(U//FOUO) Dragons, Shrimp, and XKEYSCORE: Tales from the Land of Brothers Grimm

FROM: [redacted]
European Cryptologic Center, SIGDEV (F22)
Run Date: 04/13/2012

(S//REL) The European Cryptologic Center (ECC) sits quietly nestled amongst vineyards and farmlands on

ECC

the outskirts of Darmstadt, Germany. To the passing motorist, the facility looks like many of the other random U.S. government facilities in the area, with one exception. One can almost hear a discernable buzz of activity from the analysts of the ECC executing queries, authoring fingerprints, and consuming metadata garnered from XKEYSCORE (XKS). In the past three months, the ECC has tripled, and even quadrupled in some cases, the number of queries performed, the number of items pushed to PINWALE, and the number of sessions viewed. And these numbers continue to grow.*

(S//REL) What has been the cause of this flurry of success? The ECC points to a recent ***XKS training blitz in support of the Analytic Modernization Outreach Campaign to encourage discovery.*** In early March, ECC SIGDEV analysts held an XKS Circuit Training event designed to expose analysts to five, 20-minute one-on-one sessions in a circuit-type environment. This "speed dating" for XKS consisted of five stations covering topics titled "Intro to the GUI and Basic Queries," "Metadata Setup and Manipulation," "Content and Manipulation of Results," "Introduction to Fingerprints," and "Introduction to Microplugins."

(S//REL) Over four days, 68 students were walked through these topics with five different instructors, able to ask specific questions and get more comfortable with the tool. "Everyone likes a new toy, and there was a lot of excitement about it. They will at least try it against their target and see what they will get out of it," said [redacted] one of the instructors and a SIGDEV Analyst embedded in Africa Division.

(S//SI//REL) With traditional targeting, analysts cast their nets wide into the murky waters of network traffic and haul in anything that gets caught in the net. We are like Forrest Gump on his shrimping boat off the coast of Alabama pulling in a boot, toilet seat, seaweed, and there they are... three shrimp! We burn up a lot of resources getting those shrimp, those reportable documents or metadata used to expand target knowledge, and we deal with tons of toilet seats, the spam and other junk. Then, we repeat the same process and hopefully catch enough "shrimp" to have ourselves a little cocktail. XKS has become so important because with it, analysts can downsize their gigantic shrimping nets to tiny, handheld goldfish-sized nets and merely dip them into the oceans of data, working smarter and scooping out exactly what they want.

(U//FOUO) And a short, two-hour class is an easy gamble of time for the hopes of being able to work smarter and more efficiently. ECC analysts have been trading in their old nets for new ones and are thrilled with their catches. Discovery can only occur if people are willing to try new things, and more of our analysts are getting comfortable with leaping into the relatively unknown world of XKS.

(U//FOUO) "The first time I saw XKS, I said, 'Whoa!!' It is intimidating because you open it up and you see all these queries and fields," said [redacted] "We took the students from that response to being able to approach it and navigate around in it. They see it differently now and know it's not a seven-headed dragon." This gentle introduction has definitely enabled analysts to ease into XKS and get more comfortable, and with that it has radically changed the overall mentality towards

the tool.

(S//REL) ***Across the ECC, analysts wholeheartedly agree that the Circuit Training setup and content was a catalyst to give XKS a try or take existing users to the next level.*** The one-on-one setup provided a heavy injection of tool knowledge into each student. "Before the training, I was just happy to use it and not go to jail," said [redacted] a Circuit Training student and Arabic/French Language Analyst for CT (Counterterrorism). "Now, I feel comfortable in my ability to use it and NOT go to jail. I used to always ask someone to look over my query before I submitted it. Now, my hand doesn't need to be held."

(S//REL) That Circuit Training must be one tough training to pull off, you say? Not so, says [redacted] who spoke about the "off-the-shelf" nature of the training. "The framework was already developed by GCHQ, so it was simple for us to read over their notes, make it applicable to NSA, and conduct the training. We didn't have to spend time writing modules."

(TS//SI//REL) From the leadership level's perspective, the time invested sending analysts to the class had a tremendous return. [redacted], Tech Lead for the 50-person strong Africa Division, said, "The brevity of the class made it easy to send our people. Now we know exactly why we want to use it, and we have discovered new traffic and documents. Our analysts have been building hashes for document tracking and rolling them into fingerprints. We have been getting documents in XKS that we were not getting in our PINWALE queries. Just today analysts found reportable material from the Tunisian Ministry of Interior that was not from any selectors we were targeting. Now we know what we can do with XKS and exactly why we want to use it -- to make these discoveries."

(S//REL) These discoveries are igniting a trend of using XKS on a daily basis. "For daily pulls, analysts go through TransX, PINWALE, and now XKS to see what's new for the day," [redacted] said.

(U//FOUO) Combine these exciting finds with the introduction of XKS Skilz points, and you can see why McDonald's teamed up with Monopoly years ago: people buy more and even super size their orders just to get game pieces. With the brainchild of Skilz, where analysts can earn points and unlock achievements for performing tasks in XKS, people are willing to try new things within the tool. Analysts think to themselves, "Using the Pivot Data feature will earn 30 points... I'm going to try it and see what happens." Discovery! Points! We have been lured by our geeky desire to unlock achievements and earn points, and bragging rights are everything.

(U//FOUO) "Definitely a number of users have gotten into the Skilz points. We have several people at level six. They see what they need to do to earn more points and start trying out different things," said [redacted] In fact, ECC analysts now have the highest average of Skilz points compared to all of the S2 product lines and have written the most fingerprints per-capita! Some people say that the potent combination of Skilz points, the Circuit Training, and the team of easily-accessible, on-site instructors is the secret to ECC's successes with XKS.

(U//FOUO) Maybe XKS is a seven-headed dragon as [redacted] mentioned. Big and scary? Sure. Strong and powerful? Oh yeah. But, the ECC is taming it, and it is ours

to do with whatever we like, including catching shrimp.

(U//FOUO) POC: [redacted]) ECC SIGDEV.

---

* (S//REL) Here are charts to illustrate the point:

. .