DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION
IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

Welcome! Saturday, 10 Nov 2012

- Web search
- Agency-all Emails
- SID-all Emails
- NSA Rolodex
- SCQAWK: The SID Mailbag
- SIDtoday Blog
- SIDtoday Series
- SIGINT Worldwide VTC

- SIDtoday Article
- Letter to the Editor
- SIGINT-y Social Media

(U) SIGDEV: Is It Time for a 'Target Reboot'?

FROM: (U//FOUO) [redacted]
Transnational & Strategic Partnerships SIGDEV Branch (S2C13)
Run Date: 03/23/2011

(S//REL) Introduction: This is the story of how a "target reboot" (i.e., taking a fresh look at opportunities for collection) by a SIGDEV branch ended up providing the target office with new collection and breathed new life into a stagnant situation.

(TS//SI//REL) A year-end review of our SIGDEV-supported targets in late 2010 showed telltale signs that things were getting stagnant on the Venezuelan Energy target set. Most reporting was coming from warranted collection, and what little was coming from other collectors was pretty sparse. Rather than think my way out of this box, I opted to do a "reboot" of the whole target. Turns out, I couldn't have made a better choice.

> (S//SI//REL) ***Background:*** Venezuela has some of the largest oil and natural gas reserves in the world and consistently ranks among the top ten crude oil producers. Its economy is dominated by the petroleum sector, which accounts for roughly one third of GDP, 80% of exports, and more than half of all government revenues. In the first half of the twentieth century, US oil companies were heavily involved in Venezuela, but in 1973, Venezuela voted to nationalize its oil industry outright, and effective 1 January 1976, Petróleos de Venezuela (PdVSA) took over as the primary oil producer in Venezuela. To understand PdVSA is to understand the economic heart of Venezuela.

(TS//SI//REL) I started out by reviewing the Information Needs (INs) and SURREY requirements to make sure that everything matched and was up to date, and then I met with the target office (TOPI) to re-assure myself that we were both on the same page in regards to our goals.

(S//SI//REL) The TOPI analyst stated that he didn't have time to invest an extensive target development effort, so anything that came to him had to be useable "out of the box." Plainly speaking, he wanted PdVSA information at the highest possible levels of the corporation -- namely, the president and members of the Board of Directors. He wanted as much of it as possible to be in the form of DNI data, to reduce the need to transcribe and piece together conversations.

(TS//SI//REL) I began my "reboot" by visiting the PdVSA website, where I clicked on "Leadership" and wrote down the names of the principals who would become my target list:

(S//SI//REL) Determined to follow the "document as you go" model this time around, I fired up Analyst's Notebook, opened a blank document, and dumped the names into it. Now for some SIGINT! My first stop was PINWALE, where I ran a few queries with mixed results. I had a lot of traffic "cc-ing" most of my target set, but very little info from the actual communicants. I did recover some (actually already known) email addresses, which I entered into Analyst Notebook and bounced against CADENCE and UTT to see if they were tasked. Since my TOPI didn't have time to do development, my plan was to document everything and take it to him like dessert on a tray, and let him choose whatever he wanted.

(TS//SI//REL) One thing that kept popping up in PINWALE was a type of entry which can best be likened to a "SEARCHLIGHT" entry here at NSA. A little pro-forma piece that, upon analysis, showed that it was hitting on the names of the target set as strong selectors. What's more, I discovered that while some of them were "SEARCHLIGHT entries" for the personnel on my set, others showed those same personnel names as the supervisors of other PdVSA employees. "Cool!" I thought, and began entering them into my PdVSA notebook file. A few HUNDRED employees later, I had a pretty substantial document.

(TS//SI//REL) I thought this would be a good place to stop data collection for a while and focus on data analysis.

(TS//SI//REL) Here's a PdVSA "SEARCHLIGHT" entry showing the President of PdVSA, Rafael Ramirez (*pictured meeting with Iranian President Ahmadinejad in 2009*):

Nombre RAMIREZ RAFAEL DARIO
Código Único RAMIREZRGE
Correo PDVSA RAMIREZRGE@PDVSA.COM
Correo Personal RRAMIREZ@MEM.GOV.VE
Conocido Como SIN INFORMACIÓN
Tipo de Empleado EFECTIVO PERMANENTE
Empresa INTEVEP S.A.
Gerencia GCIA.GRAL.REFINACIÑN E INDUSTRIALIZACIÑN
Supervisor RAMIREZ RAFAEL DARIO
Localidad CARACAS
Edificio LA CAMPINA TORRE ESTE
Torre TORRE OESTE
Piso PH
Oficina PH
Tlfno. Interno [redacted]
Tlfno. Interno [redacted]
Teléfono Externo [redacted]
Fax Interno [redacted]

Fax Externo SIN INFORMACIÓN
Busca Persona SIN INFORMACIÓN
Clave Busca Persona SIN INFORMACIÓN
Celular SIN INFORMACIÓN
Tlfno. Habitación SIN INFORMACIÓN
Otro Teléfono SIN INFORMACIÓN

...and here is one showing Ramirez as the supervisor of one of the PdVSA board members, Luis Vierma:

Nombre VIERMA PEREZ LUIS FELIPE
Código Único VIERMAL
Correo PDVSA SIN INFORMACIÓN
Correo Personal SIN INFORMACIÓN
Conocido Como SIN INFORMACIÓN
Tipo de Empleado JUBILADO
Empresa HOLDING PDVSA
Gerencia
Supervisor RAMIREZ RAFAEL DARIO
Localidad CARACAS
Edificio LA CAMPINA TORRE ESTE
Torre TORRE ESTE
Piso PH
Oficina PH
Tlfno. Interno [redacted]
Tlfno. Interno [redacted]
Teléfono Externo [redacted]
Fax Interno [redacted]
Fax Externo [redacted]
Busca Persona SIN INFORMACIÓN
Clave Busca Persona SIN INFORMACIÓN
Celular [redacted]
Tlfno. Habitación [redacted]
Otro Teléfono SIN INFORMACIÓN

(TS//SI//REL) Now, even my old eyes could see that these things were a goldmine of valid selectors, to include work, home, and cell phones, email addresses, LOTS! I had so much data that I was even able to make a chart with which I could "normalize" internal PdVSA numbers so that they could be tasked via OCTAVE. I put all of this together into one spreadsheet, taking only the top personnel, which I knew my TOPI wanted, and presented my TOPI analyst with this package. He was thrilled! That by itself would have been enough to warrant writing this story, but it is what happened next that really made our day.

(TS//SI//REL) As I was analyzing the metadata in PINWALE, I clicked on the "From IP" column and noticed something peculiar -- every single "SEARCHLIGHT entry," over 10,000 of them, came from the same IP!!! I ran several more queries, and every time I came up with the same result. Then, I looked at the "To IP's"... 167.134.x.x, yeah, that's PEQUIVEN (a subsidiary of PdVSA), but wait... 10.x.x.x and 172.18.x.x WTHeck??? Yep, seems I had been looking at internal PdVSA comms all this time!!! I fired off a few emails to F6 here and in Caracas, and they confirmed it!

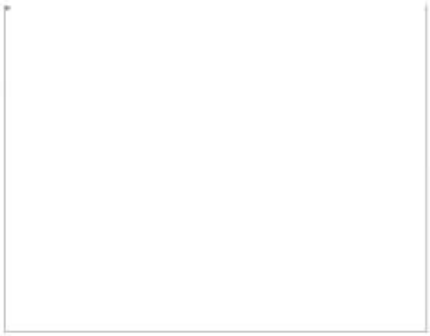
(TS//SI//REL) Since then, I have been coordinating with Caracas, who have been surveying their environment and sticking the results into XKEYSCORE. I have been lucky enough to find several juicy pdf documents in there, one of which has just been made into a report!

SUBJ: Venezuela\Energy: Venezuela State-Owned Oil Company Information Shows a Decrease in Overall Oil Thefts and Losses, January 2011 (S//REL TO USA, FVEY)

(TS//SI//REL) In addition, I have discovered a string that carries user ID's and their passwords, and have recovered over 900 unique user/password combinations which I have forwarded to TAO (Tailored Access Operations -- S32), along with other enabling data and a targeting request to see if we can pwn this network and especially, the boxes of PdVSA's leadership. Wouldn't my TOPI be happy then?

(TS//SI//REL) So, by sheer luck, (and a ton of hard work) I discovered an important new access to an existing target and am working with TAO to leverage a new mission capability.

(U//FOUO) [redacted], S2C13, [redacted]s



(U) Offshore Venezuelan oil rig (Jane's)

Comments/Suggestions about this article?

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."

Information Owner: [redacted], S0121, [redacted], (email)
Page Publisher: [redacted], S0121, [redacted], (email)

Last Modified: 11/10/2012 / Last Reviewed: 11/10/2012

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108