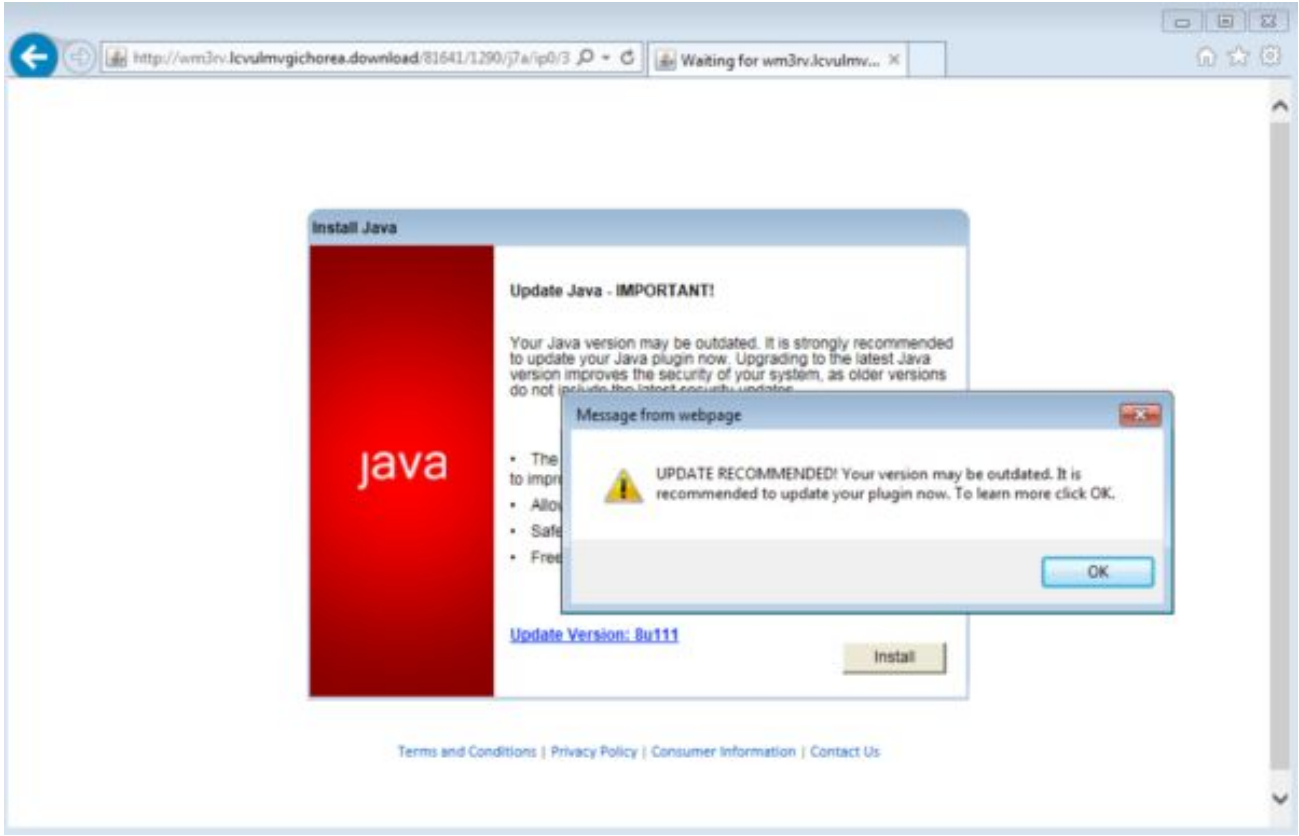
- Tricking victims into leaking personal info
- At an all time high of 3,181,155 estimated ads
- Can involve malicious redirects
  - Third-party redirects were disabled in Chrome 64 last week
- Run of the mill scams, like a voluntary survey
- Advertisement could be safe but take you to a malicious website when clicked

Malicious code

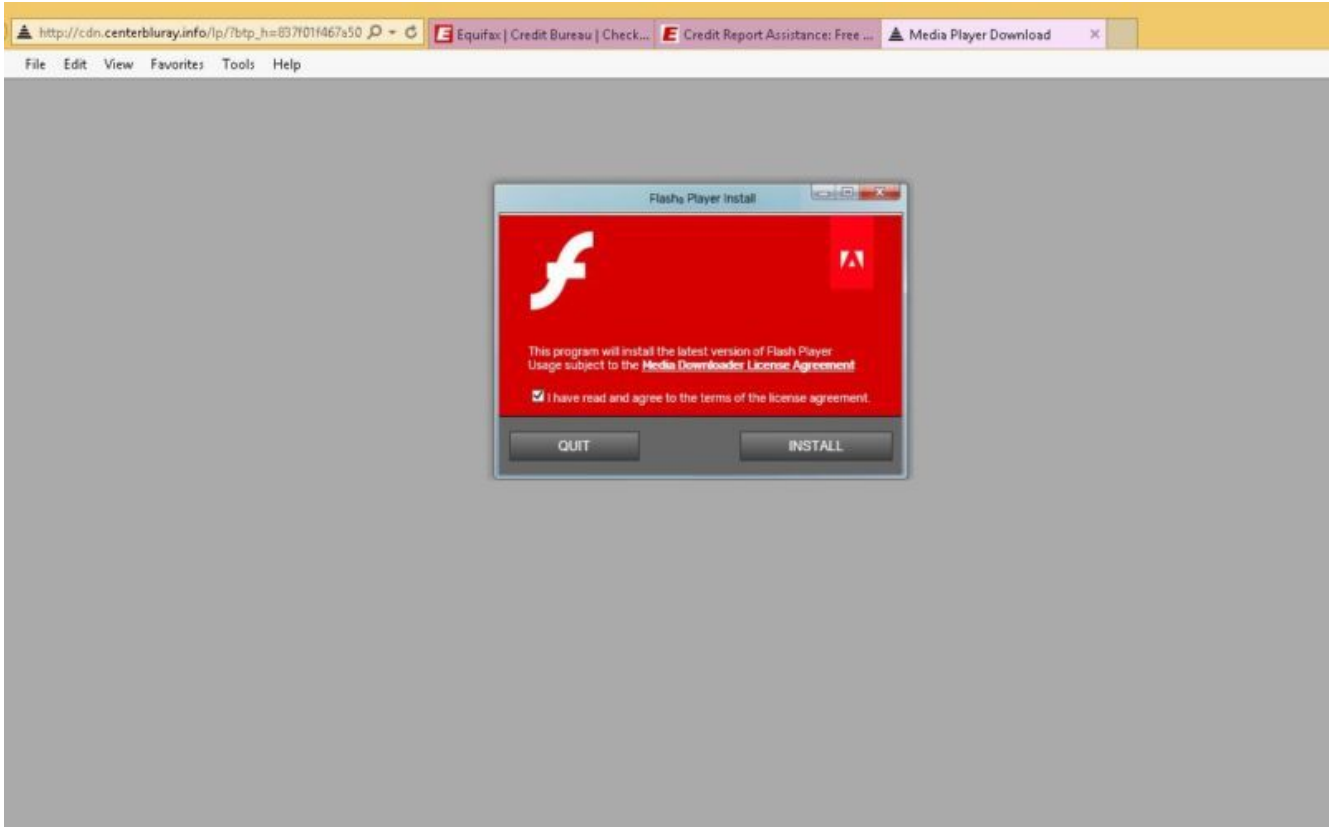
- Due to the nature of modern ads, most advertisers, including Google DoubleClick, allow advertisers to run custom JavaScript code with their ad
- This feature of modern advertising has been exploited
- Very hard to detect by advertising networks
- Hard to mitigate via browser updates
- Has been used to maliciously redirect
- Has been used to spread ransomware
- Is currently being used to mine cryptocurrency

Malicious Redirects

- macOS Flash Player redirect
- Fake Java update redirects
- App Store/iTunes redirects
- Forceful Chrome extension installations
- Surveys and other scams
- Exploit kits and ransomware (more on this in a sec)



Java update redirect



Redirect to fake Flash player install from Equifax (link to video on next slide)

Video of Flash player redirect from Equifax

Ransomware

- Recently with AdGholas using Astrum exploit kit + WannaCry
  - Exposed by ProofPoint and TrendMicro
- Typically links to a malicious website that does drive-by download
- Astrum detects if an anti-virus product is installed
- Abuses Diffie-Hellman to stop security researchers from replaying attack
- Is just an exploit kit, i.e. it targets a bunch of possible vulnerabilities
- Easy to mitigate (well, it’s easier than the others anyway)

Cryptocurrency Mining

- Trend Micro detected that Coinhive web miners tripled in the last week as the result of a malvertising campaign
- In addition to Coinhive, a custom mining tool was also used
  - Probably done to avoid commission fee
- In the foreground, a real advertisement does appear with completely safe JavaScript running the ad itself
- The campaign ran on Google DoubleClick
- Google says they’re banning such advertisers when detected, but there’s not much else that they can do
- Oh… And they typically use Monero. You all know why.

Crypto Mining Demo

Profitability of Malvertisements

- No known numbers for profit of malvertisements in general
- We can make an rough educated guess for crypto mining ads, however…
  - Based on ThePirateBay pageviews, an average view is five minutes
  - The average mid-range laptop has a hash rate of about 30 hashes per second
  - Coinhive pays about 0.00015 Monero per million hashes
  - This malvertising campaign throttled mining to 80% of CPU power
  - That's 30 x 60 x 5 x 0.8 hashes per ad impression
  - As of writing, 1 XMR ~= $275 USD
  - Or about $0.000297 USD per ad impression
  - TrendMicro detected it 22,000 times on January 24th alone
  - No estimation of number of ad impressions exist, but it is certainly more than 22,000
  - If we assume it to be 1,000,000 impressions per day, that's **$8,910 USD per month**
    - **Again, number of page impressions is purely a guess by us**

How can you prevent malvertisements?

(Yeah, I’m asking you.)

Prevention by advertising networks

- Ban advertisers once they are caught using malvertisements
  - Can be extremely hard to detect automatically
  - Ads have been known to profile users and not serve malware if the user is a bot
- Cannot restrict advertisers from using JavaScript
  - Advertisers use it to gather information about the user
  - Used to make ad look or function in a more attractive way
- Currently, ads cannot be vetted before being distributed
- Requires manual reporting, predominately by security firms
- Not much else they can do for now

Prevention by user

- Ensure your browser is always updated
  - This will help protect against some malvertisements, such as automatic redirects, but not much else
- Use an ad-blocker, such a uBlock Origin
  - Blocks all traffic using a blacklist of known domains used for advertising
    - Blacklist also often includes known malicious domains
  - Hurts content creators?
  - Might not even work, see RoughTed which uses hundreds of domains
- Block all third-party JavaScript
  - Hurts content creators less?
  - Ruins your web browsing experience
  - Sucks in general
- Not much else you can do right now

If you have nothing else to do, here are our sources...

- Malvertising Campaign Abuses Google's DoubleClick to Deliver Cryptocurrency Miner - Trend Micro
- Malvertising and crypto threats have rocketed in 2017 - High-Tech Bridge
- Tech support scammers abuse native ad and content provider Taboola to serve malvertising (updated) - MalwareBytes Labs
- AdGholas malvertising thrives in the shadows of ransomware outbreaks - MalwareBytes Labs
- AdGholas Malvertising Campaign Employs Astrum Exploit Kit - Trend Micro

If you still have nothing else to do...

- Will Astrum Fill the Vacuum in the Exploit Kit Landscape? - Trend Micro
- RoughTed: the anti ad-blocker malvertiser - MalwareBytes Labs
- How much does The Pirate Bay's cryptocurrency miner make? - ZDNet
- Equifax website borked again, this time to redirect to fake Flash update - Arstechnica