Part 1: TJX and Heartland; The Role of CERT’s Forensics Team

Julia Allen: Welcome to CERT’s Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Shownotes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm very pleased to welcome Kevin Moore and Cal Waits, members of CERT’s Forensics Team.

This podcast today is presented in two segments. First predominantly Kevin and I will be discussing two cases that the Forensics Team has been heavily involved in and that have been resolved in the U.S. court system, TJX and Heartland. And then following that portion of our conversation, Cal and I will build on these two cases and discuss the increase in sophistication and organization of the intruder community that is launching these types of attacks, and some approaches that Cal, Kevin and their team are using to combat them.

So first of all welcome Kevin, glad to have you with us.

Kevin Moore: Thank you Julia. Glad to be here.

Julia Allen: And welcome back Cal. Appreciate you making the time today.

Cal Waits: It's a pleasure.

Julia Allen: So Kevin, let's get started with some of the cases. Some of our listeners I'm sure will be familiar with the TJX case. It's been in the news quite a bit over the last couple of years. But just briefly for those who aren't, could you summarize the crime, the timeline and what happened?

Kevin Moore: Well TJX is -- I'd be surprised if your listeners haven't heard about TJX because it's been heavily covered in the news. But basically it was an attack perpetrated by Albert Gonzalez and some of his co-conspirators in which they were able to gain illegal access to the TJX network and identify credit card information that they were able to collect from the network and use maliciously, unfortunately. Basically what they were able to do was they were able to access the network through a vulnerability that existed in the corporate network and then gain access to stored-in-real-time credit card information that the retailer had. It stands as one of the largest frauds or collection of credit card information in history. And it's recently come to somewhat of a close in regards to Albert Gonzalez who was sentenced in March of this year to 20 years in prison based on the crimes that he perpetrated.

Julia Allen: So when did the first intrusion or first access of unauthorized access of data occur, and then how did it develop over time, to the best of your knowledge?
Kevin Moore: Some of the details, unfortunately, we can't go into too much detail on. But the approximate start date, or the initial attack, occurred in 2005. And the initial attack was on a node in the TJX network, basically one of the retail outlets. And through that initial intrusion, Gonzalez and his co-conspirators were able to escalate throughout and spread themselves throughout other various aspects of the TJX network. And they were able to gain and maintain access for a number of years, up until at least 2008 and possibly into 2009 as well.

Julia Allen: So what in particular -- and we'll talk about this a little bit on the Heartland case as well -- but what role did your team play in the investigation? I think our listeners would find that pretty interesting.

Kevin Moore: The CERT Forensics Team was involved primarily in aiding the Secret Service in the collection of evidence and actually going in and creating forensic images of computers from Albert Gonzalez and his co-conspirators. In addition, we were involved in some of, quite a bit of, the analysis as well.

Due to first of all the volume of data, there was a great number of terabytes involved in the matter that required a collaborative effort in order to analyze the data. But we were able to house that data in our C-CAP environment and perform a great deal of the analysis here. In addition, because of some of the complexity of the systems used by Gonzalez and his co-conspirators, we had to deal with things like encryption and certain configurations that the conspirators had on their systems, which required some additional expertise that the CERT Forensic Team was able to provide.

Cal Waits: I think what's interesting to note is, as Kevin touched upon, is one of the challenges faced. As the amount of digital evidence increases, the ability to wade through that amount of information and take a meaningful look at it becomes more and more difficult. And our role as a federally funded research and development center allows us to look at this objectively, without the same pressure of operational intensity that many of the law enforcement agencies that we support are facing. And so we can look at the challenges that they're having and come up with solutions to them. And one of those solutions is our C-CAP as we call it, our Clustered Computing Analysis Platform, C-CAP -- that allows us to host the data, or the digital evidence, to host it here in a central location. (and C-CAP happens to be here at Carnegie Mellon University but you could have a C-CAP instantiation anywhere) And then open up through secure access to analysts wherever they may be. So those analysts could be here -- we had some of our analysts working on the case -- as well as open it up to Secret Service analysts, to analysts in other agencies that are participating, if it's a joint investigation. And it allows us to take advantage of that; that the traditional computer forensics lab does not support that capability.

Julia Allen: Oh that's great information. Thanks a lot Cal. So just to add a little bit more meat to the bones of talking about some of these cases Kevin, let's talk about Heartland a little bit; it's a little more recent than TJX. So again for our listeners' benefit, what happened in the Heartland case and approximately over what period of time?

Kevin Moore: And again, the TJX and Heartland cases were very similar in that the attackers were able to find a vulnerability on the network. As is the case with most intrusions, they're able to find a vulnerability and exploit that vulnerability. And in this case, it's very similar to the TJX - the Heartland and TJX are very similar -- in that Gonzalez was able to find a vulnerability, use that vulnerability, and ultimately gain access to millions of credit card numbers that were on their systems, and then obviously use those credit cards for profit.
The Heartland case was extended during a similar time period as the TJX; it was within the time period of the TJX, approximately between 2007 and 2009, although the dates are a little bit in question exactly when the first intrusion took place and when they were able to identify the problem.

CLA: Without necessarily going into the specifics of these two cases, are you finding that there are particular types of vulnerabilities that are more readily used for these types of breaches, to get in to take credit card data, other financial data? Just in general, what kinds of vulnerabilities tend to be exploited for these types of attacks?

KM: In a lot of cases it usually has to do with, they're able to find a vulnerability on a single node in the network. And it may be a computer that isn't patched properly; that doesn't have the proper security patches; that doesn't have the proper anti-virus; that has open ports that it shouldn't in their firewall.

There really can be -- for the most part, attackers are going to use some sort of scanning tool and some methods where they're going to basically scan a network or scan a computer and identify what open ports are there; and what the current operating system is; and what the current service pack is for an XP computer or something like that; if it's running antivirus and things of that nature where they're able to either scan a single node on the network, or multiple nodes on the network, to gain detailed information about them. And then they're able to see where the most vulnerable systems are. And if they're able to access those systems through some remote means and try to escalate the privileges on that computer, they then try to escalate the privileges from that computer to the network itself, and so on and so forth, and just kind of keep on -- kind of swim upstream or climb the ladder, however you want to look at it, to make themselves more administrative in the network, or have a more substantial role in the network where they're able to exploit more systems and make larger changes.

So the most common vulnerabilities are just systems that aren't properly, don't have the proper security fixes. And unfortunately it's far more common than we'd like to think, right? But even in cases where there are systems handling credit card information, they may not have the proper fixes that are necessary or that are recommended.

CLA: Okay great, thank you. So in both the TJX and the Heartland case, both you and Cal talked a little bit about the kind of roles that we played. But I'm interested in knowing, do we get involved, does your team get involved from the very beginning of the case or as soon as the case comes to the attention of the Department of Justice, and do you participate all the way through to closure, including perhaps testifying in court? What part of, if you will, the criminal or prosecution lifecycle is the CERT Forensics Team involved in?

KM: It varies a little bit, on a case to case basis, depending on what needs the Department of Justice or Homeland Security or whoever we're helping needs for that. We may be handling a small role in the case, where it's just a small aspect of a drive or even a single file. But in many cases we're seeing it from start to finish. And in the TJX and Heartland cases, we've seen it from the point of collection -- actually collecting evidence from computer systems -- to the point of testifying, where needed. So we see it all the way through, in the point of collecting the evidence to performing the analysis and then providing reports and information to the Department of Justice regarding findings. So but that can vary on a case to case basis.
Part 2: Protect Financial Information; Understand Attack Community and Methods

Julia Allen: Okay. And from these two cases, and potentially even from other related cases that you've seen, if you were sitting down and talking to a business leader, what lessons would you encourage them to take away from cases like these?

Kevin Moore: Unfortunately, and especially with companies that are handling financial information (whether it be credit card numbers, debit card numbers, or bank account information), there's an added responsibility for those companies. It's unfortunate that a burden is placed on them but it's part of handling that information, where they are going to be vulnerable to attacks, right? Because there's a benefit for an attacker to target those systems, as opposed to a home user where they may not gain as much information from them. But if they're able to attack a retail network where there are a great deal of credit card information, they would -- that could be financially beneficial to the attacker, right? So there's an added responsibility for those companies, unfortunately.

And really the lesson to learn is -- and I'm sure that Cal can provide some more information on this -- is in regards to just having strong security policy in place. It's a lot of times easier said than done to say, "We're going to implement these security methods because you have thousands of users spread across the country," or even the world in some cases. And all those systems may be potentially vulnerable if an attacker wants to try to exploit them. But there is the responsibility to try to implement strong security policy, and also security measures in place. As I mentioned, just making sure computers are up to date and antivirus is implemented; things that seem simple but are often easier to say that they're implemented than to actually implement them, especially across nationwide or global networks.

Cal Waits: Yes. And if I can jump in here Kevin as well. I think when we talk about strong security policy, and we talk about some of the fundamentals, we want to characterize it also that strong security policy is one that demonstrates a defense-in-depth. And it's a word you'll hear security professionals throw around that phase. But when we say defense-in-depth, we're really talking about in the same way that a ship is built with compartmentalization in mind. So that if a breach occurs in some portion of a ship, you can lock down that portion and contain the damage. And so defense-in-depth is a similar strategy when designing and building out and applying policies to a network -- is that you can build it such that if an event (or one might even say when an exploit or a breach takes place) that it can be contained, it can be identified and dealt with, without spreading across an entire organization.

Julia Allen: Excellent, excellent. So Cal let me kind of turn the show over to you and let's talk. Let's bump this up a little bit, but using the cases in point that you and Kevin and I have been discussing. As I look out into the press where readers can learn a lot about these cases, if they so choose, I'm seeing more and more about what's being called advanced persistence threat; sophisticated malware that goes undetected. It seems like the intruder community is really upping the ante, and I'd be curious in your take on the kinds of behaviors and capabilities that you're seeing in your work.

Cal Waits: I think one thing that I've really taken away from seeing how these investigations play out is that it is no longer -- I think the idea or the picture that many of us carry in our heads of a lone hacker in a dark basement room, taking advantage of a computer network and then reaping the ill-gotten gains, is really a misnomer. These are organized groups of people, each with a specialized skill that they can apply -- whether that's from the person who conducts the first exploit, or even those that develop the exploits, to those that then will execute them. And then as they harvest the credit card numbers or the other personally identifiable information,
harvest those for sale or to farm out to those that will then take that information and monetize it and turn it into money. Because that is the ultimate goal, right? They're not collecting credit cards just as a badge of honor but they want to turn it into cash. And so they have other people that specialize in either selling those credit cards to other individuals or in using those credit cards to purchase goods that they can then turn into money.

**Julia Allen:** Is it fair to say that crime is present in all of our societies in various shapes and forms, and the internet and our various networked environments has just become another arena, correct?

**Cal Waits:** Certainly. Fraud has been with us for a long time and the internet certainly did not invent fraud. What it does is it's just one more avenue to facilitate that fraud. I think what scares people, and what is a concern, is that the automation that computers afford us allows the bad guys to automate that fraud.

And so as Kevin was talking about, their ability to scan a network -- it's no longer one individual has to take a lengthy amount of time casing a store in order to rob it, checking the security systems, and looking at the doors and windows and the site lines. And that takes a long time per target. Whereas with the automated scanning techniques, they can scan and check for vulnerabilities (internet and network vulnerabilities) on a much vaster scale. And so even though the return might be very few vulnerabilities that are available to exploit, they -- even if it's one out of 1000 or one out of 10,000 -- they can scan so quickly so many nodes that that still returns a usable amount of vulnerabilities.

**Julia Allen:** So we did talk about that, about the scanning techniques, finding the vulnerabilities, taking advantage of them. Would you say -- are there other common methods, other automated or tooling approaches, particular classes of vulnerabilities, that today's organized criminal element are taking advantage of and being used for these high profile breaches like TJX and Heartland, or anything beyond what we've already discussed?

**Cal Waits:** I think the important thing to take away from this is not any specific vulnerability -- or even class of vulnerability, whether that's a SQL injection or a cross-site scripting or a man-in-the-middle attack or anything like that. Because as technology changes, those specific techniques are going to change. As we hopefully get better and incorporate secure coding standards into the applications that we build, unfortunately there will just be other vulnerabilities. And so the idea -- I think the real takeaway here is to look at security from that defense-in-depth and compartmentalization viewpoint.

**Julia Allen:** Yes, I'm really glad to hear you say that, because in a lot of our other research and efforts in the program, we're really moving more to asset-centric protection; protect the host, protect the data, protect whatever the valuable item is, regardless of what's coming at it. And is that what you're saying?

**Cal Waits:** I think it's a very clear way of saying that, yes. Instead of getting bogged down in the details -- although someone needs to be paying attention to the details certainly -- but the mindset itself should be more focused on a broader look and not, "Oh listen, let's spend all of our time protecting this one specific -- whether it's SQL injection, we'll make sure that we aren't vulnerable to any SQL injections ever again." Well there's just going to be something else that you're vulnerable for, and if you spend all of the time and effort putting up one big giant brick wall -- and the bad guy can just walk 100 yards down the road and go around it -- it doesn't do a whole lot of good.
Julia Allen: So you did introduce, you and Kevin both introduced, a little bit about CERT’s Clustered Computing Analysis Platform called C-CAP. But I’d like to use this opportunity to talk a little bit more about that, and what was your motivation for developing it, and how it differs from traditional analysis approaches.

Cal Waits: Right. So I think there’s a couple of avenues that will be of interest here. One, for those that are interested in some of the more technical aspects of a computer investigation, C-CAP is an environment -- an analytic environment or an environment for the analysts to use -- to look at this digital evidence in a way that they couldn’t do with a more traditional computer forensic lab.

And so a little bit of background here. Your standard computer forensics lab is generally populated with computer examiners, each of whom have some very powerful desktop computers that allow them to run these tools, these tools to look at the digital images that they collect during the warrants and the subpoena execution. Well the computer forensic tools, the analysis tools they’re using, generally take up a lot of the resources of these machines. And so they’ll kick off an exam -- whether that’s indexing where it looks through all of the information and creates an index of it on a particular hard drive or image of a hard drive. That can take quite a long time and that just has to run. And it’s difficult for them to do anything else while those tools are running. And so they’ll have one or two of these very powerful machines running. And so you end up with a big backlog of information. Whereas we saw this as a problem that needed to be solved. And so we built C-CAP as a way to allow greater access to a wider pool of examiner resources, so that the examiners have better access to more powerful machines, for less money. But to also allow for collaboration between examiners that may not be in the same office. And thus we built into C-CAP a remote access capability, using two-factor authentication and various other security parameters, so that we can open it up for that collaborative aspect, which has worked out very well for these larger cases.

One of the other problems is this massive amount of information and data and evidence that has to be looked at requires sometimes multiple examiners or it involves people from multiple agencies. And so it has provided an excellent platform to carry that out.

From a business leaders’ perspective, what's interesting about C-CAP and its offshoot -- which we're referring to as C-CAP-light and I'll get to that in a second -- is that often a concern of a business leader when they realize that there has been a breach or a compromise, is that they may fear a lack of -- that if they open up to an investigation by law enforcement, that they will lose control over what may be very sensitive business information. And what C-CAP allows is the central repository and control of that information during the investigation. There's only one copy. It's in the same place that people are accessing it. And it's not walking around, it's not walking around on someone's laptop to be lost somewhere else, it's controlled. And you can have -- depending on the level of sensitivity -- you can raise or lower the level of access controls on that data.

The other aspect that they may fear is during the discovery phase of the legal system, when defense gets access to all of that data -- that was a big issue with the TJX and the Heartland cases. You have to remember these cases, we are talking about tens of millions of credit card information, credit card numbers. We're talking about a great deal of information, of means and access vectors of attack, as well as a lot of command and control data for various machines that were used to compromise other networks. And so this data is very sensitive and needs to be controlled. Well during a discovery phase of a trial, that data is made available to defense
as it should be. But the C-CAP environment -- what we did is we spun off a separate instance of it and called it C-CAP-light, in which we were able to put all this data into, allowed for a much greater level of control of this information during the investigation and the prosecution. And so this information, this business information, was maintained in a central environment, and it didn't -- the ability for it to leak out was greatly controlled during the criminal investigation. And so this was a great way that they could still follow through with the prosecution, at the same time protecting the intellectual property and the company secrets during the analysis and discovery phase.

Julia Allen: So if a business leader wanted to take advantage -- and I don't even know if that option exists for them to take advantage -- of the C-CAP environment, would they work it through their respective law enforcement agency? How would that work?

Cal Waits: Yes, so our role as an FFRDC, we provide support to many federal law enforcement agencies. As well as the technology behind C-CAP is one that we are also trying to transition out into -- to raise the level of practice within the digital forensics world. And so yes, it's possible to request that specifically through law enforcement, during the initial phases of the investigation. As well as if they're interested in building an in-house capability, we are happy to pass on our lessons learned and the environment that we've created as part of our mission to transition that technology.

Julia Allen: Excellent. Well as we come to our close, for both of you, Kevin and Cal, do you have any specific actions that we haven't perhaps already touched on that business leaders can take both to protect themselves from these types of attacks, to defend themselves, and to be more effective at doing investigations if they find themselves in that particular situation? So Cal or Kevin, either one jump in.

Cal Waits: Well I'll jump in. I think one thing to keep in mind is as the level of sophistication of the attacks and the tools used increases, business leaders should recognize that when there are indications -- the same tools that are used by the criminals to identify and exploit these weaknesses, can be used by the companies to identify and harden those weaknesses. So the same techniques that allow for automated scanning of vulnerabilities so that someone could exploit those vulnerabilities can be used by a business to identify and then harden those vulnerabilities. Many of the tools they're using are available to everybody.

The other thing I want to mention is that when an indicator is found of a compromise, that a company should move aggressively to begin that investigation. That a head in the sand sort of mentality is really only going to make the problem worse. And by involving law enforcement early on, they can use techniques to gather the kind of information that will make a prosecution more successful.

Julia Allen: Kevin, is there anything you'd like to add?

Kevin Moore: Yes, just somewhat reiterating Cal's point. But I think there is a tendency for private companies to fear working with law enforcement, right? Because it someone has -- there may be somewhat of a bad connotation to think that they did something wrong. But in most cases it is the attackers have done something sophisticated to access their systems. And working with law enforcement can help to identify the problem and reduce the spread of the problem because it may not be that that company was the first to be attacked. There may be others that are also involved and bringing it to law enforcement can help them work -- can identify and cross-reference between those different cases to see that they may get more information from victim number two than they did from victim number one. But they're able to
bring them both together and bring them collectively, as a case, against the attackers. So I think the private companies sometimes get a little bit worried bringing things forward to law enforcement. But it can be to the benefit of not only to the company but to the investigators working the case as well.

Julia Allen: And Kevin, before I turn it back to Cal, do you have any references or sources that you'd like to point listeners to? Of course, we'll point them to the CERT forensics site and the C-CAP site. But are there other places you would recommend our listeners go to for more information?

Kevin Moore: Well if they're looking for more information on the TJX and Heartland cases, fortunately for them there's been a great deal of news coverage. So a simple Google search should probably give them quite a bit of articles that are out there, through -- Wired magazine has had quite a bit of coverage as well as various other news agencies. And I think just as far as forensics goes, to be actively involved in the developments in the field.

Really, there's all sorts of sites that are available to them; whether it be different forums through Guidance Software or AccessData, they can provide a great deal of information. But in addition, following just information regarding the latest vulnerabilities that are out there, whether it be through the US-CERT website or through various other organizations, they can find vulnerabilities that are identified. Because those can help businesses in protecting their networks and ensuring that they can prevent an attack or at least reduce the likelihood.

Julia Allen: Great. And Cal, other sources you'd point listeners to?

Cal Waits: Yes. If they're interested more about the cases, they were just recently adjudicated. The Department of Justice website has some good write-ups on the results of the investigation as well as the sentencing that took place.

Julia Allen: And Cal, you had mentioned this notion, which I thought was a great idea, of business leaders understanding that the tools that the intruders are using are available to them to use as well. So are there any good tool sites? Or again, is that just poking around with internet searches?

Cal Waits: There are many both open-source and commercial tools, that are available for these -- for checking networks, for doing network assessment, vulnerability assessment. And I think as well as companies that specialize in those actions. I think a simple search will find many of those companies and tools. And I think it's well worth a company's time, if they don't have the in-house capability, is to at least begin the process of taking a critical look at their networks. A lot of what we find actually is that the IT staff of a company may think their networks are in one state. But an objective look at it will reveal things that they hadn't noticed before: configurations that are different from policy; nodes or portions of the network that have been added on over time that don't match the same configurations. And so it's worth having an outside expert take a look.

Kevin Moore: And just to chime in quickly, I think that in regards to the kind of vulnerability scans that Gonzalez and his co-conspirators did in the TJX case in particular, the IT departments can use those same vulnerability scanners to scan through their networks and see where the vulnerabilities are, so that they can make the changes proactively as opposed to reactively.
Julia Allen: Excellent. Well first of all Kevin, let me thank you very, very much for your time and expertise today. Really appreciate it.

Kevin Moore: Oh thank you very much. It was great.

Julia Allen: And Cal, so glad to have you back on the podcast series. And thanks for the great insights from your point of view, and for about C-CAP in particular.

Cal Waits: Thank you for the opportunity.