From: "Anglin, Matthew" <Matthew.Anglin@QinetiQ-NA.com>
To: "Matt Standart" <matt@hbgary.com>
Cc: <jeremy@hbgary.com>; <Services@hbgary.com>
Sent: Thursday, January 20, 2011 2:22 PM
Attach: 10 18 0 44Foreign Activity.xlsx
Subject: RE: FW: 10.18.0.44IranConnections.xlsx

Matt,
Take a look at the spreadsheet. In your view does this amount of traffic to various IP address resemble malware ? The date is from dec 1 to jan 7th

Did you see any indication of Skype being utilized?

Matthew Anglin
Information Security Principal, Office of the CSO
QinetiQ North America
7918 Jones Branch Drive Suite 350
Mclean, VA 22102
703-752-9569 office, 703-967-2862 cell

From: Matt Standart [mailto:matt@hbgary.com]
Sent: Thursday, January 20, 2011 1:36 PM
To: Anglin, Matthew
Cc: jeremy@hbgary.com; Services@hbgary.com
Subject: Re: FW: 10.18.0.44IranConnections.xlsx

Here is the one item I see on this host right now having successfully scanned it a few moments ago.

A (possible screensaver) file, named Qinetiq.scr is running in memory on this host. The file looks to be affiliated or created using a shareware screensaver utility from www.2flyer.com.

- 2flyer.com is registered to a person named Zhou TianHai. The whois/registration details (or lack thereof) for this site are HIGHLY suspicious. The DNS records point back to Chinese name servers, another indicator of a high risk/suspicious program.
- The file is located in c:\windows\system32.
- The earliest prefetch date I found indicating the file executing is 1/10/11 18:53.
- The security event logs were cleared on 1/10/2011 9:09am. No event logs were entered after that time, indicating the security event auditing may be disabled on this host.

At a first glance of the binary and what it does, there is highly suspicious capability here for a screensaver, including the ability to communicate out using OpenSSL and capture passwords. I recommend the host be sanitized and the user questioned regarding the screensaver file.

You can give me a call if you have any questions.

Thanks,

Matt

On Thu, Jan 20, 2011 at 8:39 AM, Matt Standart <matt@hbgary.com> wrote:
This host was brought to our attention earlier this month. We were able to deploy and initiate a scan but did not get scan results back. The host was deployed to on 1/7 but that was also the last time it checked in. I suspect it may have been taken offline and rebuilt that day, prior to the scan completing.

Matt

On Wed, Jan 19, 2011 at 10:49 PM, Anglin, Matthew <Matthew.Anglin@qinetiq-na.com> wrote:
Matt and Jeremy,
I am not totally sure were Kent is coming from when he said that HBgary couldn't find malware on STAFKEBROWNLT (10.18.0.44).
I am assuming he got that from the draft report that was released last week?
With thousands of connections outbound to the who's who of sanctioned or embargoed nations it seems to me that some sort of malware is present. So just in case that Kent is thinking of another system, would you please check to see what the latest scan results were for that system?

Matthew Anglin
Information Security Principal, Office of the CSO
QinetiQ North America
7918 Jones Branch Drive Suite 350
Mclean, VA 22102
703-752-9569 office, 703-967-2862 cell

From: Fujiwara, Kent
Sent: Wednesday, January 19, 2011 5:10 PM
To: Anglin, Matthew
Subject: FW: 10.18.0.44IranConnections.xlsx

Matthew,

10.18.0.44 initiated all connections to 22 unique Iranian hosts to Port 80 and Port 443
Typical of installed malware.
Apparently HBGary couldn't find anything – **bottom line no data was exchanged.**

10.18.0.44 was making attempts as of yesterday – haven't seen it online since then.
Between 1 DEC 2010 and 7 JAN 2011 10.18.0.44 also connected 4, 279 times to 72 unique hosts on the Secureworks' Blacklist .

HBGary may need to look more closely and failing that we may want to have the system reimaged.

See below:

IRANIAN	SW BLACKLIST
77.67.32.33	69.31.58.128
77.67.32.34	69.31.58.106
77.67.32.45	68.142.123.254
77.67.32.15	66.220.149.18
77.67.32.41	207.46.148.33
77.67.32.14	204.160.119.126
77.67.32.42	204.2.216.18
77.67.32.39	69.63.189.34
77.67.32.31	69.31.58.171
77.67.32.12	69.31.58.176
77.67.32.9	66.220.149.32
77.67.32.17	69.63.189.16

77.67.32.40
77.67.32.32
77.67.32.10
77.67.32.36
77.67.32.18
77.67.32.44
77.67.32.35
77.67.32.37
77.67.32.38
83.147.249.252

209.8.118.98
208.89.14.135
66.220.149.11
66.220.153.11
69.63.189.26
67.195.160.76
72.21.214.39
74.125.93.102
69.63.189.31
68.142.122.70
69.63.189.39
69.63.189.11
69.31.58.203
66.220.147.33
66.220.146.32
69.147.125.65
8.26.221.126
66.220.149.25
66.220.147.11
66.220.147.22
138.108.12.10
69.31.58.170
209.8.115.8
69.31.58.195
66.220.146.18
204.0.59.113
66.114.53.49
198.78.200.126
66.220.158.25
24.143.197.50
66.220.153.19
209.8.118.81
74.125.159.132
76.13.6.132
205.234.175.175
66.114.53.42
205.128.64.126
72.21.211.171
69.31.58.26
66.114.53.50
69.31.58.202
66.114.53.43
66.114.53.19
72.21.211.176
69.31.58.161
69.31.58.177
72.21.203.149
72.21.214.128
69.31.58.178
72.21.211.174
96.6.44.11
69.31.58.179
69.63.181.11
66.114.53.17
96.17.161.97
72.14.204.113

72.14.204.102
205.178.145.65
72.14.204.165