**Project Completed by:**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

>> And we're back. Our final session today is hunting a ghost on the trail of adversary. Jodi Ito.   
  
>> Thank you very much, Jacqueline. I also have sitting here with me is Melvin security specialist on my team and he's going to be here monitoring the chat session too so if any questions pop in, please feel free and he'll be able to get to them as I'm talking. One, I'd like to thank the EDUCAUSE organizationer to put us last. It allows me to reference the excellent presenters preceding me because I'm going to reinforce concepts, processes and procedures that I'm going to discuss. To get started, I just wanted to throw up a quick slide about what we're going to be talking about in a brief time. I apologize if I talk quickly but this is different from the previous sessions as it is about a particular situation that we underwent here at the University of Hawaii: Just a little bit about the University of Hawaii system. I'm the chief security officer for this system and we're a system consisting of ten campuses of which three are four year and seven are two year campuses. We have a flagship campus and did you ever have one of those days? Really we've had about three hundred and forty-one of them since last year, September 15th and it's still ongoing but probably not at the intensity that it was last September, but we consider it as an ongoing situation. So, this all started with a text. Well not that text. For those of you not familiar with this situation in Hawaii we actually had an emergency management team from Hawaii text us out but the text that kicked us off was this one. This particular text was sent to me from a researcher in charge of a research unit and we'll describe the things that focused on. What that did for us was on September 15th that researcher was actually contacted by a colleague at another University. What had happened was the researchers e-mail account was come prommized and the attackers sent spear phishing mal ware attachments and that's when the researcher contacted me by text at six in the morning and we were concerned that the entire male server was compromised and we immediately blocked that server on the network and at that time I received an attachment from another institution. The reason why those two items have the red star next to them is that those two events actually triggered and escalated some of the attackers actions on the network because the attackers were monitoring the male server and they were also monitoring virus total. When they saw that go up, they immediately started taking more aggressive actions like large scale. This is a screen shot of the actual e-mail that started all of this. So that red arrow actually highlights the document name and the reason why I leave that document name there in this and didn't sanitize it is because it's referenced in a public report and I'll give you a link to that a little bit later on, but this e-mail was sent specifically to key researchers at other institutions and after we did some analysis, after we stepped back and had time and went through all of it, we realized that the attackers were targeting a specific type of research. Notice it's research. This is a type of data at the University that we really don't have a good handle on. People don't put the same value on research data as we would with institutional sensitive data such as social security numbers, student information, personnel information. This to us, we knew that research data was being targeted but we hadn't seen it here at our institution previously. We actually did an analysis of the attachment and the mal ware embedded in the attachment was specific ex/PHROEUTing and it had the specific attackers IP address and that's important to us because that helped further our analysis and if you notice the date on the CV E it was announced by firewall on September 12th. Now remember that we got the notice of an attack on September 15th so the actual time between the announcement of the CV E versus when we noticed it was being used on us is a very short window. So, for us, this is an all hands on debt. We don't know exactly what's happening, we don't know the extent of the compromise and because the recipients of the spear phish at the other institutions worked with defense, some federal scrutiny was brought to a situation here and we needed to identify the route cause of the compromised account quickly. Was the entire server for that initial researcher compromised which would be all of the credentials for that unit come pro /PHAOEUZed? Because we knew it was using the initial researchers e-mail credentials we were able to grab the outlook web access logs from the male server itself. Obviously, it was annex change male server and when we went into the logs we were able to see that the researchers credentials were us to log into the webs access for male on those dates. As you can see, the durations varies. Initially it seems to be a first check for about five minutes. A day later we can see the attackers were trying to use another e-mail account from a University University of Hawaii IP address. The first user is from an external IP and the three subsequent accesses was from a University--University of Hawaii IP address and you can look on the 31st and the first for the researchers e-mail account, you can see that the durations of their time spent in the account was a lot longer room. Probably guessing accurately that the attackers were in there reading all of the e-mails in the researchers account to one, understand more about the role that the researcher played and who their key contacts were at other institutions. We were actually able to track that to the researchers e-mail account, specific e-mails that were in the mail box that had the addresses where the highly targeted spear phishing e-mail were tracked to and the attackers were using it to cross their out bound spear phishing accounts. Then on the 15th the attackers used the account and then sent those highly targeted spear phishing e-mails out. In particular, there were eleven e-mail spear phishing e-mails sent to twelve individuals and these individuals opened the attachment but there were firewall rules on their subnet that we used at that time and even though they opened attachments the malicious code couldn't communicate with the commanding controls that the attackers set up. We were able to identify seven University University of Hawaii systems that were communicating with the attackers IP that we got from the first mal ware attachment and then that department also conducts maritime related research. Now, of note, the department listed here is different from the initial researchers department. But the initial researchers had an office in the building of this second department. Okay? So, these are the seven computers that we observed communicating with the command and control. All of these seven computers were in that second departments network. And as you can see, we have an active directive file server and a combination of old outdated operating systems as well as a few newer operating systems but they are all windows based. And then for us, sort of like the tidal wave begins. We don't know what it's actually going to lead to but after we dive down into the technical details, the slides will have a lot of specific information but I'm going to just talk to you briefly about it but the slides will be your reference materials. If you have questions about the technical analysis please contact us afterwards. We started with the Windows XP machine and we had trouble identifying the location of that machine. If we had Joels scope in place it might have been easier for us to access the machine. Because there were so many computers in that room we had to trace wires to locate the actual machine and the actual machine appeared to be an old machine that was destined to be disposed of. It was under a desk. There was no monitor connected to it or a keyboard connected to it, the fan was broken, the light was broken so we had no physical indicators that the machine was actually running, but we suspect that that machine was what we call patient zero. That PC was exposed to the public internet, exposed and the attackers immediately compromised the machine and replaced the sticky keys with the command prompt. Very subtle and again, there wasn't a keyboard on it, nobody knew the machine was running so it made it hard for us to track down. The attackers then followed up and downloaded additional tools to machines and executed their backdoor. They established persistence in that machine and that machine again is on that second departments network and then the attackers strategically leveraged tools like packet captures so that they can capture credentials that's transiting the network in the clear. Here is actually some of the specific tool sets that they were using. They didn't necessarily use all of these on all of the machines but for the most part most of these were being used. Again, we had seven different machines that we identified and we had to go out and do imagine captures of all of those machines, just memory dumps and then we had to bring them back and analyze it to identify how much broader this attack was. The attackers were pretty well buried in that departments network. You know, we're just trying to discover and learn more as we go along. We're trying to analyze, re mediate and also keep in touch with all of the community members affected by this, deal with our federal partners some of which were law enforcement and also the communication piece of it was the thing that we had problems keeping up-to-date with because there were so many things going on at the same time. With the Windows XP, again, there were brute force into it and then from there with their packet captures they were able to compromise the modern Windows 7 and windows ten and also something that we need to mention is that that department was using active directory, the main controller and because they were able to snip the network we suspect that the attackers also gained the credentials to the domain controller itself. Basically they had the keys to the Kingdom. For the modern operating systems, Windows 7 and windows ten they were then using the compromised credentials. Based on persistence by established by a service. In some instances there was databased servers on that machine and we actually saw the tackers craft their service to represent a database process and it wasn't the same service on all of the machines so that's how we knew they were being very stealthy and very crafty and customizing their persistence based on what they found on each of those systems. The service then executed Java script that downloaded cobalt stripe and avoided the attackers huge advance. Based on our investigations of what we knew and what we could find online we deduced that this was a particular group that was attacking us. And we actually were able to put together this slide that has the tactics and procedures and we were trying to create a template that we could use to search and hunt these attackers anywhere else throughout our network. Not much time left so I'm not going to go through all of these in detail. Please feel free to download this presentation and contact us offline if you have more specific questions about what we found. It always is compromising the victims PC, executing a Java script which would download additional tools from the command and control and then using a whole suite of tool sets to try to in filtrate additional systems throughout the network. Of particular note is that last bullet with a call back to the command and control is done in a quickly get done request. That was encoded in base64. By far this is the most sophisticated attackers that we've seen on our network to date. We suspect that they may be residing at other parts of the network. We have not been able to actually discover anymore of their persistence in other networks yet but this is sort of an ongoing situation. I wanted to provide on this slide a few more links to additional information related to what we are thinking is our attackers. And the checkpoint next to that last bullet item again is that public report that actually called out our specific situation. This is a screen shot from that website, that link there on the last slide and it actually specifically identities maritime and defense targets and again, that was the type of research that the two research units were dealing with. So the key takeaway, it's industry targeting defense contractors and Universities particularly those with military research ties. Particular interest in naval industries including shipbuilding and related research. Again, this is the document that I had highlighted on that screen shot of the actual spear phishing e-mail. This is the file name of the document that was actually attached to that spear phishing e-mail. That was the mal ware that was in that document. That was the one that was uploaded to virus total and one of the other institutions that the spear phishing e-mail was sent to utilizes proof point. That's how they got involved into this particular incident of ours. Again, ongoing incident. As was mentioned earlier, I believe Randy talked a little bit about web bugs and using it for proactive protection of our documents with sensitive information. We think that the attackers were actually using these web bugs to gain more information about the networks that these potential re con sense e-mails were sent to. What we saw in the initial researcher, the researcher that initially alerted me to this situation is that the researchers had in their mailbox a number of these similar types of e-mails that appeared to be resumes. Most of them were from foreign contacts and at the very bottom of it there is a one by one pixel. That un displayed graphic links back to a website that we suspect will provide additional information about the information on which that e-mail was read. IP address, operating system and it will also provide web browser inversion such that the tackers may have additional information to know how to come back in and additionally, find weak and vulnerable systems that they can now attack. What happens with these types of e-mails that a lot of the researchers received is that one person would get it and if it's not in their area of expertise they would then start forwarding that e-mail to other members within the entire department. It's potentially possible that the researchers were able to gain a lot of information about the network just by the forwarding of these types of e-mails. We did a lot of recommendations because now we're trying to fix the problem while we're still analyzing the problem. The analogy for us is we're trying to fix the plane while its flying but the number one thing that I think everybody needs to understand is that understand that all of you needs to inventory their computing assets. Get rid of every old machine, old operating system, X P, server 2003 and replace with modern operating systems. Remember that we said that the X P systems were brute forced and that's how they were able to gain the credentials for other active domain users including the domain administrators credential. They were able to grab the credentials and logged into the more modern systems. People like to share things widely and we have a lot of remote access to systems. People want to R VP without providing the adequate protections in place, and then simply put, moving support doesn't protect it because they are scanning the heck of the network also. As talked about in a previous session, use two factor multi factor authentication whenever possible because even when the credentials are required that second factor would still be required to gain access to that privileged accounts. We have an entire information campaign going on. Since this occurred last September we immediately mobilized and did a ten campus awareness road show. We framed it from the per secretary tiff data governance and protecting sensitive information. We did ten campus briefings and did additional presentations to the functional areas. We used employees, professional development opportunities, we used the research certification track that is put on by the office that handles all of our research contracts. We talked to fiscal administrators and officers and all of the IP staff at an annual all campus workshop and this is an ongoing process. This is not a one and done. This is going to be happening to us continuously so we will be doing these road shows again this semester and following up with mandatory training sessions. As always, never waste a good crisis. Always make sure that you leverage any opportunities that you have. In this case, it's using a situation to promote awareness and ensure that people understand that research data is also just as sensitive and desirable as traditional institutional sensitive information such as student information, personnel information, social security numbers and credit card numbers. For us, we had an incident response plan but we really need to broaden it so that more people are aware of it so that we can on board people into what we're calling an incident S.W.A.T. team. As I said, we had seven compromised machines that we knew of that we needed to take the images of so that we could more fully determine the impact of this situation on our entire university network and that actually is something that you should put in place ahead of time, provide training opportunities to those individuals and also so that they understand their role when you invoke them in an incident. The other part of it that we struggled with was sort of a communications response plan. What about the internal communications to the technical IT staff that is supporting this? It's also a need to know because some of the guidance that we're getting from our federal partners indicated that it was not a known attack TT P so they really wanted to keep that a little bit under wraps, but as the incident unfolded and over time we actually could see that other institutions and other organizations actually were affected beyond the University of Hawaii. As I mentioned, it's an ongoing investigation and that actually brings me to the end of my slides. I believe I have five minutes left for you guys to wrap up.   
  
>> Yes so Melvin has been fielding a number of the questions that have popped up in the chat window but there's one from Dave at Oregon State that perhaps you could comment on. Did you get cooperation and support from the DMD?   
  
>> Actually, they were there and they asked if we needed assistance. Because we weren't sure about what we were up against we actually decided to try to do most of the analysis inhouse. We did involve FBI, DHS DS S and MC IS. Was that enough acronyms for everybody? But really it was difficult coordinating with all of those federal agencies. It did add a level of complexity to the conversations that we were having. Additionally, we had to bring our general council on board because of the sharing that, I guess some of the agencies wanted us to do with them. But because most of the systems, we were not sure it was research only or if there was student information or other University information sensitive information on those images we had to require subpoenas before we could turn those images over to the FBI. I guess that the key takeaway here is to make sure that you have those discussions with your general council ahead of time. You know, really to understand the legal processes and what the Universities stance is the most important thing.   
  
>> That would facilitate the conversations that you have beyond the University. I'm not seeing any additional questions at the moment. You can see that the slides from Jody and Melvin are available online at the moment from the agenda. Thank you again, Jody. This was fascinating and informative and I'm sorry you had to go through it.   
  
>> Thank you very much for your sympathies. We appreciate that.   
  
>> Alright. Thank you everyone who is online right now for joining us for the past few hours. We heard amazing talks and I'll turn it back over to Valerie.   
  
>> Thanks so much, Jacqueline. As we end today we wish to extend our warmest thanks on behalf of EDUCAUSE, to all of our speakers and we sincerely thank all of you for your active participation today. If you are trying to submit for CPE credits if youself report and maybe include the agenda and your registration confirmation, hopefully that should be enough but you can feel free to contact me offline. I'd be happy to verify your participation. We also hope to see you next year at our 2019 security professionals conference. It will be next May in Chicago. If you are feeling inspired by today's sessions and want to submit a proposal it opens in September. Please keep on eye out for that. Complete the evaluation. On behalf of my cohost EDUCAUSE colleagues, this is Valerie wishing you a wonderful afternoon. Thank you

**[End of Webinar]**