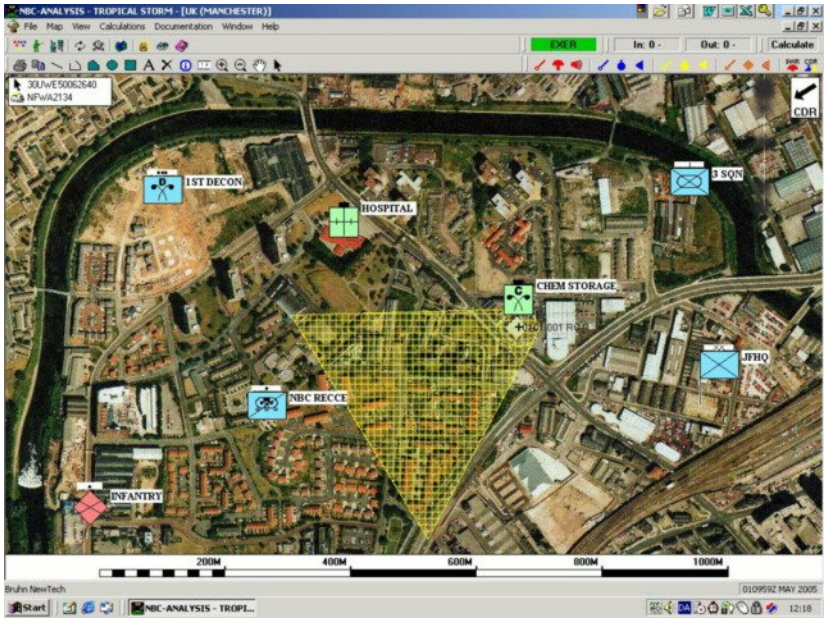
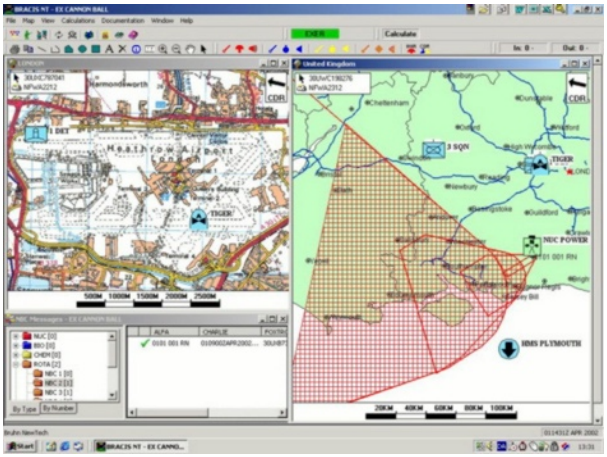
opWinterIsComing
from : SOBH Cyber Jihad
to : DOE

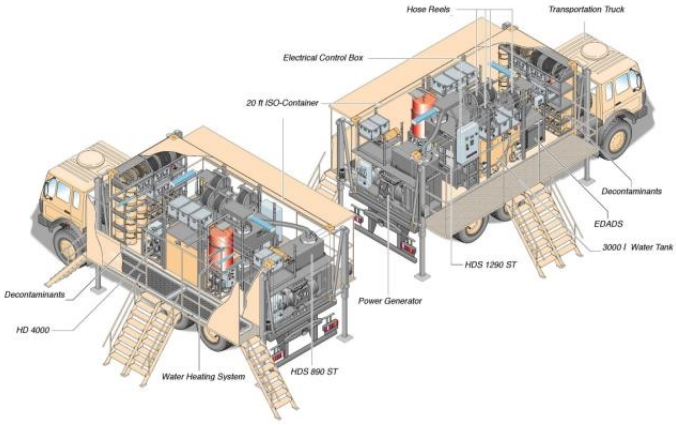
we tried to understand under what circumstances you would be vulnerable to a total Energy chaos as a nation of voters and fat defense contractors [1]. cool experiences been these past months .

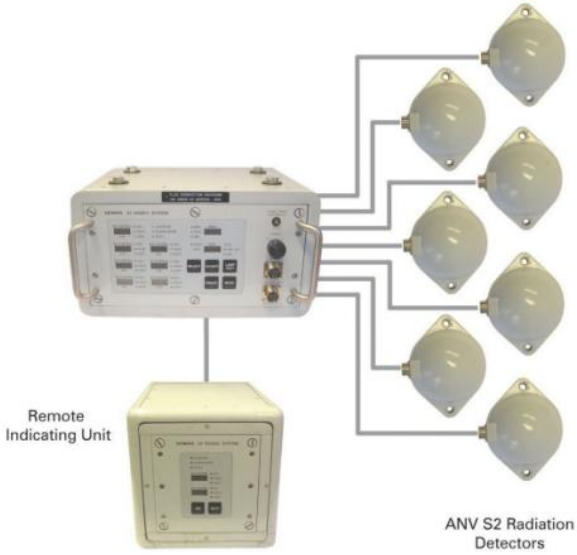
we are not [2] going to have a massive dump here since the essence of the op was getting the sensitive target docs to the right hands . our target was mainly U.S Department of Energy (DOE) and several national labs that help this organization works .

even for us and our brothers this data is mostly valuable when kept secret but if the US officials introduce retard questions to our op in their statements we would happily publish a bunch of dox here and there for lulz and lessons .


NBC-ANALYSIS - TROPICAL STORM - [UK (MANCHESTER)]
1ST DECON
HOSPITAL
3 SQN
CHEM STORAGE
JFHQ
NBC RECCE
INFANTRY
CDR
200M
400M
600M
800M
1000M




Hose Reels
Transportation Truck
Electrical Control Box
20 ft ISO-Container
Decontaminants
EDADS
3000 l Water Tank
HDS 1290 ST
Power Generator
Decontaminants
HD 4000
Water Heating System
HDS 890 ST


Remote
Indicating Unit
ANV S2 Radiation
Detectors

Compromised targets :

Analyzed ASNs :
46846,32982,291,36473,68,377,10702,1226,292,3428,36029,683,
26910

Pwned Emails to hop in :
archlt@lanl.gov
jghelle@sandia.gov
helena.tirone@srs.gov
amfmenergy@aol.com :D
jeff.davis@hq.doe.gov
thornwiii@y12.doe.gov
cheryl.thompson@hq.doe.gov
scott.clemons@nnsa.doe.gov
pamela.garrett@em.doe.gov
ammy.james@spr.doe.gov
ammy.james@spr.doe.gov
jw.peterson@inl.gov
amy@cic-mail.lanl.gov
arvel.callwood@spr.doe.gov
jennifer.osullivan@inl.gov
ann.legum@hq.doe.gov
karin.king@oak.doe.gov
steve.eckstrand@science.doe.gov
berryla@ornl.gov
kylematthewmack@gmail.com

najmolame@y12.doe.gov
jbeyers@pantex.com
hgarriso@pantex.com
andrea.mcnemar@netl.doe.gov
jameseb@fnal.gov
mauche@cygnus.llnl.gov
eva.auman@hq.doe.gov
klingeal@nv.doe.gov
klingeal@nv.doe.gov
kathleen.binder@hq.doe.gov
troy.saffle@deq.idaho.gov
jelee@water.ca.gov
jslee@energy.state.ca.us
amalia.manzo@yahoo.com
tara.fuller@hq.doe.gov
angela.lanauze@netl.doe.gov
jessica.sosenko@netl.doe.gov
kimberly.yavorsky@netl.doe.gov
amy.joslin@srs.gov
baindt@ornl.gov
susannah.burrows@pnnl.gov
elaine.king@pnnl.gov
mary.beckman@pnnl.gov
james.riley@nnsa.doe.gov
ralph.tennant@nnsa.doe.gov
jbailey@lanl.gov

Pwned Servers for Pivoting evil traffic to resources , Thank you for "Remotes" :)

remote.pnnl.gov [java 0day + Outdated Cisco VPN]
ydesktop-rsa.vdi.doe.gov [Citrix 0day]
http://workplace.science.doe.gov/CitrixLogonPoint/External/ [Citrix 0day]
webmail.eia.gov/owa [Outlook Exploit bypassing Token]
portal.pnl.gov/+CSCOE+/logon.html [Outdated Cisco SSL VPN]
drupal.llnl.gov [Drupal 0day + watering holes go here]

the following assets called for extra work and Prayers :) its never easy to mess with HSM-protected Auth but we did it .do you remember the Commodohacker? :>

cryptocard-green.lanl.gov
https://mail.sandia.gov/CookieAuth.dll
https://weblogin.lanl.gov/?referer=https://auth1.lanl.gov/

but lets get real . the coolest one was DOE email servers being hosted by google using Google Mail Enterprise . we hit Israeli FM accounts using our 0day on Google mail a while back .

cryptome.org/2015/04/sobh/sobh-attacks-israel.htm
cryptome.org/2015/04/sobh-iaea/sobh-iaea.htm

now Check this shit out :D

gmail.inl.gov
gmail.doe.gov

btw , not only the bug still exist , the stupid Israelis are still using infected assets even after their shit went online .[2]

full list of IPs we scanned or examined for entry during the op (almost 3 months):

65.199.24.0-65.199.24.255
192.101.108.0-192.101.109.255
23.34.58.0-23.34.59.255
192.208.22.0-192.208.22.255
134.186.0.0-134.186.255.255
204.134.133.0-204.134.133.255
192.65.95.0-192.65.95.255
192.5.86.0-192.5.86.255
141.221.0.0-141.221.255.255
23.3.136.0-23.3.136.255
23.15.0.0-23.15.0.255
192.69.190.0-192.69.190.255
134.20.0.0-134.20.255.255
192.208.27.0-192.208.27.255
198.124.0.0-198.127.255.255
12.192.16.0-12.192.16.255

141.221.68.0-141.221.68.15
192.5.99.0-192.5.99.255
146.139.0.0-146.139.255.255
192.5.200.0-192.5.200.255
204.121.3.0-204.121.3.255
198.105.241.0-198.105.241.255
159.145.0.0-159.145.255.255
132.175.0.0-132.175.255.255
192.12.95.0-192.12.95.255
205.254.135.0-205.254.135.255
192.83.111.0-192.83.111.255
192.206.135.0-192.206.135.255
199.201.153.0-199.201.153.255
162.249.104.0-162.249.111.255
164.54.0.0-164.54.255.255
198.51.238.0-198.51.238.255
198.102.151.0-198.102.151.255
146.138.0.0-146.138.255.255
198.207.238.0-198.207.238.255
199.167.78.0-199.167.79.255
192.5.84.0-192.5.84.255
192.26.8.0-192.26.8.255
130.202.0.0-130.202.255.255
156.41.0.0-156.41.255.255
132.175.188.0-132.175.188.255
192.208.20.0-192.208.21.255
205.254.159.0-205.254.159.255
146.137.81.0-146.137.81.255

12.172.44.0-12.172.44.255
146.137.252.0-146.137.255.255
12.192.17.0-12.192.17.255
153.48.0.0-153.48.255.255
192.94.168.0-192.94.168.255
159.64.0.0-159.64.255.255
192.208.26.0-192.208.27.255
198.179.181.0-198.179.181.255
199.167.76.0-199.167.76.255
205.254.128.0-205.254.159.255
192.12.184.0-192.12.184.255
198.105.240.0-198.105.255.255
162.220.4.0-162.220.7.255
206.197.198.0-206.197.198.255
198.207.239.0-198.207.239.255
64.18.4.0-64.18.4.255
151.143.0.0-151.143.255.255
198.105.240.0-198.105.240.255
23.14.88.0-23.14.89.255
192.101.105.0-192.101.105.255
198.147.246.0-198.147.246.255
139.121.0.0-139.121.255.255
67.156.0.0-67.157.255.255
141.111.0.0-141.111.255.255
192.101.100.0-192.101.103.255
23.211.62.0-23.211.63.255
198.184.177.0-198.184.177.255
192.107.175.0-192.107.175.255

162.2.0.0-162.2.255.255
198.102.154.0-198.102.154.255
160.88.0.0-160.88.255.255
198.102.152.0-198.102.153.255
192.73.213.0-192.73.213.255
198.51.238.0-198.51.239.255
132.172.0.0-132.172.255.255
192.138.169.0-192.138.169.255
204.134.0.0-204.134.255.255
198.105.243.0-198.105.243.255
205.254.128.0-205.254.128.255
146.137.0.0-146.137.255.255
198.133.156.0-198.133.156.255
198.151.8.0-198.151.15.255
204.121.6.0-204.121.6.255
192.5.170.0-192.5.171.255
198.128.2.0-198.128.2.255
198.102.153.0-198.102.153.255
198.207.237.0-198.207.237.255
192.112.183.0-192.112.183.255
198.105.249.0-198.105.249.255
68.64.143.0-68.64.143.255
146.114.0.0-146.114.255.255
74.121.192.0-74.121.199.255
158.96.0.0-158.96.255.255
205.254.146.0-205.254.146.255
141.221.67.0-141.221.67.255
192.5.172.0-192.5.175.255

128.165.0.0-128.165.255.255
130.55.0.0-130.55.255.255
192.74.216.0-192.74.216.255
205.254.131.0-205.254.131.255
192.12.208.0-192.12.208.255
12.177.5.0-12.177.5.255
134.20.2.17-134.20.2.17
74.125.244.0-74.125.247.255
205.167.106.0-205.167.107.255
134.167.0.0-134.167.255.255
205.254.132.0-205.254.132.255
204.154.137.0-204.154.137.255
23.45.66.0-23.45.66.255
198.204.105.0-198.204.105.255
192.35.193.0-192.35.193.255
192.43.188.0-192.43.188.255
204.132.0.0-204.133.255.255
199.167.72.0-199.167.79.255
192.147.242.0-192.147.243.255
204.121.0.0-204.121.255.255
192.48.238.0-192.48.238.255
192.101.104.0-192.101.107.255
192.5.192.0-192.5.199.255
134.187.0.0-134.187.255.255
205.137.80.0-205.137.95.255
134.186.116.0-134.186.116.255
198.128.0.0-198.131.255.255
198.105.242.0-198.105.242.255

134.253.0.0-134.253.255.255
140.221.0.0-140.221.127.255
199.201.154.0-199.201.154.255
192.103.128.0-192.103.128.255
199.201.157.0-199.201.157.255
12.177.6.0-12.177.6.255
128.165.4.0-128.165.4.255
198.102.155.0-198.102.155.255
199.201.155.0-199.201.155.255
134.253.96.0-134.253.96.255
69.174.51.0-69.174.51.255
192.52.70.0-192.52.70.255
192.5.176.0-192.5.191.255
192.160.227.0-192.160.227.255
192.84.216.0-192.84.217.255
205.254.147.0-205.254.147.255
134.253.9.0-134.253.9.255
192.188.23.0-192.188.23.255
192.83.251.0-192.83.251.255
23.34.60.0-23.34.61.255
156.60.0.0-156.60.255.255
130.20.0.0-130.20.255.255
198.105.244.0-198.105.244.255

identities we used throughout the social engineering :

Amalia Mccubbins

Richard Kouzes
Curtis Smith
Debora Lewis
Kelly Welch
Mary Beckman
Douglas Nordwall
Kimberly Dellinger
Cheryl Thompson
Steve Piotrowski
Jennifer Reichert
Ann Legum
Jennifer O'Sullivan
Jianguo Yu
Dan Connelly

Finally we decided to get the counterintelligence team a bit more involved . not a challenge . a real deal . what is it ?

We used a custom tool to manage the attack and exfiltration the data no matter where the code runs , and DOE is exceptionally Java friendly environment , we learned :D

We are releasing our tool for analysis . there are clear indications about the identity of the hacking crew in the binary . it is a simple tool with complicated crypto and totally AV undetectable .

This tool is here , among the data there are tips and bits for the wise who know what kind business they are getting into ;)

We invite the DOE and other agencies and all the readers to take the chance and see if they can defeat our tool and by that , do they go to the next level , which is kinda exotic ? ☺

You must understand the plain crypto elements in the package and try to make things sense and reconstruct the tool , then contact Cryptome with answers . we don’ t care about anonymity and the attribution game . its for children . this is war , yo :)

DOE is pwned without harm , we could vandalize obviously but there was no sense to it . although exfil data is highly technical , we most interested in NNSA data . maybe as we see politic scene , we publish some dox . game changing shit , yo :D

https://filetea.me/t1sS0A1JEBURyWuLGdqJliAKA
or https://dropfile.to/UvP9s

SOBH Cyber Jihad

[1] http://cryptome.org/2013/05/parastoo-13-0513.pdf

[2] https://cryptome.org/2015/09/nnsa-iranian-target.htm

[3] www.youtube.com/watch?v=PTI89Qe4fBU

مَثَلُ ٱلَّذِينَ ٱتَّخَذُوا۟ مِن دُونِ ٱللَّهِ أَوْلِيَآءَ كَمَثَلِ
ٱلْعَنكَبُوتِ ٱتَّخَذَتْ بَيْتًا ۖ وَإِنَّ أَوْهَنَ ٱلْبُيُوتِ لَبَيْتُ
ٱلْعَنكَبُوتِ ۖ لَوْ كَانُوا۟ يَعْلَمُونَ ﴿٤١﴾