#DontTrustTheDarkSide

@c0rdis

OWASP EEE - Bucharest
Whoami

Luke Skywalker in EY

OWASP Russia Chapter Leader, co-org of EEE
Darkweb

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.
Darkweb

Picture from http://jordan-wright.com/
Darkweb

„... unfortunately for thrill-seekers, almost all the sites purporting to offer this type of content far have turned out to be fake, be that live streams of torture, hitmen for hire, or human trafficking.

In reality, the dark web is a relatively tiny collection of difficult-to-reach sites, that, for criminals, deal in drugs, weapons, stolen data, and child pornography. On the brighter side, are sites for dropping sensitive documents to journalists, and that page that just endlessly tells cat jokes.”

Some known darknet attacks

- Controlling nodes (MitM/traffic confirmation/timing/correlation attacks)
- Exploits against Flash/FF/...
- Vulnerable protocols
Approach

- Conventionally low-risk vulnerabilities of all kinds of information disclosure
- In a normal pentest that would rather be marked as recommended
- In darknet it can be game over for one’s privacy
Similar research

- Hyperion Gray – Mass 'Dark Web' Scanning with PunkSPIDER

Outcomes:

- hidden service web apps are actually reasonably secure as a general whole
- hidden services aren't trivial to attack in an automated way reliably, decreasing the effectiveness of script kiddies
- vulnerabilities do exist in hidden services (maybe this was obvious) and they can have a serious impact on privacy
Similar research

• @cthulhusec

@thegrugq @thegrugq · Aug 22
“@c0rdis: Deanonymization made simple: aan.sh/Ob2M” << same techniques that @CthulhuSec uses in his blog post. Cool

RETWEETS 23
FAVORITES 24
How it all started
Instant win

- /phpinfo.php ~ 1% (10 out of 1000)
- /server-info ~ 0% (1 out of 1000, rather exception)

Who really puts a phpinfo file at the root of their server? Nice try though. In the meantime try learning some hacking.
Redirects

- Generally bad practice of having clear- and darknet services enabled at the same time (we will see it many times today 😊)
- Simple access to the IP address may lead to fail
Shodan

- Lazy bastard way
General appsec

- Nothing really new
- Access to the server (SQLi, command injection, upload restrictions bypass and so on) → privacy
Special word for /server-status

- 7% of the known darkweb (≈500 out of 7000)
Special word for /server-status

127.0.1.1:80 NULL
127.0.1.1:80 GET /index.php?q=Mushroom+kingdom&session=536976303&numRo
127.0.1.1:80 GET /server-status HTTP/1.1
127.0.1.1:80 OPTIONS * HTTP/1.0
127.0.1.1:80 OPTIONS * HTTP/1.0

Variant of Dark Google
Special word for /server-status

- “About 2% of the known darknet is controlled by one organization” ≈ 350 out of 7000
- Would you really trust your identity to someone else?
- ... especially if it might be (IS) vulnerable? 😊
Special word for /server-status

- "It works!"/"Forbidden" on your IP address access?
- Bots/scanners → full GET-request along real IP-address
- If “deanonymizer” accesses it, it will be reflected too!
  - Zmap / Masscan / your variant of global scanner
  - Monitor

Your scanner’s IP
Real hidden IP
Special word for /server-status

- Clients of such services might be vulnerable even if no clearnet accesses were made! (if no real IP addresses were logged)
- Example: poor auth scheme with "key" as a unique identifier

127.0.0.1 apple.onion:8082   GET /?page_id=6&order-received=520&key=wc_order_

- Guess what happens next.
Special word for /server-status
Some better examples?
Your riseup.net email account is a wonderful thing. Although we don't provide as much storage quota as surveillance-funded corporate email providers, riseup.net email has many unusual features: <...> we do not log internet addresses of anyone using riseup.net services, including email.

- [http://cwoiopiifrlzcuos.onion/server-status](http://cwoiopiifrlzcuos.onion/server-status) - black.*, api.black.*
- [http://zsolxunfmbfuq7wf.onion/server-status](http://zsolxunfmbfuq7wf.onion/server-status) - cotinga.*, mail.*
- [http://yfm6sdhnbulpsew.onion/server-status](http://yfm6sdhnbulpsew.onion/server-status) - labs.*, bugs.otr.im*
- [http://xpgylzydxykgdqvq.onion/server-status](http://xpgylzydxykgdqvq.onion/server-status) - lists.*, whimbrel.*
- [http://j6uhdvbhz74oefxf.onion/server-status](http://j6uhdvbhz74oefxf.onion/server-status) - user.*
- [http://7lvd7fa5yfbdqaii.onion/server-status](http://7lvd7fa5yfbdqaii.onion/server-status) - we.*
Riseup has three types of accounts sorted by security level: **GREEN** (lists, wiki), **RED** (email, shell, OpenVPN) and **BLACK** (Bitmask enhanced security). In this section I will concentrate on red and black accounts, since green ones do not seem to have that much importance in terms of privacy.

**RED**: currently logged in user, and his actions
**BLACK**: correlation between real user login and his unique hash ID, which is used later to anonymize all the activities he makes.

```plaintext
127.0.0.1 api.black.riseup.net   GET /users/677f7ad7b5849c7f28e32259876746ce HTTP/1.1
127.0.0.1 api.black.riseup.net   POST /1/sessions.json HTTP/1.1
127.0.0.1 cwoiopiifrlzuos.onion GET /server-status HTTP/1.1
127.0.0.1 api.black.riseup.net   PUT /1/sessions/c0rdis.json HTTP/1.1
```
**RED** : remote IP address of the current user, his actions and address book contacts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Port</th>
<th>Request Details</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>GET</td>
<td>/rc/skins/larry/images/listicons.png?v=1877.13442</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>GET</td>
<td>/rc/program/js/common.min.js?z=1433508438</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>POST</td>
<td>/rc/?_task=mail&amp;_action=refresh</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>GET</td>
<td>/rc/?_task=addressbook&amp;_action=photo&amp;_email=joha%40riseup.n</td>
<td>NULL</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>209.105.152</td>
<td>mail.riseup.net:443</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>POST</td>
<td>/rc/?_task=mail&amp;_action=refresh</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>POST</td>
<td>/rc/?_task=mail&amp;_action=refresh</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>POST</td>
<td>/rc/?_task=settings&amp;_action=refresh</td>
<td>HTTP/1.1</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>mail.riseup.net:443</td>
<td>POST</td>
<td>/rc/?_task=mail&amp;_action=refresh</td>
<td>HTTP/1.1</td>
</tr>
</tbody>
</table>
One of the largest Russian mobile operators. In this case, it was set of old subscription services along with WAP.

Apache Server Status for 6lp4oyoooup5zatu.onion

Server Version: Apache/2.2.15 (Unix) DAV/2 mod_ssl/2.2.15 OpenSSL/1.0.0-fips
Server Built: Apr 29 2013 04:13:12

Current Time: Thursday, 17-Sep-2015 00:25:13 MSK
Restart Time: Tuesday, 01-Sep-2015 12:42:42 MSK
Parent Server Generation: 0
Server uptime: 15 days 11 hours 42 minutes 30 seconds
Total accesses: 300902578 - Total Traffic: 1386.4 GB
CPU Usage: u764.28 s444.21 cu10.33 cs0 - .0911% CPU load
225 requests/sec - 1.1 MB/second - 4947 B/request
277 requests currently being processed, 58 idle workers
Admin credentials to vulnerable services

Disclaimer: admin credentials were not used by me to break into the system, however, log analysis has shown that further attack on other Megafon systems is very likely from there.
Several more examples...
Something is wrong here...

Took me 10 minutes to found what's wrong with this picture
Zen

Default state of status.conf:

<Location /server-status>
SetHandler server-status
Order deny,allow
Deny from all
Allow from 127.0.0.1 ::1
#Allow from
192.0.2.0/24
</Location>
Local attacker

Hi, @ircmaxell!

"... this new menu item was named "Admin". Curious, I clicked the link, figuring I'd be immediately denied access. What happened next surprised me. Not only was I not denied access, but I was granted full access to everything. I had the developer console to see what people were doing. I had a database query interface where I could directly query any database that I wanted. I had admin access to chat"
Trust model seems to be overlooked...

"Home, sweet home"
Local attacker

It’s not just about auth bypass!

- PHPSESSID is generated based on remote IP address
  \( \text{hash( client IP . timestamp . microseconds1 . php\_combined\_lcg() )} \)

- Flood detection

- Brute force / lockouts

- Any other security measure based on IP address
<table>
<thead>
<tr>
<th>K</th>
<th>87</th>
<th>9</th>
<th>0</th>
<th>0.3</th>
<th>0.01</th>
<th>365.03</th>
<th>176</th>
<th>1</th>
<th>check.torproject.org</th>
<th>GET /?TorButton=true HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>73</td>
<td>12</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>351.09</td>
<td>93</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>1.14</td>
<td>1</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>350.05</td>
<td>89</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>_</td>
<td>1.16</td>
<td>0</td>
<td>2</td>
<td>0.0</td>
<td>0.02</td>
<td>369.44</td>
<td>77</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>69</td>
<td>14</td>
<td>0</td>
<td>1.1</td>
<td>0.01</td>
<td>364.62</td>
<td>77</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /favicon.ico HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>1.10</td>
<td>2</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>376.06</td>
<td>171</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>78</td>
<td>11</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>350.54</td>
<td>171</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>77</td>
<td>12</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>369.29</td>
<td>109</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>1.15</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.18</td>
<td>355.29</td>
<td>185</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>79</td>
<td>11</td>
<td>0</td>
<td>12.4</td>
<td>0.01</td>
<td>343.88</td>
<td>185</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /torcheck/img/tor-not.png HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>70</td>
<td>14</td>
<td>0</td>
<td>0.1</td>
<td>0.00</td>
<td>356.42</td>
<td>176</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /RecommendedTBBVersions HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>89</td>
<td>8</td>
<td>0</td>
<td>0.3</td>
<td>0.01</td>
<td>358.68</td>
<td>112</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>74</td>
<td>12</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>345.91</td>
<td>91</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>79</td>
<td>11</td>
<td>0</td>
<td>0.3</td>
<td>0.00</td>
<td>345.01</td>
<td>209</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>1.16</td>
<td>0</td>
<td>0</td>
<td>20.9</td>
<td>0.02</td>
<td>377.14</td>
<td>127</td>
<td>0</td>
<td>sergii.torproject.org</td>
<td>GET /TRUST_ME_I_M_LOCALHOST HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>99</td>
<td>5</td>
<td>0</td>
<td>0.16</td>
<td>0.16</td>
<td>354.02</td>
<td>80</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /RecommendedTBBVersions HTTP/1.1</td>
</tr>
<tr>
<td>K</td>
<td>96</td>
<td>5</td>
<td>0</td>
<td>0.3</td>
<td>0.06</td>
<td>359.59</td>
<td>37</td>
<td>1</td>
<td>check.torproject.org</td>
<td>GET /?TorButton=true HTTP/1.1</td>
</tr>
</tbody>
</table>