WikiLeaks - Vault 8

wikileaks.org/vault8/

Key fingerprint **9EF0 C41A FBA5 64AA 650A 0259 9C6D CD17 283E 454C**

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQQBBGBjDtIBH6DJa80zDBgR+VqlYGaXu5bEJg9HEgAtJeCLuThdhXfl5Zs32RyB
I1QjIlttvngepHQozmglBDmi2FZ4S+wWhZv10bZCoyXPIPwwq6TylwPv8+buxuff
B6tYil3VAB9XKGPyPjKrlXn1fz76VMpuTOs7OGYR8xDidw9EHfBvmb+sQyrU1FOW
aPHxba5lK6hAo/KYFpTnimsmsz0Cvo1sZAV/EFIkfagiGTL2J/NhINfGPScpj8LB
bYelVN/NU4c6Ws1ivWbfcGvqU4lymoJgJo/l9HiV6X2bdVyuB24O3xeyhTnD7laf
epykwxODVfAt4qLC3J478MSSmTXS8zMumaQMNR1tUUYtHCJC0xAKbsFukzbfoRDv
m2zFCCVxeYHvByxstuzg0SurlPyuiFiy2cENek5+W8Sjt95nEiQ4suBldswpz1Kv
n71t7vd7zst49xxExB+tD+vmY7GXIds43Rb05dqksQuo2yCeuCbY5RBiMHX3d4nU
041jHBsv5wY24j0N6bpAsm/s0T0Mt7IO6UaN33I712oPlclTweYTAesW3jDpeQ7A
ioi0CMjWZnRpUxorcFmzL/Cc/fPqgAtnAL5GIUuEOqUf8AlKmzsKcnKZ7L2d8mxG
QqN16nlAiUuUpchQNMr+tAa1L5S1uK/fu6thVlSSk7KMQyJfVpwLy6068a1WmNj4
yxo9HaSeQNXh3cui+61qb9wlrkwlaiouw9+bpCmR0V8+XpWma/D/TEz9tg5vkfNo
eG4t+FUQ7QgrrvIkDNFcRyTUO9cJHB+kcp2NgCcpCwan3wnuzKka9AWFAitpoAwx
L6BX0L8kg/LzRPhkQnMOrj/tuu9hZrui4woqURhWLiYi2aZe7WCkuoqR/qMGP6qP
EQRcvndTWkQo6K9BdCH4ZjRqcGbY1wFt/qgAxhi+uSo2IWiM1fRI4eRCGifpBtYK
Dw44W9uPAu4cgVnAUzESEeW0bft5XXxAqpvyMBIdv3YqfVfOElZdKbteEu4YuOao
FLpbk4ajCxO4Fzc9AugJ8iQOAoaekJWA7TjWJ6CbJe8w3thpznP0w6jNG8ZleZ6a
jHckyGlx5wzQTRLVT5+wK6edFlxKmSd93jkLWWCbrc0Dsa39OkSTDmZPoZgKGRhp
Yc0C4jePYreTGI6p7/H3AFv84o0fjHt5fn4GpT1Xgfg+1X/wmIv7iNQtljCjAqhD
6XN+QiOAYAloAym8lOm9zOoCDv1TSDpmeyeP0rNV95OozsmFAUaKSUcUFBUfq9FL
uyr+rJZQw2DPfq2wE75PtOyJiZH7zljCh12fp5yrNx6L7HSqwwuG7vGO4f0ltYOZ
dPKzaEhCOO7o108RexdNABEBAAG0Rldpa2lMZWFrcyBFZGl0b3JpYWwgT2ZmaWNl
IEhpZ2ggU2VjdXJpdHkgQ29tbXVuaWNhdGlvbiBLZXkgKDIwMjEtMjAyNCmJBDEE
EwEKACcFAmBjDtICGwMFCQWjmoAFCwkIBwMFFQoJCAsFFgIDAQACHgECF4AACgkQ
nG3NFyg+RUzRbh+eMSKgMYOdoz70u4RKTvev4KyqCAlwji+1RomnW7qsAK+l1s6b
ugOhOs8zYv2ZSy6lv5JgWITRZogvB69JP94+Juphol6LIImC9X3P/bcBLw7VCdNA
mP0XQ4OlleLZWXUEW9EqR4QyM0RkPMoxXObfRgtGHKIkjZYXyGhUOd7MxRM8DBzN
yieFf3CjZNADQnNBk/ZWRdJrpq8J1W0dNKI7IUW2yCyfdgnPAkX/lyIqw4ht5UxF
VGrva3PoepPir0TeKP3M0BMxpsxYSVOdwcsnkMzMlQ7TOJlsEdtKQwxjV6a1vH+t
k4TpR4aG8fS7ZtGzxcxPylhndiiRVwdYitr5nKeBP69aWH9uLcpIzplXm4DcusUc
Bo8KHz+qlIjs03k8hRfqYhUGB96nK6TJ0xS7tN83WUFQXk29fWkXjQSp1Z5dNCcT
sWQBTxWxwYyEI8iGErH2xnok3HTyMItdCGEVBBhGOs1uCHX3W3yW2CooWLC/8Pia
qgss3V7m4SHSfl4pDeZJcAPiH3Fm00wlGUslVSziatXW3499f2QdSyNDw6Qc+chK
hUFflmAaavtpTqXPk+Lzvtw5SSW+iRGmEQICKzD2chpy05mW5v6QUy+G29nchGDD
rrfpId2Gy1VoyBx8FAto4+6BOWVijrOj9Boz7098huotDQgNoEnidvVdsqP+P1RR
QJekr97idAV28i7iEOLd99d6qI5xRqc3/QsV+y2ZnnyKB10uQNVPLgUkQljqN0wP
XmdVer+0X+aeTHUd1d64fcc6M0cpYefNNRCsTsgbnWD+x0rjS9RMo+Uosy41+IxJ
6qIBhNrMK6fEmQoZG3qTRPYYrDoaJdDJERN2E5yLxP2SPI0rWNjMSoPEA/gk5L91
m6bToM/0VkEJNJkpxU5fq5834s3PleW39ZdpI0HpBDGeEypo/t9oGDY3Pd7JrMOF
zOTohxTyu4w2Ql7jgs+7KbO9PH0Fx5dTDmDq66jKIkkC7DI0QtMQclnmWWtn14BS
KTSZoZekWESVYhORwmPEf32EPiC9t8zDRglXzPGmJAPISSQz+Cc9o1ipoSIkoCCh
2MWoSbn3KFA53vgsYd0vS/+Nw5aUksSleorFns2yFgp/w5Ygv0D007k6u3DqyRLB
W5y6tJLvbC1ME7jCBoLW6nFEVxgDo727pqOpMVjGGx5zcEokPIRDMkW/lXjw+fTy
c6misESDCAWbgzniG/iyt77Kz711unpOhw5aemI9LpOq17AiIbjzSZYt6b1Aq7Wr
aB+C1yws2ivIl9ZYK911A1m69yuUg0DPK+uyL7Z86XC7hI8B0IY1MM/MbmFiDo6H
dkfwUckE74sxxeJrFZKkBbkEAQRgYw7SAR+gvktRnaUrj/84Pu0oYVe49nPEcy/7
5Fs6LvAwAj+JcAQPW3uy7D7fuGFEQguasfRrhWY5R87+g5ria6qQT2/Sf19Tpngs
d0Dd9DJ1MMTaA1pc5F7PQgoOVKo68fDXfjr76n1NchfCzQbozS1HoM8ys3WnKAw+
Neae9oymp2t9FB3B+To4nsvsOM9KM06ZfBILO9NtzbWhzaAyWwSrMOFFJfpyxZAQ
8VbucNDHkPJjhxuafreC9q2f316RlwdS+XjDggRY6xD77fHtzYea04UWuZidc5zL

```
VpsuZR1nObXOgE+4s8LU5p6fo7jL0CRxvfFnDhSQg2Z617flsdjYAJ2JR4apg3Es
G46xWl8xf7t227/0nXaCIMJI7g09FeOOsfCmBaf/ebfiXXnQbK2zCbbDYXbrYgw6
ESkSTt940lHtynnVmQBvZqSXY93MeKjSaQk1VKyobngqaDAIIzHxNCR941McGD7F
qHHM2YMTgi6XXaDThNC6u5msI1l/24PPvrxkJxjPSGsNlCbXL2wqaDgrP6LvCP9O
uooR9dVRxaZXcKQjeVGxrcRtoTSSyZimfjEercwi9RKHt42O5akPsXaOzeVjmvD9
EB5jrKBe/aAOHgHJEIgJhUNARJ9+dXm7GofpvtN/5RE6qlx11QGvoENHIgawGjGX
Jy5oyRBS+e+KHcgVqbmV9bvIXdwiC4BDGxkXtjc75hTaGhnDpu69+Cq016cfsh+0
XaRnHRdh0SZfcYdEqqjn9CTILfNuiEpZm6hYOlrfgYQe1I13rgrnSV+EfVCOLF4L
P9ejcf3eCvNhIhEjsBNEUDOFAA6J5+YqZvFYtjk3efpM2jCg6XTLZWaI8kCuADMu
yrQxGrM8yIGvBndrlmmljUqlc8/Nq9rcLVFDsVqb9wOZjrCIJ7GEUD6bRuolmRPE
SLrpP5mDS+wetdhLn5ME1e9JeVkiSVSFIGsumZTNUaT0a90L4yNj5gBE40dvFplW
7TLeNE/ewDQk5LiIrfWuTUn3CqpjIOXxsZFLjieNgofX1nSeLjy3tnJwuTYQlVJO
3CbqH1k6cOIvE9XShnnuxmiSoav4uZIXnLZFQRT9v8UPIuedp7TO8Vjl0xRTajCL
PdTk21e7fYriax62IssYcsbbo5G5auEdPO04H/+v/hxmRsGIr3XYvSi4ZWXKASxy
a/jHFu9zEqmy0EBzFzpmSx+FrzpMKPkoU7RbxzMgZwIYEBk66Hh6gxllL0JmWjV0
iqmJMtOERE4NgYgumQT3dTxKuFtywmFxBTe80BhGlfUbjBtiSrULq59np4ztwlRT
wDEAVDoZbN57aEXhQ8jjF2RlHtqGXhFMrg9fALHaRQARAQABiQQZBBgBCgAPBQJg
Yw7SAhsMBQkFo5qAAAoJEJxtzRcoPkVMdigfoK4oBYoxVoWUBCUekCg/alVGyEHa
ekvFmd3LYSKX/WklAY7cAgL/1UlLIFXbq9jpGXJUmLZBkzXkOylF9FIXNNTFAmBM
3TRjfPv91D8EhrHJW0SlECN+riBLtfIQV9Y1BUlQthxFPtB1G1fGrv4XR9Y4TsRj
VSo78cNMQY6/89Kc00ip7tdLeFUHtKcJs+5EfDQgagf8pSfF/TWnYZOMN2mAPRRf
fh3SkFXeuM7PU/X0B6FJNXefGJbmfJBOXFbaSRnkacTOE9caftRKN1LHBAr8/RPk
pc9p6y9RBc/+6rLuLRZpn2W3m3kwzb4scDtHHFXXQBNC1ytrqdwxU7kcaJEPOFfC
XIdKfXw9AQll620qPFmVIPH5qfoZzjk4iTH06Yiq7PI4OgDis6bZKHKyyzFisOkh
DXiTuuDnzgcu0U4gzL+bkxJ2QRdiyZdKJJMswbm5JDpX6PLsrzPmN314lKIHQx3t
NNXkbfHL/PxuoUtWLKg7/I3PNnOgNnDqCgqpHJuhU1AZeIkvewHsYu+urT67tnpJ
AK1Z4CgRxpgbYA4YEV1rWVAPHX1u1okcg85rc5FHK8zh46zQY1wzUTWubAcxqp9K
1IqjXDDkMgIX2Z2fOA1plJSwugUCbFjn4sbT0t0YuiEFMPMB42ZCjcCyA1yysfAd
DYAmSer1bq47tyTFQwP+2ZnvW/9p3yJ4oYWzwMzadR3T0K4sgXRC2Us9nPL9k2K5
TRwZ07wE2CyMpUv+hZ4ja13A/1ynJZDZGKys+pmBNrO6abxTGohM8LIWjS+YBPIq
trxh8jxzgLazKvMGmaA6KaOGwS8vhfPfxZsu2TJaRPrZMa/HpZ2aEHwxXRy4nm9G
Kx1eFNJO6Ues5T7KlRtl8gflI5wZCCD/4T5rto3SfG0s0jr3iAVb3NCn9Q73kiph
PSwHuRxcm+hWNszjJg3/W+Fr8fdXAh5i0JzMNscuFAQNHgfhLigenq+BpCnZzXya
01kqX24AdoSIbH++vvgE0Bjj6mzuRrH5VJ1Qg9nQ+yMjBWZADljtp3CARUbNkiIg
tUJ8IJHCGVwXZBqY4qeJc3h/RiwWM2UIFfBZ+E06QPznmVLSkwvvop3zkr4eYNez
cIKUju8vRdW6sxaaxC/GECDlP0Wo6lH0uChpE3NJ1daoXIeymajmYxNt+drz7+pd
jMqjDtNA2rgUrjptUgJK8ZLdOQ4WCrPY5pP9ZXAO7+mK7S3u9CTywSJmQpypd8hv
8Bu8jKZdoxOJXxj8CphK951eNOLYxTOxBUNB8J2lgKbmLIyPvBvbS1l1lCM5oHlw
WXGlp70pspj3kaX4mOiFaWMKHhOLb+er8yh8jspM184=
=5a6T
-----END PGP PUBLIC KEY BLOCK-----
```

Tor

Tor is an encrypted anonymising network that makes it harder to intercept internet communications, or see where communications are coming from or going to.

In order to use the WikiLeaks public submission system as detailed above you can download the Tor Browser Bundle, which is a Firefox-like browser available for Windows, Mac OS X and GNU/Linux and pre-configured to connect using the anonymising system Tor.

Tails

If you are at high risk and you have the capacity to do so, you can also access the submission system through a secure operating system called Tails. Tails is an operating system launched from a USB stick or a DVD that aim to leaves no traces when the computer is shut down after use and automatically routes your internet traffic through Tor. Tails will require you to have either a USB stick or a DVD at least 4GB big and a laptop or desktop computer.

Tips

Our submission system works hard to preserve your anonymity, but we recommend you also take some of your own precautions. Please review these basic guidelines.

1. Contact us if you have specific problems

If you have a very large submission, or a submission with a complex format, or are a high-risk source, please contact us. In our experience it is always possible to find a custom solution for even the most seemingly difficult situations.

2. What computer to use

If the computer you are uploading from could subsequently be audited in an investigation, consider using a computer that is not easily tied to you. Technical users can also use Tails to help ensure you do not leave any records of your submission on the computer.

3. Do not talk about your submission to others

If you have any issues talk to WikiLeaks. We are the global experts in source protection – it is a complex field. Even those who mean well often do not have the experience or expertise to advise properly. This includes other media organisations.

How to contact WikiLeaks? What is Tor? Tips for Sources After Submitting

After

1. Do not talk about your submission to others

If you have any issues talk to WikiLeaks. We are the global experts in source protection – it is a complex field. Even those who mean well often do not have the experience or expertise to advise properly. This includes other media organisations.

2. Act normal

If you are a high-risk source, avoid saying anything or doing anything after submitting which might promote suspicion. In particular, you should try to stick to your normal routine and behaviour.

3. Remove traces of your submission

If you are a high-risk source and the computer you prepared your submission on, or uploaded it from, could subsequently be audited in an investigation, we recommend that you format and dispose of the computer hard drive and any other storage media you used.

In particular, hard drives retain data after formatting which may be visible to a digital forensics team and flash media (USB sticks, memory cards and SSD drives) retain data even after a secure erasure. If you used flash media to store sensitive data, it is important to destroy the media.

If you do this and are a high-risk source you should make sure there are no traces of the clean-up, since such traces themselves may draw suspicion.

4. If you face legal action

If a legal action is brought against you as a result of your submission, there are organisations that may help you. The Courage Foundation is an international organisation dedicated to the protection of journalistic sources. You can find more details at https://www.couragefound.org.

Submit documents to WikiLeaks

WikiLeaks publishes documents of political or historical importance that are censored or otherwise suppressed. We specialise in strategic global publishing and large archives.

The following is the address of our secure site where you can anonymously upload your documents to WikiLeaks editors. You can only access this submissions system through Tor. (See our Tor tab for more information.) We also advise you to read our tips for sources before submitting.

http://ibfckmpsmylhbfovflajicjgldsqpc75k5w454irzwlh7qifgglncbad.onion

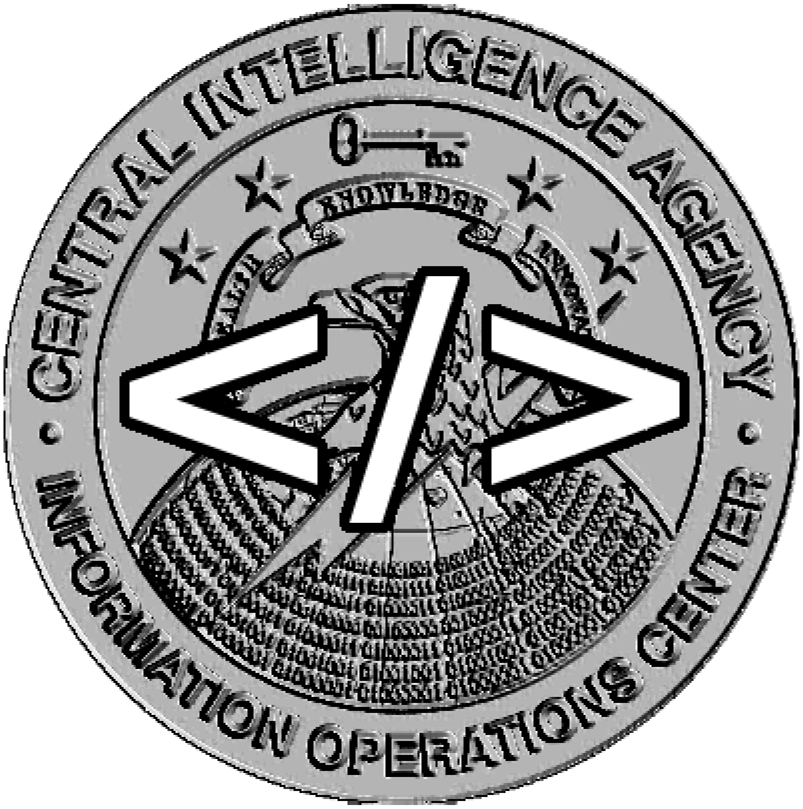
If you cannot use Tor, or your submission is very large, or you have specific requirements, WikiLeaks provides several alternative methods. Contact us to discuss how to proceed.

Vault 8

Source code and analysis for CIA software projects including those described in the Vault7 series.

This publication will enable investigative journalists, forensic experts and the general public to better identify and understand covert CIA infrastructure components.

Source code published in this series contains software designed to run on servers controlled by the CIA. Like WikiLeaks' earlier Vault7 series, the material published by WikiLeaks does **not** contain 0-days or similar security vulnerabilities which could be repurposed by others.



Releases
Documents

All Releases

Hive - 9 November, 2017

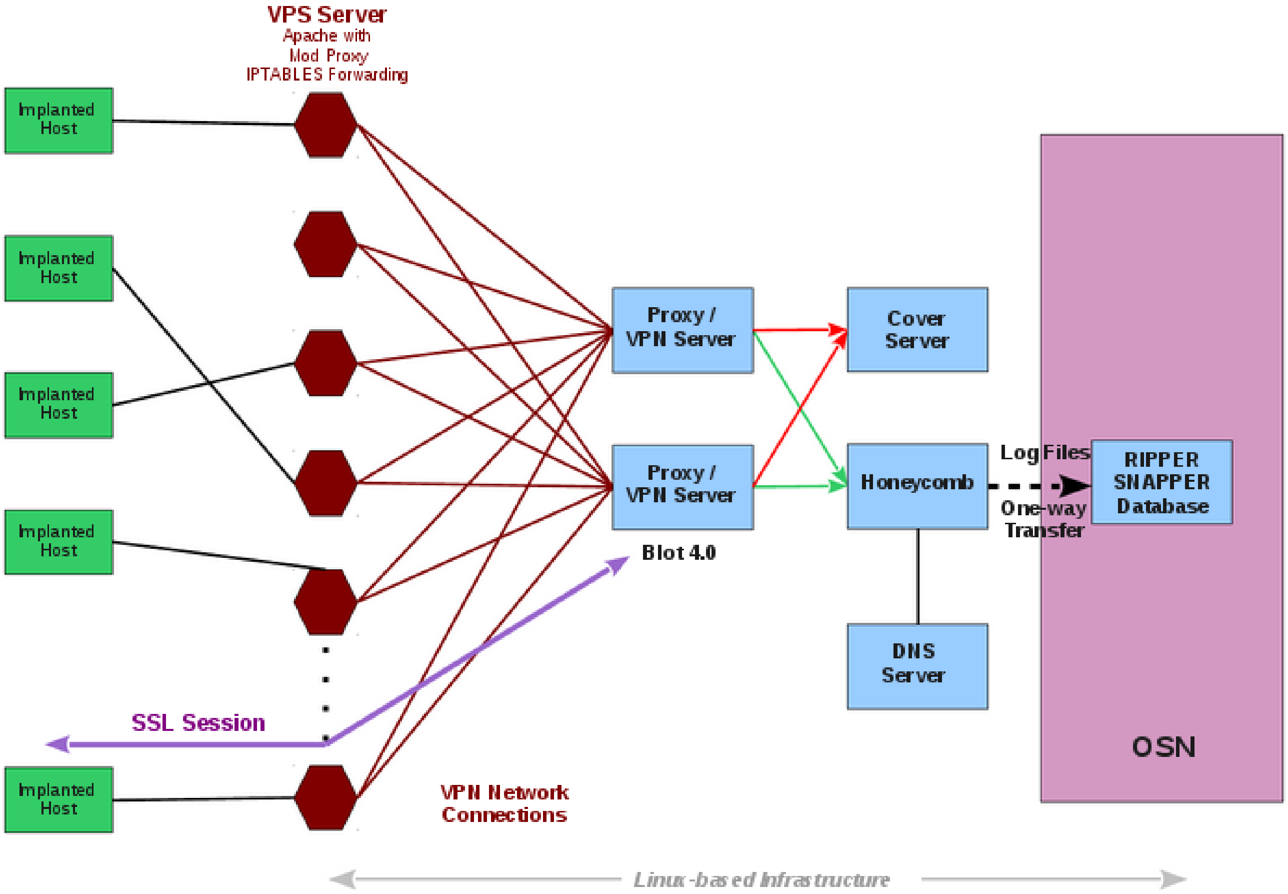
Hive

9 November, 2017

Today, 9 November 2017, WikiLeaks publishes the source code and development logs to *Hive*, a major component of the CIA infrastructure to control its malware.

Hive solves a critical problem for the malware operators at the CIA. Even the most sophisticated malware implant on a target computer is useless if there is no way for it to communicate with its operators in a secure manner that does not draw attention. Using *Hive* even if an implant is discovered on a target computer, attributing it to the CIA is difficult by just looking at the communication of the malware with other servers on the internet. *Hive* provides a covert communications platform for a whole range of CIA malware to send exfiltrated information to CIA servers and to receive new instructions from operators at the CIA.

Hive can serve multiple operations using multiple implants on target computers. Each operation anonymously registers at least one cover domain (e.g. "perfectly-boring-looking-domain.com") for its own use. The server running the domain website is rented from commercial hosting providers as a VPS (virtual private server) and its software is customized according to CIA specifications. These servers are the public-facing side of the CIA back-end infrastructure and act as a relay for HTTP(S) traffic over a VPN connection to a "hidden" CIA server called 'Blot'.



The cover domain delivers 'innocent' content if somebody browses it by chance. A visitor will not suspect that it is anything else but a normal website. The only peculiarity is not visible to non-technical users - a HTTPS server option that is not widely used: *Optional Client Authentication*. But *Hive* uses the uncommon *Optional Client Authentication* so that the user browsing the website is not required to authenticate - it is optional. But implants talking to *Hive* do authenticate themselves and can therefore be detected by the *Blot* server. Traffic from implants is sent to an implant operator management gateway called *Honeycomb* (see graphic above) while all other traffic go to a cover server that delivers the insuspicious content for all other users.

Digital certificates for the authentication of implants are generated by the CIA impersonating existing entities. The three examples included in the source code build a fake certificate for the anti-virus company Kaspersky Laboratory, Moscow pretending to be signed by Thawte Premium Server CA, Cape Town. In this way, if the target organization looks at the network traffic coming out of its network, it is likely to misattribute the CIA exfiltration of data to uninvolved entities whose identities have been impersonated.

The documentation for *Hive* is available from the WikiLeaks Vault7 series.