Chapter 29: A New Day In Paradise: Day 13

Sandy and Lionel meet Jane, Mark, Anna, and Brian in the Trawler's adjoining apartments for a walk to breakfast. Brian walks with Sandy and Lionel toward the Eneida along the local shoreline road. Brian checks out the new parking location of the van on the parking deck. Anna, Jane and Mark follow a comfortable distance behind. Brian request seating for six on the Terrace so they can observe the Liman II beach and the Operations Building. When the Weldons and Anna approach the Eneida Terrace, Brian rises.

In Italian Brian signals the Weldons to join them. "Buongiorno. Come va?"

Mark responds, "Va bene. Va bene."

The Weldons and Anna join the earlier group. After the first trip to the breakfast buffet and coffee has been served conversation begins.

"Our ladynada has done it again. She and her crew have created an application that Randy has already uploaded this morning to the Daisy 3 (Ramesh). It is designed to infect computers that are attached to the WiFi server to which Daisy 3 is connected. Once the a computer is infected with the application, the application searches for a unique GUID 64 bid identifier in the /var/log folder. If there is none the application then searches the '/var/svn/repos/eclipse_devwrk' repository folder. If it is found the application then crawls across the computer looking for the root user's id and root user password. If the repository folder is not found the application destroys itself leaving random none sense where the application had been previously stored on the infected computer. Except that it leaves a unique GUID 64 bid identifier in the /var/log folder. It will take a while for the application to propagate through the population of computers in the Operation Building.

"Bottom-line ladynada's virus searches for the root user identifier and password. When that is found it is decrypted by the application. If the application can not decrypt it the encrypted password is sent to the Daisy and forwarded to the NSA for assistance. It will be cracked. Then with the root identifier and root password the repository is ours and the telltale GUID identifier are overwritten in /var/log folder with trash for of the infected computers.

"So all we need to do now is wait and begin planning actions. DorsalFin wants complete approval of any further actions besides listening to Daisy 3 and Daisy 4 and monitoring the crawler application."

"Jane and I still need to have a presence here at the Eneida apartments now that the van listener have cleared from here," points out Mark. "We need to end the photographing of the external staircase of the Compound and send the equipment to the warehouse. Let's keep it here in Ulcinj until we wrap-up. Then expedite it to the States. "

"Anna, you need to plan staying in Ulcinj and perform your daily monitoring of Daisy3," requests Brian. "Lionel if you do not mind will you also sit with Anna to assist?"

"It's good clean work in a scenic Adriatic coast resort. Who could complain? Especially since Sandi and I have not yet received of return tickets?"

"Nice way of asking 'how much longer'," notes Brian. "A couple of more days maybe before we want you to relocate away from any 'action' that may be approved."

“Lionel, you and Sandy need to talk it over about whether you want to spend a bit of vacation time here in Ulcinj after the Daisy 3 monitor is no long critical. DorsalFin is good with whatever you decide. If you wanted to vacation on the project’s dime you could probably plan on four-five weeks. I would have Randy work with you as a guide and translator. He has developed an affinity for one of the local ladies. So it would be a win-win for everyone.”

As the waiter returns to pour coffee conversation drifts back to the weather and touring the Museum of Local History in Ulcinj.

“So let me understand what we are doing for the next few days as we phase down,” says Jane. “First we continue with the ladynada virus crawler search. Second we continue the daily Daisy 3 active monitor. All the other Daisies stay in place and revert to passive listening. Three we breakdown and closeup all other surveillance equipment. Fourth we take no other action without approval of DorsalFin. Our guest play tourist except for the daily Daisy 3 active session.

“If you agree give me a thumbs up, please.”

Surveying the table she sees everyone with their thumbs-up.

“Good we have a general agreement. But watch-out for details and bumps.

“Mark, are you ready to pack some equipment?”

“Let’s doit,” say Mark as he rises. “We will call you Brian when we need a van and some Marines to help tote the equipment over to the warehouse.”

“Roger that.”

“Why don’t the four of us wander back to the Hotel,” suggests Brian. “We have until around 1630 to sample the coffee houses in the area.

“I would like to check with Randy and Joe to see how the virus is working. But that is basically the show for today.”

Brian signals the waiter for the check in the classic Italian raised left hand opened palm and right hand two fingers making a scribbling motion. As the waiter approaches he adds ‘biglietto per la colazione” for effect. The waiter presents the breakfast bill and Brian puts the meal on the room key card and a healthy tip.

The foursome walks two by two down the local shoreline road without incident to the Hotel. In the Trawler’s enclave at the Hotel, Randy reports good, slow progress in weeding out the computers that are not serving in the svn server role.

Brian hands Lionel and Sandy credit cards and passports that properly reflect their names, visa stamps, etc. He encourages them to investigate the city with Joe as their guide if they chose. He explains that their per diem on each card is $1000US. He also tells them that they will be tracked via their cell phone. If an issue arises just tap the Mayday icon. It will take a few minutes to mount the cavalry. But it will come so just play the role of ‘pazzo americano’.

The honeymoons decide to go without the guide but accept a ride to the Old Town district. They will see how tired they become before calling for a Trawler courtesy ride. Brian suggests that if they need a ride they call by 1530 hours to insure making the Daisy 3 late afternoon monitor.

At 1530 hours Lionel calls from Restaurant Fisherman Hari's terrace for a ride. Shortly, Randy arrives to return the Lionel and Sandi to the Trawler's Hotel suites.

The Operations Building crew of Sunfish begins to close-up shop just a about 1700 hours. Daisy 3 is soon capturing Ramesh in a technical discussion about a feature being developed in one of the projects branches. Apparently, the phantom reviewer or as the Agile Manifesto would say the customer stakeholder was pushing for something a bit different. The discussion dies quickly as the evening build began to suffer significant failures. Ramesh was forced to apologize and ask for more time on that feature. The Daisy 3 goes silent as Ramesh utters frustration in having to deal with a customer and floating design goals. He leaves the office shortly for the evening.

There is nothing that Lionel can contribute to Anna's translation from the standpoint of a programmer's knowledge of the original prototype of Spinnaker. Anna closes up her listening station and meets Ron and Joe at the door for a conservative evening of dining.

Mark, Brian, and Randy pull Lionel into a discussion of the findings from today's search for the root identifier, root password, and the location of the svn server. Thanks to ladynada's scanning virus crawler and NSA decryption this confidential project support information is now know.

Randy brings Daisy 7 back into an active mode. He confirms the GPS location with its prior location from its original verification. He announces that he has now connected the Trawler's laptop to the Daisy 7 as the system root using the virus search results. Then he asks Lionel if he would like to drive. That is Geek slang for take over the keyboard and mouse inputs. Before leaving the garage, Lionel asks for an image backup of the laptop Randy is allowing Lionel to drive. Lionel makes a Clonezilla backup of the laptop. That done he knows he can restore the laptop to the exact condition it was in when Randy allowed him to drive. That will prevent cross contamination with agents and monitors that one might be encounter 'jumping across' to the Sunfish Operations Building computer network.

Via Daisy 7, Lionel as root now logs-on to the Sunfish Operations server on which the Trawler ruse found the /var/svn repository. As the super user root Lionel immediately creates a new user name mightymouse and generates a password flopdog*87882, he adds mightymouse to the 'root group' and several other groups like the sudo, adm, tty, dialout, www-data, and svn. Then Lionel logs the root user out and logs in as mightymouse.

As mightymouse he starts a browser session and checks to see if the Sunfish Operations Building crew is using the Apache Subversion tools as the Spinnaker crew had used. Lionel discovers that the answer is yes. Then all he needs to do is enter the Uniform Resource Locator (URL) for the svn of the Sunfish project. After a couple of tries he establishes that it is http://svnwebhost/svn/repos/eclipse_devwrk/. Then he follows the same path he used for the Spinnaker project to locate the critical build folder as: http://lsvnwebhost/svn/repos/eclipse_devwrk/trunk/e4SpnSpn/build/. Within that folder he finds three files: build.properties, build.xml, and build_out.txt. He pulls down these three files to the Trawler' s laptop he was provided for his use. He also finds a history folder were several months of nightly build history has been stored.

After completing the acquisition of the critical files from the …/e4Spn/build folder, he navigates to the …/e4Spn/com folder. This folder has multiple subfolders and roughly 210 code modules. To avoid appearing in the svn history log as 'checking-out' artifacts he must use the Read-Only, he must individually open and save each java source file. Although time consuming it does not

leave a ‘trail’ or ‘log’ of his presence. He warns the Trawler observers that this effort will consume a good while. He also warns that a similar effort will be required on the …/e4Spn/web folder.

Lionel starts the capture effort for the …/e4Spn/com folder artifacts.

As he performs the capture processing, Brian tasks Ron to order heavy hors d oeuvres Adriatic style from the maître d' with aqua con gas.

Sometime later Lionel begins the same capture processing on the …/e4Spn/web. This is where the web applications html pages and web support resources reside. It is also where the Spinnaker-Sunfish Roadmap and User Stories reside.

With the Roadmap and the User Stories now available he is ready to prowl the various branches that might exist in the http://svnwebhost/svn/eclipse_devwrk/ repository.

Lionel explains, “Projects like the Spinnaker-Sunfish typically have only one trunk. The contents of the trunk are the gold standard artifacts for the project. Artifacts in the trunk are used to generate or produce the functioning release of the project like Spinnaker-Sunfish. Typically a new feature or a change to an existing feature is managed from a branch. The branch is a safe playground where a developer can make mistakes and develop code without ‘breaking’ artifacts. To create a ‘safe place to play’ code is pulled from the trunk. The developer or team of developers can then hammer away without harming the ‘gold’ trunk version. Then when the new code has been create or changes made they are tested. Upon review they are pushed back to the ‘trunk’. Protocols vary between projects but typically there is a daily build of the the code in the ‘trunk’. If new code ‘breaks’ the project’s application, a tiger team looks into the failure mechanism. But still no harm is done since the trunk can be unwound to its prior state.

“What we want to do is prowl the branches looking for any feature or change that is not officially on the Roadmap or in a User Story. That will be where Ramesh’s tormentor has driven Ramesh.”

Lionel next goes to the /var/log folder and pulls copies of the syslog, syslog.1, six sequential files with the labeled syslog.*.gz where * represents a single digit number between 2 to 7 inclusive. He explains that he wants to examine the system logs for the eight days. Then he begins to search for ‘cron’ activity. Shortly he recalls the the Spinnaker project did not employ any date/time trigger to perform builds or provide automated svn archiving of work product. That explains why Ramesh ended his day as the last person to leave the developer’s alcove.

Cautiously he performs a checks the laptop he is using to see what process may be talking between his laptop, the Daisy 7, WiFi, and the svnweb server. Using the System Monitor, Nutty, and WireShark tools, he does not detect any unwanted communications flow. He then reverts to the root account on the svnweb server and deletes the mightymouse account.

Turning to Brian, Lionel says, “I will need a decision on how you want me to proceed. I have a good feeling that we will have left minimal tracks in the Sunfish’s network once the ladynada unwinds the GUID that were placed in the various computers’ /va/log folder.

“Do you want me to use this laptop for my looksie into the files we pulled or do you have one that is pristine that I can borrow for a day or two. Either way the the laptop that Randy gave me to use tonight needs to be restored to its original condition.”

“I can have an Ubuntu laptop pulled from the warehouse that will have the basic load plus whatever you feel you need loaded to it.”

“Okay. I will start moving the files we downloaded this evening to the portable storage media you already provided for the Clonezilla image backup of Randy’s laptop. When that is done I will restore it to it prior state,” finishes Lionel.

“While we wait for the transfer, I need a plate of those hors d oeuvres.

“Thanks for pairing Anna with Sandy while I do this ash-n-trash stuff.”

“Do you any ideas or recommendations at this point?”

“Let me look at the branches versus the Roadmap first.”

“Okay.”

Brain and Lionel join the gaggle around the serving cart of hors d oeuvres and aqua con gas.

Following a brief interlude for a hurried supper Lionel returns to the task of restoring the Randy’s laptop to the same state in which it was just before he loaned it to Lionel. The restore takes a little more than an hour. During that time Lionel meets Sandy and Anna as they return from a beach walk.

“How’s the beach?” asks Lionel.

“A little colder than I like but the sun was pleasant.

“How’s the Geek stuff going?”

“I am working as we speak. I will spend another hour or so and then call it a night. There is plenty to do tomorrow. Then I have another monitoring session in the late afternoon. How about we plan on breakfast then spend some time in the morning sightseeing? Then if I return in after mid-afternoon, I should be able to keep the government happy.”

“Sounds like a plan.”

“My duty calls. I will see you in a bit.”

Checking the status of the Clonezilla image restore, Lionel finds it nearly done. While he waits for it to complete he introduces himself the the pristine laptop that he can use and abuse without worrying about infecting any other system or device. Lionel takes and inventory of the applications on the Ubuntu Trawler loaner laptop. Currently he has access as the root user. As the root he creates a user justme with administrator rights and membership in root, and a slew of other groups to support his needs.

He switches user identity to justme. He adds Geany and Meld for starters. That gives him a powerful editor, a tool for making rapid file and directory comparisons. He plugs in the storage media with the downloaded folders and files from the Spinnaker-Sunfish svnweb. Then he installs an SD card with a copy of the original Spinnaker prototype that he created from Frank Rana original micro

SD card from what feels like many, many years ago. By then the Clonezilla image of has completed. He powers that laptop off and returns it to Randy.

Returning to the Ubuntu Trawler loaner laptop, he starts the Sunfish Roadmap, roadmap.html. This is a webpage that has a table with six columns. Each column represents a different Release during a calendar quarter. Each release is decomposed into Sprints. Each Sprint has a collection of User Stories listed.

Based on this document he expects to see branches associated with code modules that can be referenced directly back to individual User Stories, Sprints, and Releases. If a branch exists that is not linked to a release it is either a Spike or something created 'off-the-books'. A Spike is a valid Agile approach. Any 'off-the-books' entity is not valid and outside the vision of the project. Lionel is looking to determine if either are present in the Sunfish artifacts.

A Spike is a short-term experiment to overcome an obstacle or to test some specific innovation that has risks. A Spike never lasts more than two weeks before being terminated or becoming the foundation of a code module.

An 'off-the-books' entity is being funded from outside the purview of the project sponsors and valid stakeholders. Lionel suspects that there will be 'some number' of off-the-books branches.

Lionel limits tonight's search to the current calendar quarter and the next quarter. Lionel locates seven branches that appear to be bona fide Sunfish Roadmap Sprints with corresponding User Stories. He finds two branches which do not appear to be bona fide. There is one each under the two Releases he studied.

Bottom-line, he know suspects that Ramesh is pushing unapproved code module development that may not necessarily be sanctioned by the Sunfish executive review team. In other words he is double dealing his Catalina employer.

It is getting late when Lionel joins Brian, Jane, and Mark in a reflection on today's 'doings'.

"Well Lionel what did you discover?" asks Jane.

"It definitely looks like Ramesh is two timing his Sunfish patron as well as at least the state of Georgia."

"What would you do if we gave you complete control?" Brian queries.

"Well first would you give me complete knowledge of what you already have in play?" challenges Lionel.

"No Lionel it does not work that way," jokes Brian. "We would have to shoot you after we told you."

"Then setting that spike in the ground, I would want to know as much as I can about Ramesh's rouge partner. One way to do that would be to setup a Ransom-ware type operation to see what shakes-out.

“By that I mean with the Sunfish project is set up with the golden production artifacts held in the trunk folder. The development goes on in one of many branches. When it is completed and verified as good the ‘new artifacts are merged back into the trunk.

“However, Ramesh has apparently had unsanctioned development underway in two ‘rouge’ branches. Both branches are likely destine for a future merges with ‘rouge trunk’ other than the Sunfish trunk.

“But your guess is probably as good as mine as to where that ‘rouge’ trunk might be located.”

Violating a common tradecraft rule, Jane announces, “We already have a double sting running on one member of the Sunfish executive team. So we know that there are at least two bidders attempting to purchase ‘licenses’ to use the Sunfish application in two regions of the US.

“What we have learned from you is that Ramesh may already have found someone outside that scope of the known sponsors or patron with who he is dealing.

“Question for you, Lionel. How far along has the Ramesh-Rouge-Link progressed? Has he started transmitting Sunfish artifacts from the ‘rouge’ branches you identified?”

“I can not tell you that merges have or have not already been executed to the ‘rouge’ trunk. What I can tell you is, Ransom-ware is a good way to lock-up Ramesh’s environment and may be smoke out his ‘rouge-buyer’. It will also tell you whether Ramesh uploads the content from the rouge branches each day or whether he plans a one-time merge.

“Unless you have something further, I am going to join Sandy and Anna on the balcony downstairs. I will see in the AM.”

“I will contact the Spook Tower to rush ladynada efforts on a Ransom-ware application-sting set-up using the Ramesh’s Daisy 3. They can run the ransom administration from the Spook Tower.”

With that the Three Ulcinj Plumbers call it a day. They wander out onto the balcony for a final Pinot Noir. Anna joins them shortly to close the loop.