The shadow knows: Malvertising campaigns use domain shadowing to pull in Angler EK | Proofpoint US

By December 15, 2015 Proofpoint Staff

Published: 2015-12-15 · Archived: 2026-04-06 01:08:57 UTC

Most online ads are displayed as a result of a chain of trust, from the publishers to the malicious advertiser via ad agencies and/or ad networks.

For “traffers” (that is, actors bringing traffic to a malicious destination; for example, exploit kits) that rely on malvertising, one of the goals is to gain access to a high-profile ad network such as DoubleClick, Bing Ads, AdTech or AppNexus. A reputable, high-profile ad network provides traffers with access to higher-quality traffic, and the more reputable an ad network appears, the easier it is for traffers to reach this target traffic.

Uncovering domain shadowing

In early November, one of those high-profile ad agencies appeared in Proofpoint sensors as “referrer” to Angler exploit kit. Further investigation by Proofpoint researchers determined that the creative in question (ad banners) was pointing to content from https://ads.mikeholt[.]com and landing at www.mikeholt[.]com.".

Figure 1 Creative served by the abused ad agency (click to enlarge)

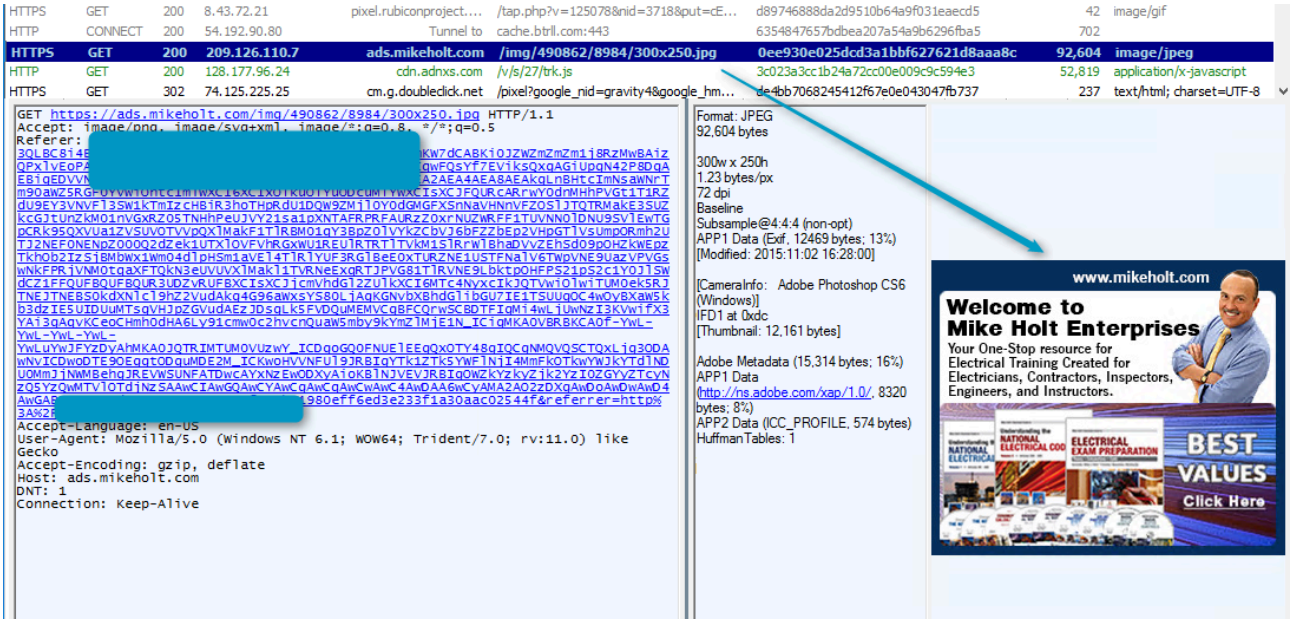


Figure 2 A fake online ad for an authentic Website, displayed using a shadowed domain of that Website

A disparity in the SSL certificate used by both servers is the first hint that something is suspicious about this ad.

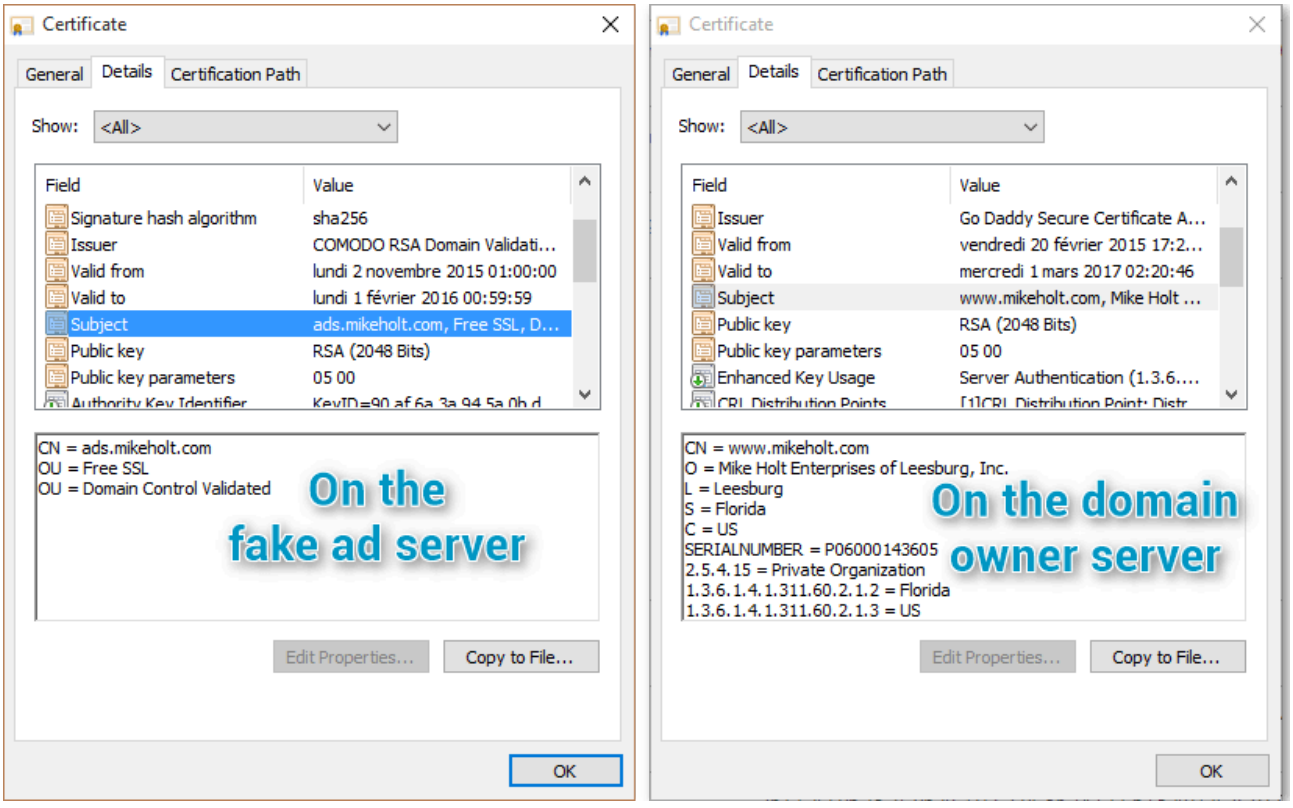


Figure 3 Shadowed domain SSL certificate vs legitimate site owner's domain SSL certificate

Comparison of the SSL certificates for two domains is a clue that this could be a case of “domain shadowing” [3].

Domain shadowing is a technique for generating malicious subdomains from a legitimate domain, typically using stolen registration credentials for the domain owner. With the stolen credentials, the threat actor can create a large

number of fraudulent subdomains (for example, ads.mikeholt[.]com) below the legitimate domain mikeholt[.]com. (The domain owners for these examples were contacted as part of this investigation and alerted to the fact that their registration credentials have probably been compromised.) The attacker can then configure servers on the fraudulent subdomain to perform filtering and redirection actions that pull in their preferred exploit kit.

Multiple parallel campaigns

Further investigation identified other campaigns employing other compromised domains and abused ad agencies. For example:

adv.mtcharlestonlodge[.]com

Figure 4: Example of ad with stolen creative linking to malicious domain

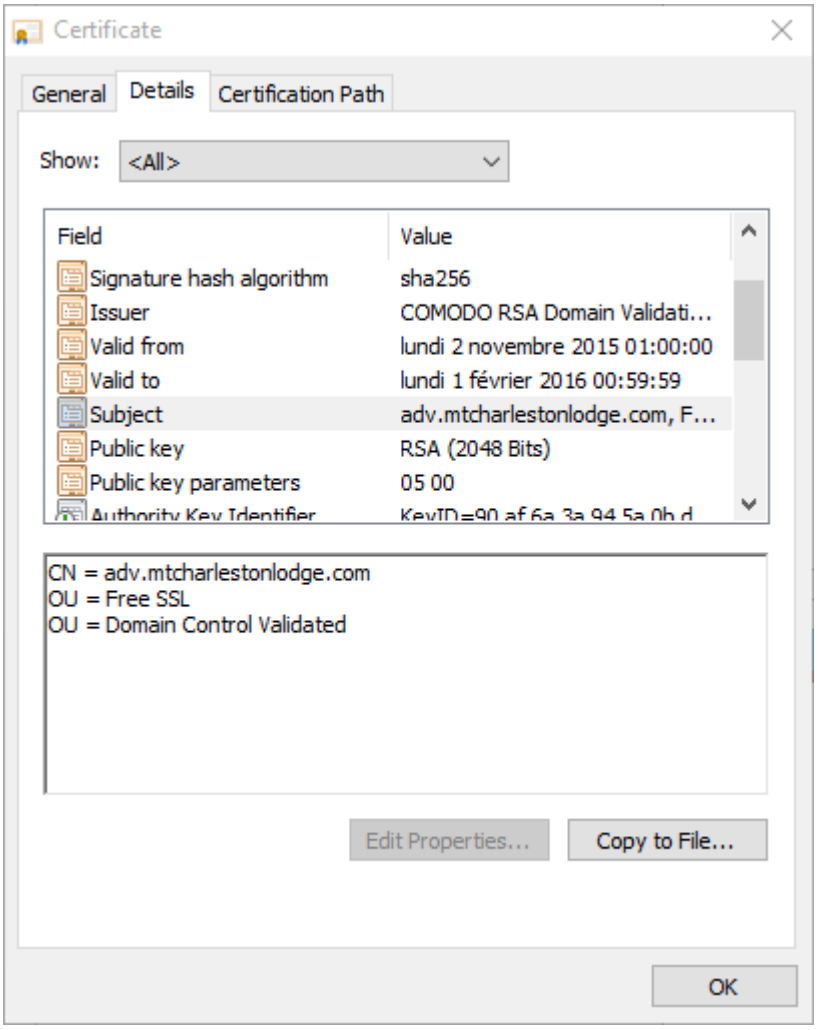
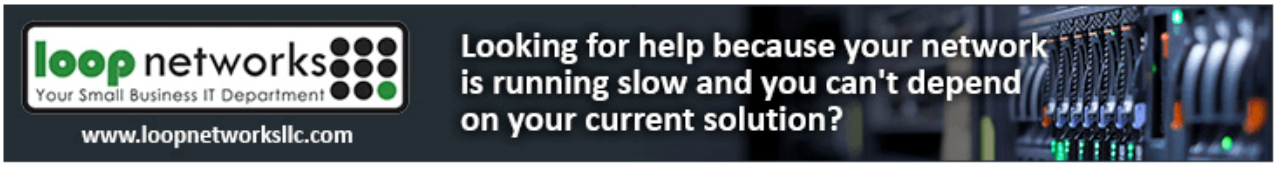


Figure 5: SSL certificate details for compromised domain

media.healthy-homemakers[.]com

promo.loopnetworksllc[.]com



An exploit kit out of nowhere

Researchers who have the opportunity to replay this attack in a controlled environment will not be able to see much without SSL man-in-the-middle capabilities (Fig 6); instead the attack will appear to be Angler EK materializing ‘out of thin air’.

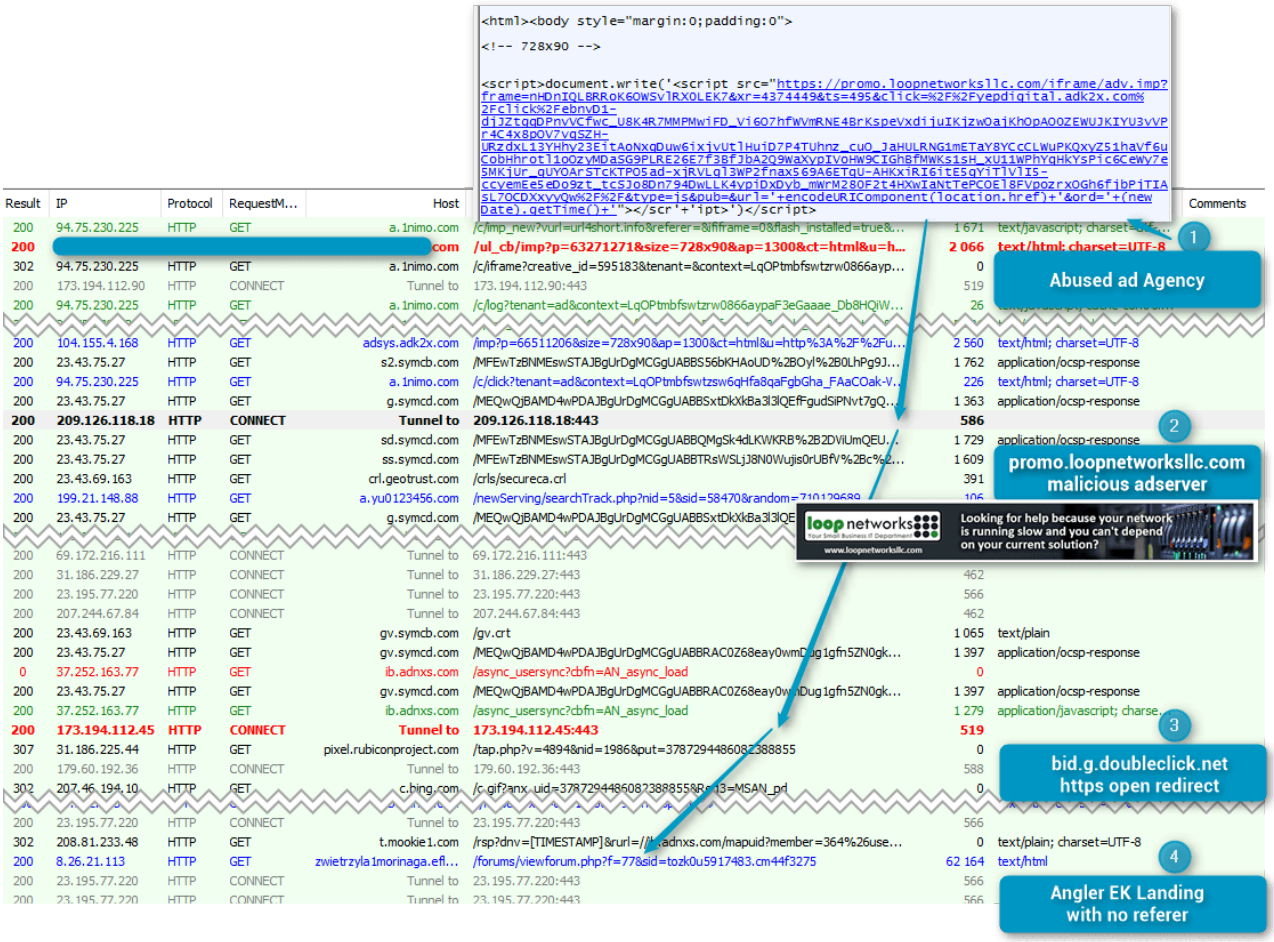


Figure 6: Traffic captured on the 2015-11-21 without MITM capabilities

A look in the SSL tunnel

One of the reasons that malvertising is appealing to threat actors is that the ad agency / network itself performs a significant portion of the targeting, including geo, browser and other options. However, the malicious ad server also includes filtering settings, and as a result non-targeted clients (such as known IP address, wrong country) will receive harmless ad code.

Figure 7: Harmless code served by the server if the client does not match the filtering options or if the campaign is on hold

When a targeted client visits a site served by the infected content delivery network (CDN), the attack follows these steps:

1. Send a post to filter proxied traffic.
2. A global JavaScript reads the results of the filtering;
3. If the reply is as expected, decode a bogus GIF (Fig. 8).
4. Check the system using two information disclosure bugs in Microsoft Internet Explorer to avoid researchers, sandboxes and some security products.
5. Abuse an HTTPS open redirect by DoubleClick. [2]
6. Land the browser on Angler EK without a referrer.

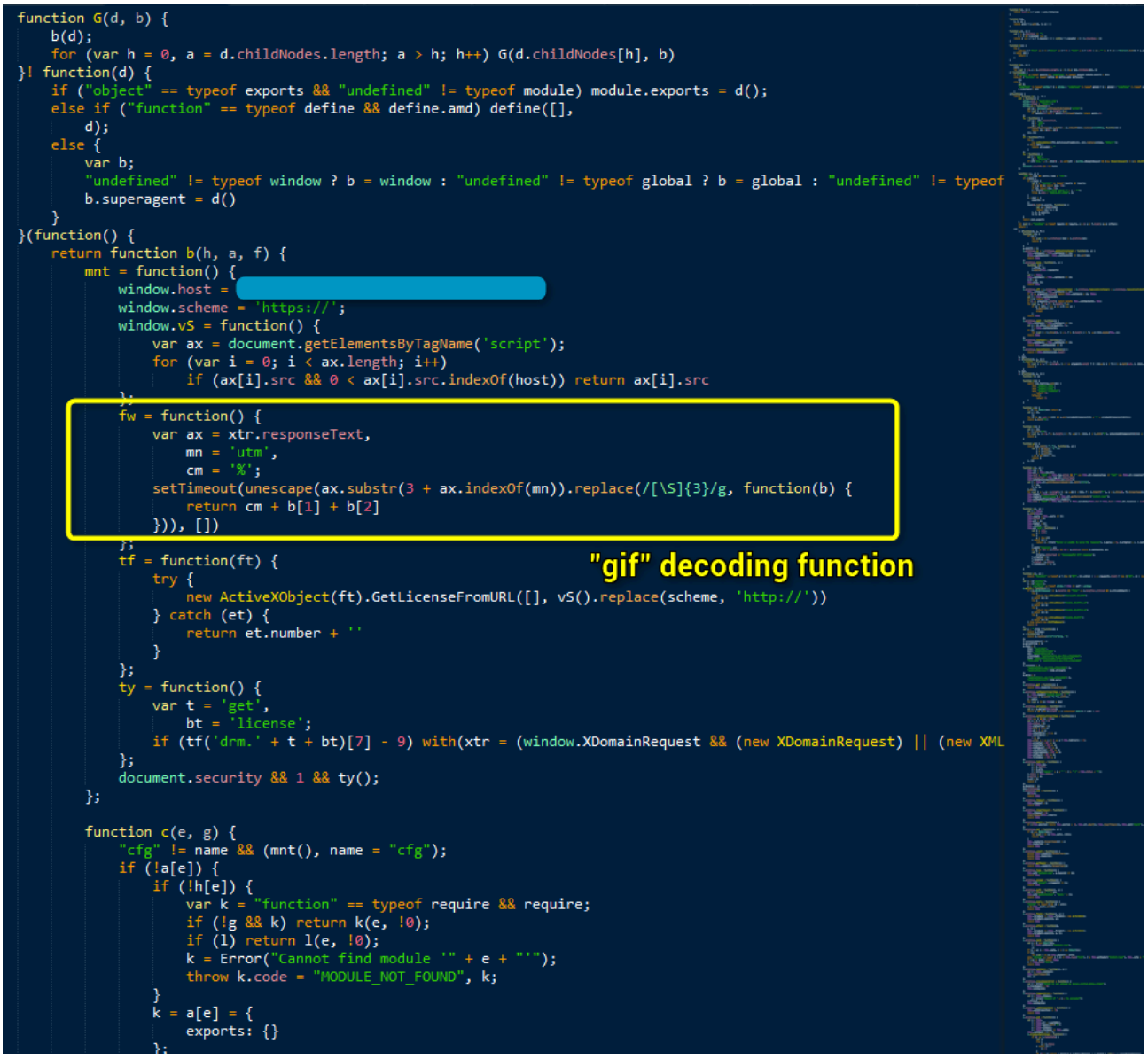


Figure 8: Malicious code sent by the fake ad server, including fake GIF image file

Decoding the fake GIF produces a JavaScript function (Fig. 9).

Figure 9: Encoded JavaScript function inside a "GIF"

Client filtering

The decoded JavaScript function leverages two information disclosure bugs in Internet Explorer in order to filtering potential victims. (Fig. 10)

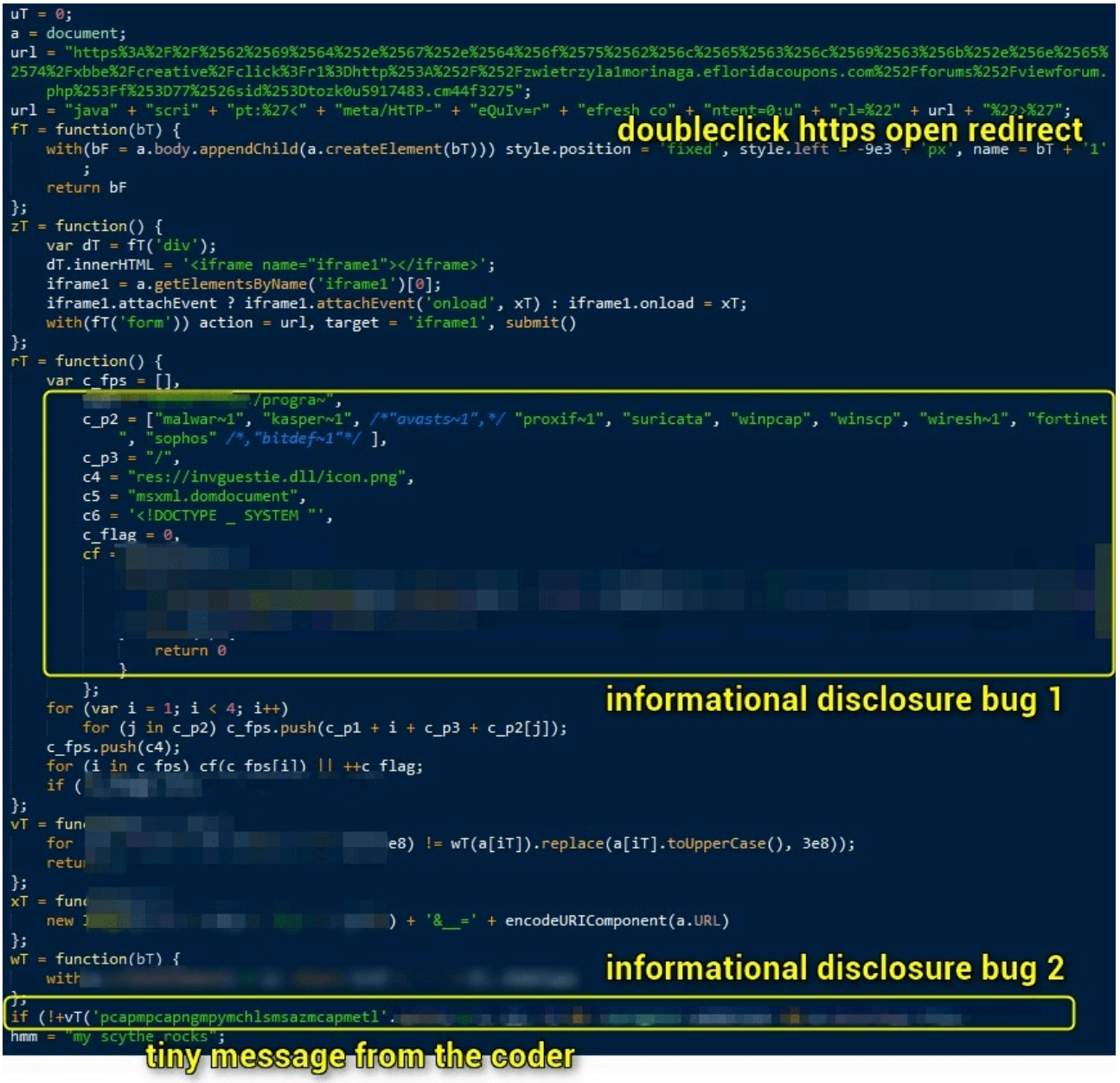


Figure 10: Decoded fake GIF showing redirect and additional filtering

In order, these checks are:

- A variation of a technique used by Magnitude and Angler EKs and is used to filter the client by certain security products.
- A MimeType check in order to filter certain shellex associations, including .py, .pcap and .saz (Fig. 10).

Both of these bugs were reported to Microsoft in May.

All replay attempts of this threat revealed fileless Angler EK [4] [5] threads loading Bedep in memory. The Bedep in action is "buildId" 1926. Over the course of November, Proofpoint researchers have observed this Bedep version loading a variety of malware payloads including Fileless Ursnif [4], Ramnit, Blowcrypt, some Vawtrak campaigns 13 and 60 [7], and most recently Reactor Bot.

Conclusion

Malvertising is by now a well-known attack vector and organizations, web sites, and ad network operators have adapted their defenses to detect and defend against it. As this example, shows, however, threat actors are also evolving their techniques, using more sophisticated attack chains that make it more difficult for even diligent ad agencies and ad network operators to detect malvertising in their ad streams. These adaptations will enable malvertising to remain an effective malware distribution method for months to come.

References

[1] https://en.wikipedia.org/wiki/Online_advertising

[2] http://malware.dontneedcoffee.com/2015/10/a-doubleclick-https-open-redirect-used.html

[3] http://blogs.cisco.com/security/talos/angler-domain-shadowing

[4] http://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html

[5] https://hiddencodes.wordpress.com/2014/10/01/digging-deep-into-angler-fileless-exploit-delivery-2/

[6] http://malware.dontneedcoffee.com/2015/07/a-fileless-ursnif-doing-some-pos.html

[7] https://www.proofpoint.com/us/threat-insight/post/In-The-Shadows

Indicators of Compromise (IOC's)

ads.mikeholt[.]com	209.126.110.7	Shadowed domain
adv.mtcharlestonlodge[.]com	209.126.118.13	Shadowed domain
media.healthy-homemakers[.]com	209.126.118.11	Shadowed domain
promo.loopnetworksllc[.]com	209.126.118.18	Shadowed domain
delivery.dpis[.]com	209.126.118.18	Shadowed domain
promo.socialmagnetmarketing[.]com	209.126.118.14	Shadowed domain
POS Reco "Fileless" Ursnif	c1bc86552e558cc37ee7df3a16ef8ac7	2015-11-22

Ramnit	2839b5e418adc25b0d3a2b9bd04efb99	2015-11-21
Blocrypt	d37994ac8bb0df034d942c10ae471094	2015-11-07
Vawtrak 13	2408e9df8cb82e575002176a4dcd69a5	2015-11-15
Vawtrak 60	d3670b3a2bba2ff92f2e7cbfc63be941	2015-11-21
Reactor Bot	b37717d09b61cbfe5c023e8d5fd968ed	2015-11-23
ninthclub[.]com	81.177.22.179	Vawtrak C&C
atlasbeta[.]com	176.9.188.147	Vawtrak C&C
alutqlyzoxglge7s[.]com	95.211.205.229	Bedep Domain
browneyandrebun[.]net	107.170.83.113	Ursnif C&C
zwietrzyla1morinaga.efloridacoupons[.]com	8.26.21.113	Angler EK
cloud75[.].eu	51.255.59.117	Reactor Bot C&C

ET signatures:

(NOTE: older rules would fire on older traffic)

2018558 || ET TROJAN Win32/Ramnit Checkin

2019678 || ET TROJAN Ursnif Checkin

2019400 || ET TROJAN Possible Bedep Connectivity Check

2021418 || ET TROJAN Bedep HTTP POST CnC Beacon

2022141 || ET CURRENT_EVENTS Angler encrypted payload Nov 23

2811284 || ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2

2814948 || ETPRO CURRENT_EVENTS Possible EK Redir SSL Cert

2815003 || ETPRO CURRENT_EVENTS Angler EK Landing Nov 18 2015

2815071 || ETPRO CURRENT_EVENTS Possible Angler EK Payload Nov 23 2015

2814630 || ETPRO CURRENT_EVENTS Possible Angler EK IE DHE Post M2

2807957 || ETPRO TROJAN Win32/TrojanDownloader.Blocrypt Checkin

2814112 || ETPRO TROJAN Vawtrak HTTP CnC Beacon

2813060 || ETPRO TROJAN Vawtrak Retrieving Module
