Amerandus
RESEARCH

Digital Communications Security Assessment of a Qui Tam Law Firm and Its Associated Whistleblower Website

This report provides the results of some tests of the encryption and other aspects of security for a *qui tam* law firm, K------ of Washington, D.C., and their associated whistleblower support entity, the N----------- W----------------- C-------.

This report was produced as part of an on-going effort with a variety of law firms to improve the confidentiality of information submitted by potential whistleblowers and other clients.

Verbal notice of several of these findings was given by one of the authors (--) to one of the K-- principals (S------ K---) during the last three months of 2015. We now present this information in a written form to K-----. W e hope to discuss the implications and potential solutions to these issues in a conference call (week of -).

G------- N------

Network Security Expert (multiple SANS certifications)

R----- B--------

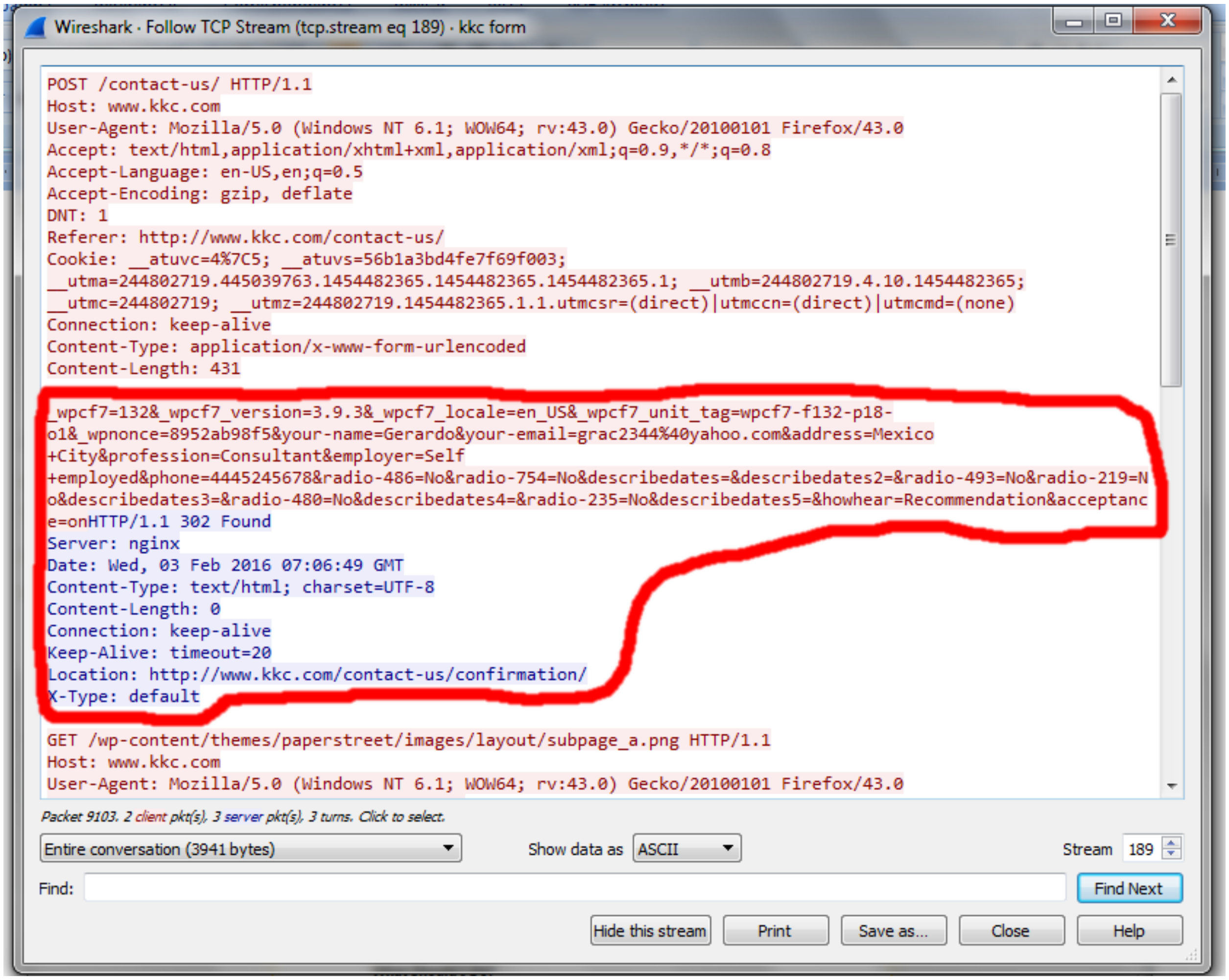
(CompTIA Security+ certification)

February 2, 2016

Contact form for KKC.COM

The following summarizes the security posture regarding kkc.com contact form as of February 2, 2016:

1. There is no encryption whatsoever. The form is sent in plain http and any information posted on the form is sent back to the site unencrypted. This conclusion is based on a test done against the formulary and intercepting the traffic using Wireshark 2.0.1



Wireshark · Follow TCP Stream (tcp.stream eq 189) · kkc form

```
POST /contact-us/ HTTP/1.1
Host: www.kkc.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://www.kkc.com/contact-us/
Cookie: __atuvc=4%7C5; __atuvs=56b1a3bd4fe7f69f003;
__utma=244802719.445039763.1454482365.1454482365.1454482365.1; __utmb=244802719.4.10.1454482365;
__utmc=244802719; __utmz=244802719.1454482365.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 431

_wpcf7=132&_wpcf7_version=3.9.3&_wpcf7_locale=en_US&_wpcf7_unit_tag=wpcf7-f132-p18-
o1&_wpnonce=8952ab98f5&your-name=Gerardo&your-email=grac2344%40yahoo.com&address=Mexico
+City&profession=Consultant&employer=Self
+employed&phone=4445245678&radio-486=No&radio-754=No&describedates=&describedates2=&radio-493=No&radio-219=N
o&describedates3=&radio-480=No&describedates4=&radio-235=No&describedates5=&howhear=Recommendation&acceptanc
e=onHTTP/1.1 302 Found
Server: nginx
Date: Wed, 03 Feb 2016 07:06:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=20
Location: http://www.kkc.com/contact-us/confirmation/
X-Type: default

GET /wp-content/themes/paperstreet/images/layout/subpage_a.png HTTP/1.1
Host: www.kkc.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0
```

Packet 9103. 2 client pkt(s), 3 server pkt(s), 3 turns. Click to select.

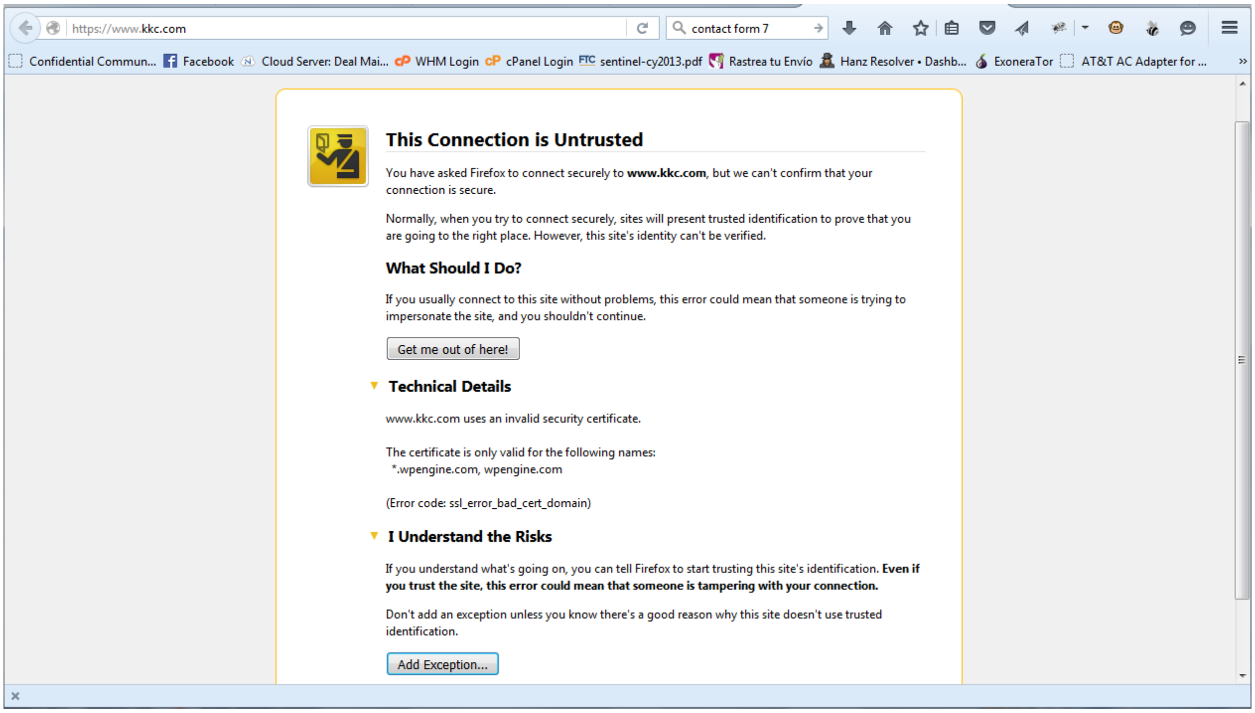
Entire conversation (3941 bytes) | Show data as: ASCII | Stream: 189

The red mark shows how the information is being sent in plain text:

```
_wpcf7=132&_wpcf7_version=3.9.3&_wpcf7_locale=en_US&_wpcf7_unit_tag=wpcf7-
f132-p18-o1&_wpnonce=8952ab98f5&your-name=Gerardo&your-
email=grac2344%40yahoo.com&address=Mexico+City&profession=Consultant&employer=
Self+employed&phone=4445245678&radio-486=No&radio-
754=No&describedates=&describedates2=&radio-493=No&radio-
219=No&describedates3=&radio-480=No&describedates4=&radio-
235=No&describedates5=&howhear=Recommendation&acceptance=on
```

In fact, we can get other information that will be useful to an attacker: the site is Word press based site and it's using a plug-in known as Contact Form 7 (https://es.wordpress.org/plugins/contact-form-7/). This form doesn't provide any kind of encryption, at least based on what was seen in the test. Furthermore, as the website doesn't have an https version (see following), we would expect that all communication back and forth through the KKC website would be easy to intercept

2. Connecting to https://www.kkc.com (forcing the site to use https) gives the following warning regarding the secure connection:



https://www.kkc.com
contact form 7
Confidential Commun... Facebook Cloud Server: Deal Mai... WHM Login cPanel Login sentinel-cy2013.pdf Rastrea tu Envío Hanz Resolver • Dashb... ExoneraTor AT&T AC Adapter for ...

This Connection is Untrusted

You have asked Firefox to connect securely to **www.kkc.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

www.kkc.com uses an invalid security certificate.

The certificate is only valid for the following names:
*.wpengine.com, wpengine.com

(Error code: ssl_error_bad_cert_domain)

I Understand the Risks

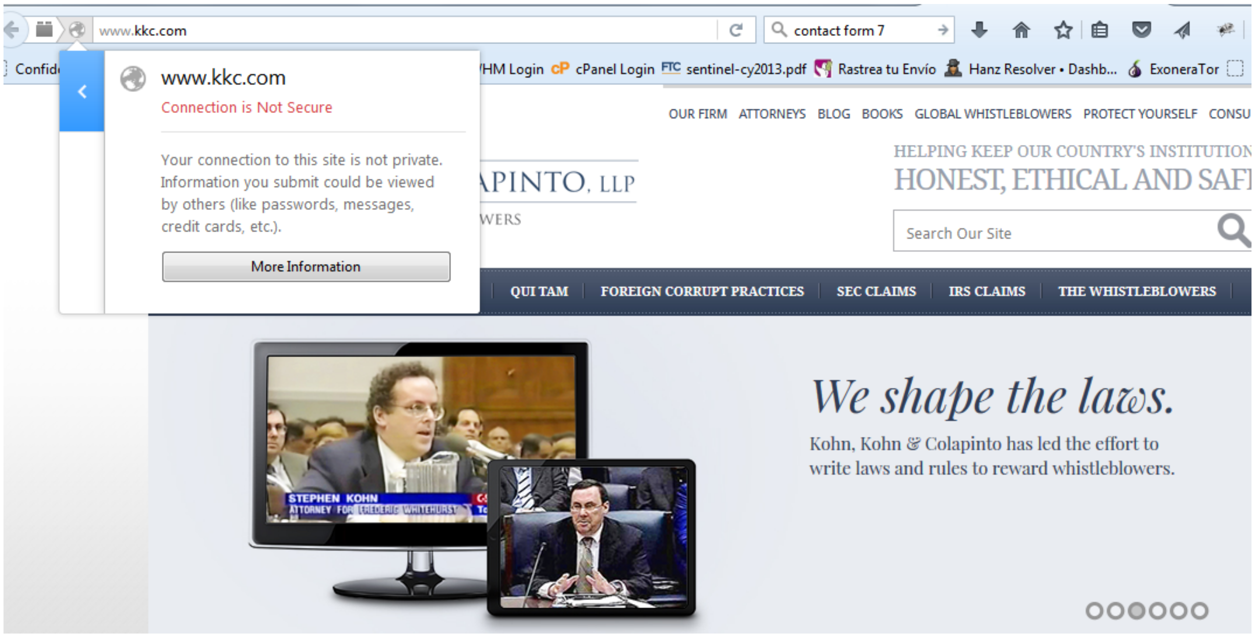
If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

The warning indicates that there is a mismatch between the website name and the certificate and hence the Error code: ssl_error_bad_cert_domain. Also the certificate being send by the website is for *.wpengine.com or wpengine.com, confirming the use of a Word Press site at wpengine.com (a premium WordPress hosting provider).

Once the exception is added in order to continue browsing to the site, we are redirected to an http version (unsecured), as confirmed in the following screen capture:



www.kkc.com

Connection is Not Secure

Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

More Information

We shape the laws.

Kohn, Kohn & Colapinto has led the effort to write laws and rules to reward whistleblowers.

The reason of this behavior usually is based on the lack of a proper ssl certificate on the website as mentioned in the following blog page of the host provider (https://wpengine.com/support/why-am-i-seeing-a-certificate-error-for-wpengine-com/).

3. The source code indicates that the contact form page is using Google web analytics to track usage of the page:

```
<script type="text/javascript">
  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-16024912-1']);
  _gaq.push(['_trackPageview']);

  (function() {
    var    ga    =    document.createElement('script');    ga.type    =
'text/javascript'; ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' :
'http://www') + '.google-analytics.com/ga.js';
    var      s      =      document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(ga, s);
  })();
</script>
```

This piece of code is nearly identical to one found in:

https://developers.google.com/analytics/devguides/collection/gajs/

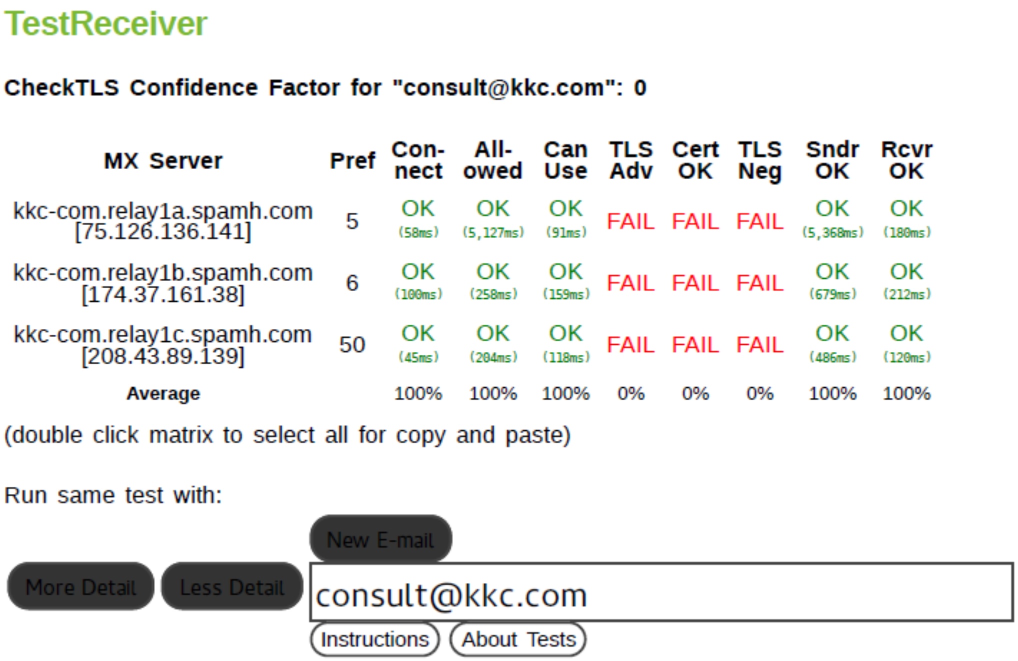
The link offers a detailed description of what it does.

A company that is dedicated to preserving the identity and communications of whistleblowers in as confidential a manner as possible must ask if this web form structure should be avoided.

4. In terms of security use of wpengine.com is a bad choice for a high security communication channel because its overall security is based on whatever the hosting provider offers and because is often a one size fits all approach, since the security measures should be shared across all the sites hosted on the same platform.

KKC email

5. The failure of passing a checktls.com test on KKC's email also indicates that such emails would be expected to be totally unsecure and potentially intercepted with ease



TestReceiver

CheckTLS Confidence Factor for "consult@kkc.com": 0

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
kkc-com.relay1a.spamh.com [75.126.136.141]	5	OK (58ms)	OK (5,127ms)	OK (91ms)	FAIL	FAIL	FAIL	OK (5,368ms)	OK (180ms)
kkc-com.relay1b.spamh.com [174.37.161.38]	6	OK (100ms)	OK (258ms)	OK (159ms)	FAIL	FAIL	FAIL	OK (679ms)	OK (212ms)
kkc-com.relay1c.spamh.com [208.43.89.139]	50	OK (45ms)	OK (204ms)	OK (118ms)	FAIL	FAIL	FAIL	OK (486ms)	OK (120ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

(double click matrix to select all for copy and paste)

Run same test with:

consult@kkc.com

Conclusion

a. Move the site at least to a Virtual Private Server, or if the security really requires it, to dedicated server. Both options allows more flexibility in hardening and maintaining the security posture of the client's website

b. Obtain advice or hire a third party to be in charge of the security architecture of their infrastructure based on their security requirements and policy.

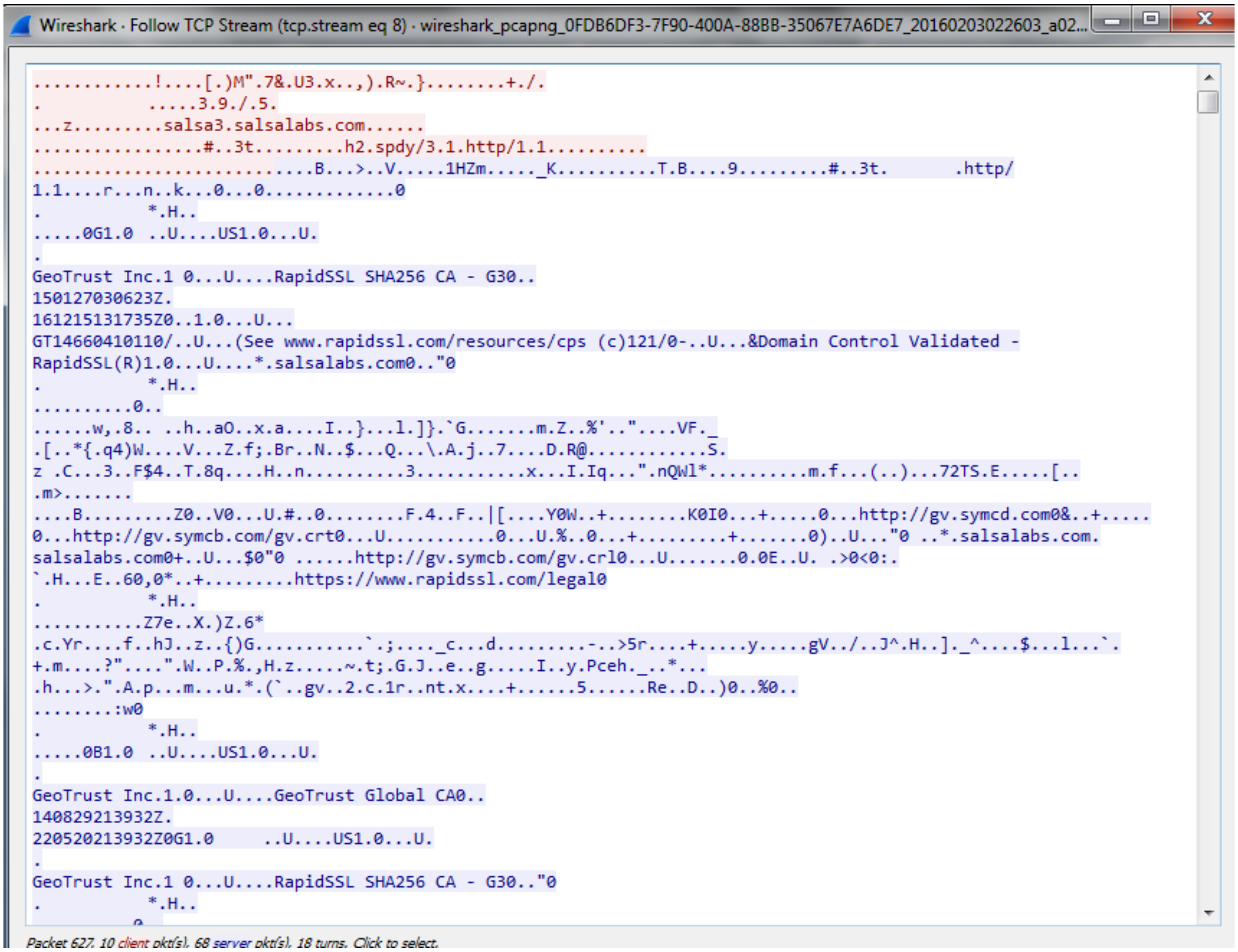
c. Review the causes for not supporting secure email and fix them.

d. Make an in depth security assessment, including security policies and procedures, auditing infrastructure, and pen testing of high risk elements such as mail and web servers. This can be done by stages once the scope and requirements are defined

Contact Form for NWC

The National Whistleblower Center (NWC) contact form resides on a domain named salsa3.salsalabs.com. This could cause confusion for a potential user since he or she would be expecting to see http://www.whistleblowers.org. Mr. Kohn told Dr. Bauchwitz that NWC was outsourcing the contact form to the Salsa Labs provider. Dr. Bauchwitz subsequently spoke with Salsa Labs about email security (see below).

The connection to the NWC form is encrypted as shown in the following Wireshark capture:


Wireshark · Follow TCP Stream (tcp.stream eq 8) · wireshark_pcapng_0FDB6DF3-7F90-400A-88BB-35067E7A6DE7_20160203022603_a02...

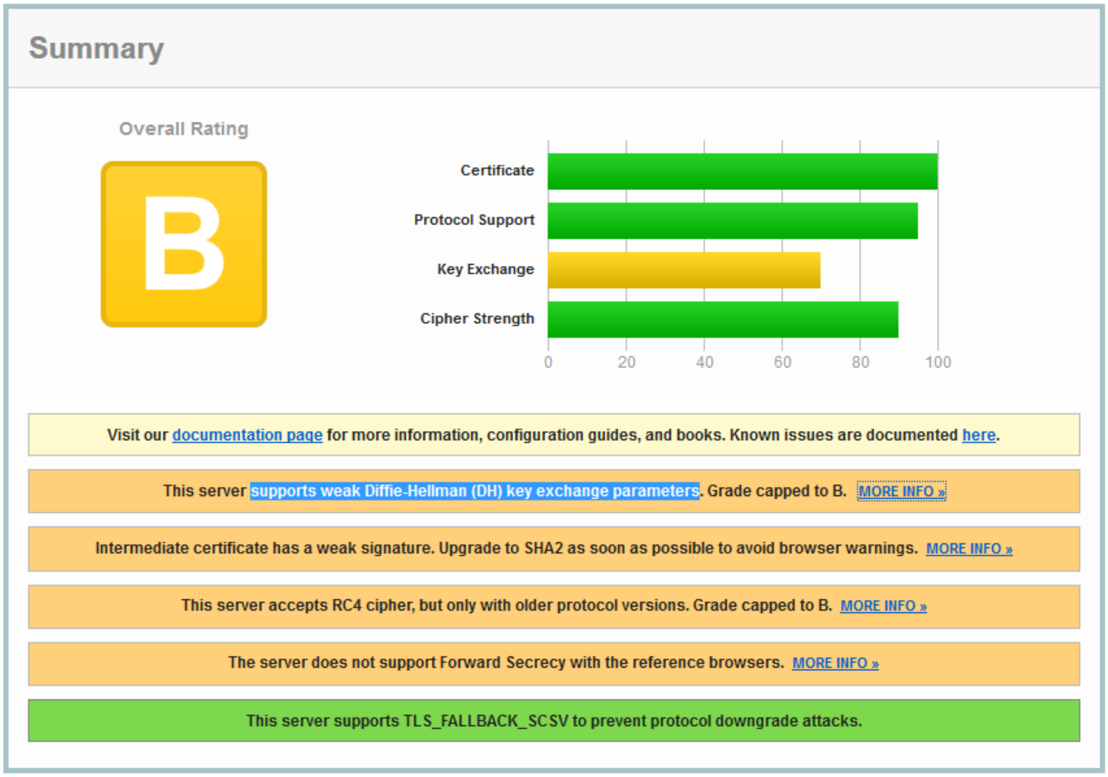
```
............!....[.)M".7&.U3.x..,).R~.}........+./.
.           .....3.9./.5.
...z.........salsa3.salsalabs.com......
.................#..3t.........h2.spdy/3.1.http/1.1..........
..........................B...>..V.....1HZm....._K..........T.B....9.........#..3t.      .http/
1.1....r...n..k...0...0.............0
.           *.H..
.....0G1.0  ..U....US1.0...U.
.
GeoTrust Inc.1 0...U....RapidSSL SHA256 CA - G30..
150127030623Z.
161215131735Z0..1.0...U...
GT14660410110/..U...(See www.rapidssl.com/resources/cps (c)121/0-..U...&Domain Control Validated -
RapidSSL(R)1.0...U....*.salsalabs.com0.."0
.           *.H..
..........0..
......w,.8.. ..h..aO..x.a....I..}...l.]}.`G.......m.Z..%'.."....VF._
.[..*{.q4)W....V...Z.f;.Br..N..$...Q...\.A.j..7....D.R@...........S.
z .C...3..F$4..T.8q....H..n..........3...........x...I.Iq...".nQWl*..........m.f...(..)...72TS.E.....[..
.m>.......
....B.........Z0..V0...U.#..0........F.4..F..|[....Y0W..+........K0I0...+.....0...http://gv.symcd.com0&..+.....
0...http://gv.symcb.com/gv.crt0...U...........0...U.%..0...+.........+.......0)..U..."0 ..*.salsalabs.com.
salsalabs.com0+..U...$0"0 ......http://gv.symcb.com/gv.crl0...U.......0.0E..U. .>0<0:.
`.H...E..60,0*..+.........https://www.rapidssl.com/legal0
.           *.H..
...........Z7e..X.)Z.6*
.c.Yr....f..hJ..z..{)G...........`.;...._c...d.........-..>5r....+.....y.....gV../..J^.H..]._^....$...l...`.
+.m....?"....".W..P.%.,H.z.....~.t;.G.J..e..g.....I..y.Pceh._..*...
.h...>.".A.p...m...u.*.(`..gv..2.c.1r..nt.x....+......5......Re..D..)0..%0..
........:w0
.           *.H..
.....0B1.0  ..U....US1.0...U.
.
GeoTrust Inc.1.0...U....GeoTrust Global CA0..
140829213932Z.
220520213932Z0G1.0     ..U....US1.0...U.
.
GeoTrust Inc.1 0...U....RapidSSL SHA256 CA - G30.."0
.           *.H..
           0
```

Packet 627. 10 client pkt(s), 68 server pkt(s), 18 turns. Click to select.

Because most of the information is encrypted, its interception should be made more difficult.

The source code that was provided is custom code. The analysis of this code is beyond the scope of this report.

Results from QualysSSL Labs (www.ssllabs.com) tests indicates that there is a room to improve the handling of the secure channel by Salsa Labs, in particular its support for weak Diffie-Hellman (DH) key exchange parameters



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

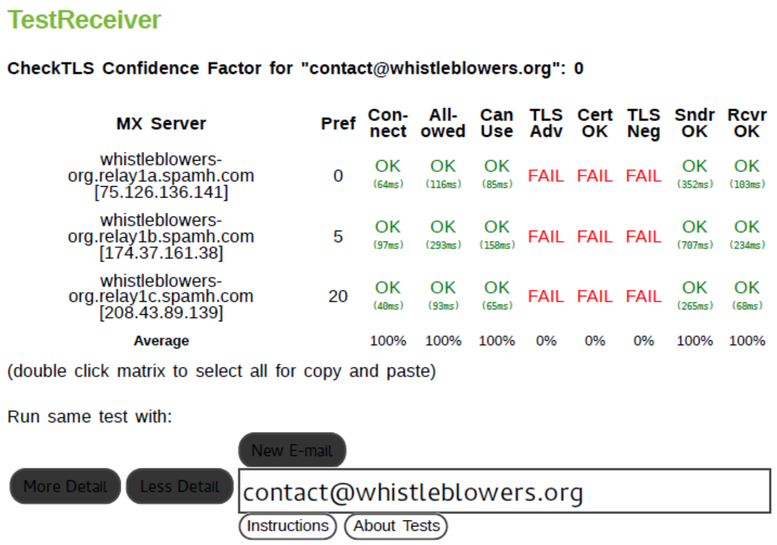
This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

The server hosting the contact form is vulnerable to the **logjam attack**. A detailed description can be found at https://weakdh.org/. The fundamental risk is that a server with this vulnerability can have its communications decrypted. Such attacks seem to have been achieved by state-level adversaries, which could have implications for those whistleblowers with potential cases involving such governments.

NWC email also failed to pass checktls.com tests. As noted for the KKC emails, such results indicate that information being sent by potential whistleblowers to the email adresses shown on the NWC webpages are not secure and could be intercepted with ease



TestReceiver

CheckTLS Confidence Factor for "contact@whistleblowers.org": 0

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
whistleblowers-org.relay1a.spamh.com [75.126.136.141]	0	OK (64ms)	OK (116ms)	OK (85ms)	FAIL	FAIL	FAIL	OK (352ms)	OK (103ms)
whistleblowers-org.relay1b.spamh.com [174.37.161.38]	5	OK (97ms)	OK (293ms)	OK (158ms)	FAIL	FAIL	FAIL	OK (707ms)	OK (234ms)
whistleblowers-org.relay1c.spamh.com [208.43.89.139]	20	OK (40ms)	OK (93ms)	OK (65ms)	FAIL	FAIL	FAIL	OK (265ms)	OK (68ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%

(double click matrix to select all for copy and paste)

Run same test with:

contact@whistleblowers.org

Conclusion

a. Review the NWC (Salsa Labs) server ssh/https configuration in order to eliminate the vulnerabilities reported by the test. A high security site must look to achieve an A/A+ grade.
b. Review the causes for not supporting secure email and fix them.
c. Make an in depth security assessment, including security policies and procedures, auditing infrastructure, and pen testing of high risk elements such as email and web servers. This can be done by stages once the scope and requirements are defined.

Amerandus Research

BNY Mellon Center

1735 Market Street, Suite 3750

Philadelphia, PA 19103

director-netsec_AT_ amerares.com

215-586-4944