
From: "Ted Vera" <ted@hbgary.com>
To: <mark@hbgary.com>; "Barr Aaron" <aaron@hbgary.com>
Sent: Thursday, January 20, 2011 2:04 PM
Attach: 20110114-Anonymous.pdf; VE-20101227-Cable.pdf; smime.p7s
Subject: Fwd: Question

---------- Forwarded message ----------
From: S. Alan Carroll <alan@endgames.us>
Date: Thu, Jan 20, 2011 at 12:00 PM
Subject: RE: Question
To: "ted@hbgary.com" <ted@hbgary.com>
Cc: Thomas Zebley <tzebley@iptrust.com>, Kevin Skapinetz <kskap@endgames.us>

Ted,

We have done some preliminary analysis on the Anonymous group (see attached). It is a cursory view of Anonymous and their activities. I have also included a Venezuela report we did concerning the possible US-reachable missile housings from Iran.

Not sure what we will be able to dig up, but I will definitely take a look into possible data collection surrounding your target example. Any other details you might have would help in the lookup routines.

Let me know if any of this information helps or if you have any other questions.

S. Alan Carroll

Engineering Manager

Endgame Systems, Inc.

Office: 404-941-3830

Mobile: 404-409-7403

Begin forwarded message:

From: Ted Vera <ted@hbgary.com>

Date: January 20, 2011 12:37:23 PM EST

To: Thomas Zebley <tzebley@iptrust.com>

Subject: Question

Hi Thomas,

We are doing a talk at an upcoming security expo related to analysis we are conducting on the Anonymous group. I wonder if this group is using any botnets to help attack their targets. Can EndGames search their database for specific targets (like the one below) during an operational window (date/time span) to see if any botnet(s) are participating in attacks? Below is an attack which is currently ongoing. I can also send you previous attacks to see if you have any historical data. If EndGames can provide any relevant data that we can cite in our report we'll give you credit for your contributions.

Operation Payback ITA ---NOW--- #OpVenezuela:http://bit.ly/dI8Oyt | Target: www.presidencia.gob.ve method http |Hive: net.operationfreedom.ru default.| Reason: http://bbc.in/g6ux7z | Sad/Shocking info: http://pastebin.com/LC7aAiYZ | Help with ideas here: http://bit.ly/fpUaCZ

Ted

--
Ted Vera | President | HBGary Federal
Office 916-459-4727x118 | Mobile 719-237-8623
www.hbgaryfederal.com | ted@hbgary.com

--
Ted Vera | President | HBGary Federal
Office 916-459-4727x118 | Mobile 719-237-8623
www.hbgaryfederal.com | ted@hbgary.com

Endgame Systems, Inc.
December 2010

Bolivarian Republic of Venezuela

Development of Nuclear and Military Technology

Scope: UNCLASSIFIED

Bolivarian Republic of Venezuela

Endgame Systems, Inc.

Engineering & Analysis Department

Iranian Presence in Venezuela

Iran is suspected of circumventing UN sanctions by establishing a presence in and alliances with Latin American countries, particularly Venezuela. Reports indicate that Iranian technicians have been in the country since 2006 seeking uranium deposits. Rodolfo Sanz, the Mining Minister of Venezuela, has acknowledged the Iranian presence helping to estimate the amount of uranium reserves[1], while other testimonies have reported that a over 50 Iranian technicians, under Iranian control, have worked with mining and geological organizations such as the Venezuelan Ministry of Basic Industry and Mines and the Venezuelan Institute of Geology and Mines[2]. Without any outside help, Venezuela does not have qualified scientists or sufficient capital to begin a nuclear program.

A great deal of Venezuela's wealth lies in natural gas and petroleum as well as other minerals like iron ore and gold, managed by Venezuela's state-run mining and minerals company Corporación Venezolana de Guayana (CVG). A large portion of mining and exploration occurs on the Guyana Shield along the east coast, while suspected uranium deposits could be in the states of Merida and Trujillo in the west, though there are doubts as to the presence of any significant amounts of uranium anywhere in the country[3].

According to media reports, Iran has made a recent agreement with Venezuela to place medium-range missiles in military bases in Venezuela capable of reaching the United States. These military bases are to be manned by Iranian officers and soldiers of the Iranian Revolutionary Guard (IRGC) in addition to Venezuelan missile officers; the Qods Force (IRGC-QF), an elite force within the IRGC, has long had capabilities worldwide, including in Venezuela[4]. In the event of an "emergency" or for "national needs" Venezuela may use the facilities, per the agreement[5].

Iran's known missile capabilities include regional ballistic missiles able to reach such countries as Israel and those in central Europe. It is also possible Iran is equipped with an intermediate-range ballistic missile (IRBM) that would be able to reach Europe[6]. Iran has recently developed its own version of the Russian S-300 missile, according to state-run news agency IRNA; furthermore, Iran has capabilities for atomic warhead-carrying missiles[7].

After UN sanctions deterred Russia from selling air defense systems to Iran, Russia announced that it had sold at least 100 anti-aerial defense systems (called Igla or *aguya*) with 90 launches to Venezuela, prompting concerns that such arms could fall to other organizations, such as FARC[8]. Russia has also reached an agreement with Venezuela to aid with the building of a nuclear reactor for the latter country's outdated hydroelectric system, according to Venezuelan official announcements[9].

Infected Organizations

A number of state-owned and other prominent organizations showed infection activity during the month of November:

IP	Organization	Location	Infection
150.185.128.152 150.185.129.30 150.185.129.37 150.185.133.41 150.185.160.109 [others]	National Center of Information Technology	Mérida [Others]	Compromised or Hostile Host Traffic Conficker_A/B Conficker_C Mariposa P2P - Limewire
200.1.0.100 [others]	CAF, Corporación Andina de Fomento	Caracas	DShield (Suspicious)
190.170.184.49 190.170.148.5 [others]	Venezuelan Institute of Scientific Investigations	Caracas Los Teques	Conficker A/B Conficker C
200.44.57.49	Central Budget Office	San Joaquín	Conficker C

Vulnerable Assets

Most detected servers in Venezuela IP space were Microsoft-IIS and Apache; thttpd and cisco-IOS also had a significant presence. The largest detected web device was RDP Web, or Remote Desktop Web Portal, which enables users to connect computers using an Internet browser; other prominent web-facing applications and devices included Mikrotik RouterOS, Joomla, and cPanel.

The following table of organizations is not an inclusive list of the data discovered.

IP Address	Organization	Location	Server	App	EGS Vuln.
190.153.24.66 190.153.24.86	Ministry of the Office of the Presidency	Caracas	Apache	Open Webmail Shockwave Login	Yes Yes
190.9.128.98	National Center of Information Technologies	Caracas	Apache	Joomla	Yes
190.202.108.114	Water of Mérida, Governorate of Mérida	Caracas	Apache	Drupal	Yes
190.9.129.225 190.9.129.226	Treasury Bank	Caracas	Apache	Drupal	Yes
200.11.137.34 200.11.137.42	Hugo Chavez's Official Blog	Caracas	Apache	Wordpress	--
200.71.154.229	Official Site of the Bolivarian Army	Caracas	Apache	Joomla Joomla Mitra	Yes Yes
150.188.20.8	Official Site of the Direction General of Military Intelligence (Ministry of Denfense)	Caracas	Apache	Joomla Joomla Mitra	Yes Yes
190.9.130.28	Direction of Communications of the Bolivarian Armed Forces, Operational Strategic Command of the Ministry of Defense	Caracas	Apache	Joomla	Yes
150.187.40.12	FIDETEL, Research and Development Fund of Telecommunications	Caracas	Apache	Joomla Wordpress	Yes --
200.44.119.57 200.90.34.132	Ministry of Defense	Curacao Caracas	Apache	Joomla	Yes
190.202.88.138 190.202.88.139	Ministry of Foreign Affairs	Caracas	Apache NoServerGiven	Joomla	Yes
200.75.143.46	Arturo Michelena International Airport	Valencia	Apache	Wordpress	--
200.44.112.82	Transmissions Network of Venezuela	Machiques	Apache	Joomla	Yes
190.202.89.45	Ministry of	Barcelona	Apache	Joomla	Yes

	Transportation and Communications				
190.9.128.118	Integrated System of Surface Transport	Caracas	Apache	Joomla	Yes
200.44.148.70	Petrochemicals of Venezuela	Caracas	Apache	Joomla	Yes
200.109.249.141 200.44.61.76	SIDOR, Ministry of Basic Industries and Mines	Puerto Ordaz Turmero	Apache NoServerGiven	Joomla	Yes
159.90.10.151 159.90.10.9 159.90.128.15 159.90.13.201 159.90.15.217 159.90.16.205 159.90.170.100 159.90.200.160 159.90.200.177 159.90.200.183 159.90.200.193 159.90.200.229 159.90.200.7 159.90.201.9 159.90.23.15 159.90.250.234 159.90.52.20 159.90.60.218 159.90.61.39 159.90.61.43 159.90.61.44 159.90.80.55 159.90.8.45 159.90.91.11 159.90.91.27 159.90.91.8	University Simón Bolívar	Caracas	Apache	Joomla Mediawiki Roundcube Silverstripe	Yes -- -- Yes

[1] Irán sigue la pista del uranio en América Latina. El País, 2 Dec 2010.
[2] Venezuelan scientists doubt country has uranium. The Miami Herald, 1 Dec 2010.
[3] *Ibid.*
[4] Unclassified Report on Military Power of Iran. Congressionally Directed Action (CDA) – Military Power of Iran. April 2010.
[5] Iran Placng Medium-Range Missiles in Venezuela; Can Reach the U.S. Hudson New York, 8 Dec 2010.
[6] *cf.* 4
[7] *cf.* 5
[8] Rusia vendió a Chávez al menos 100 sistemas antiaéreos muy sofisticados. El País, 9 Dec 2010.
[9] *cf.* 2

Endgame Systems

817 West Peachtree Street

Suite 770

Atlanta, GA 30308

U.S.A.

Produced in the United States of America.

Dec-10