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 Page](#)

(U//FOUO) Interview with a SID "Hacker" -- Part 2: Hacker Culture and Worker Retention

FROM: the SIDtoday Editor

Run Date: 07/13/2012

(U//FOUO) Here's the conclusion of SID*today*'s 2-part interview with [TAO](#)'s ███████ ███████ (pictured). If you missed it, you can find part 1 [here](#).

3. (U) What kind of people gravitate to this kind of work?
(U) Hackers, geeks, nerds! The people in TAO are very interesting. There's an annual event for hackers in Las Vegas called [DEF CON](#), and many of us attend. When there, we feel as though we are among our bretheren! We all have a similar mindset of wanting to tear things apart, to dig in, to see how things work. Here in TAO, the atmosphere is casual. You'll see people in shorts, tee-shirts, flip-flops, black clothes. There is a DEF CON feel to the place.

(U//FOUO) The skills we are after are technical. The people in the ROC have hacker skills, while R&T analysts often have hands-on experience as network administrators

skills, while R&T analysts often have hands-on experience as network administrators. When those former network admins are hired and we put them to work in TAO, there's a mental shift that takes place as they switch from playing defense to offense, but they have the knowledge they need. There are some really great R&T analysts who came here with S2 and SIGDEV backgrounds, but those with network admin experience have the easiest transition.

4. (U) Aren't the skills needed for CNE highly marketable on the "outside"? If so, is it hard for the government to attract and retain those workers?*

(S//SI//REL) There are two sides to it. On the positive side, the job is amazing and awesome! We do things that you can't do anywhere else in the country... at least not legally. We are gainfully employed to hack computers owned by al-Qa'ida! I was even involved in the operation against UBL [Usama bin Laden] -- how many people can say they were involved in something like that? We get great job satisfaction. CNE is enabling kinetic [i.e., bullets, bombs, missiles, etc.] operations against bad people on a regular basis. We also get immediate feedback, which means instant gratification, shared by everyone on the team. Also, the people we work with are good. As I mentioned, we feel as though we are among bretheren. All of these factors make people reluctant to leave TAO.

(U//FOUO) Now on the other hand, there *are* lures to leave. It's not the highest-paying job, especially for developers who can write exploits that are worth a lot of money on the open market. Even locally -- within just the Washington, DC, metro area -- people could probably make more money. Another factor is that the people who are close to active operations -- in R&T and the ROC, for example -- are civilians or military, not contractors. That is because the jobs they do are considered an inherently governmental function, not something that is appropriate for contract work. Many young people have more of a short-term mentality than the older generations, and they don't necessarily want or expect to stay in the same job with the same employer for an extended period of time.

(U) ...Do TAO "hackers" feel uneasy about the fact that they work for the government? Do they feel restricted?

(U//FOUO) I think some people do chafe a bit at government restrictions, but overall I don't think it is a big problem. We train people to make things happen and to not let bureaucracy stand in the way. If necessary, we'll get management involved, and they are very supportive of us. We are a very high-priority mission and management really looks out for us and makes problems go away. They are willing to convey a sense of urgency to all involved that we need to "get it done."

(U) ...Do you have the workers in tee shirts on one side and managers in suits on the other? Is there a big cultural divide?

(U) Actually, I think the managers get absorbed into the "hacker" culture! I remember we had a new manager join us and he wore a suit for a while, but eventually he started dressing more casually like the rest of us.

(U//FOUO) ▮▮▮▮▮▮▮ *(seated) among the "bretheren" at a hackers convention.*

5. (U) You've spoken of some of the best aspects of the job. What are the most

5. (U) You've spoken of some of the best aspects of the job. What are the worst aspects?

(S//SI//REL) One negative would be the long hours that people in TAO need to work, and the times are often inconvenient. For example, ■■■ analysts are often working here at midnight, because we have to work when our targets are active. Also, in CT we are often on call, and might even be called in during holidays. Those are sacrifices you have to be willing to make. Also, ■■■■ Building [which is home to most of the TAO workforce] isn't the best building. The cafeteria is relatively small and not open after-hours, although they did add some vending machines recently with sandwiches and wraps. The parking at ■■■ is somewhat better than the ■■■ however.

6. (U) What has been the most nerve-wracking moment of your career so far? ...the greatest thrill?

(U//FOUO) I'd say they were the same event: the UBL takedown. I was brought in early on, months in advance. I was told, "We think UBL is in this compound -- how can you help?" In the prep stages, one of the NSA primary analysts was flown to Afghanistan and even DIRNSA was involved. During the actual raid [by Navy SEALS], the [TAO] CT employees were all here on chat rooms following the events. When we heard that the helicopter had crashed, that was a "Whao, what just happened??" moment. Were lives lost? Then when we heard "Jackpot!" there was a moment of great jubilation. It was awesome! We were all pleased that we could make a direct contribution to this success -- something we will remember for the rest of our lives.**

7. (U) Is there anything else you think people should know about TAO?

(U//FOUO) I think a lot of people in SID don't fully understand what we can do -- they believe we are focused only on a few particular missions. But that's really not the case. We are the technical experts on CNE [computer-network exploitation], and we can apply those skills to *all* missions -- against *every* target that uses computer networks. So, I hope people will keep in mind that we can support everyone.

(U) Notes:

* (U//FOUO) See a Tapioca Pebble on a related theme: "Best way to retain highly in-demand technical employees?"

** (U//FOUO) Mr ■■■■ related another thrilling event from his career at a SID town hall meeting last year. You can see it in this video, starting at the 29:50 mark.)

Comments/Suggestions about this article?

Information Owner: ███████████████████████████
  Page Publisher: ███████████████████████████
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