CONDUCTING INCIDENT POST MORTEMS

By Peter Stephenson

(Originally Published in *Computer Fraud and Security* April 2003)

We were scheduled to discuss back tracing this month but events since I wrote the last column have persuaded me to put that topic on hold briefly in favor of an important, but often overlooked, use of the digital investigative process: incident post mortems. Within the last couple of months we saw yet another massive worm infection on the Internet. Organizations that should have been prepared weren't and the effects on some were, however temporarily, catastrophic. Many of those organizations had suffered under Code Red, Nimda, Love Letter and other global infections.

They weren't ready for those and they weren't ready for SQLSlammer. However, most learned something out of 'Slammer: the ability with past worms to recover as the worm was infecting by isolating damage doesn't always work. 'Slammer simply spread too fast to contain. All generally accepted incident response techniques came up short with 'Slammer. Many organizations wanted to know why. The only way to find out is to conduct a thorough post mortem investigation.

Digital Forensics and the Digital Investigative Process

We tend to think of digital forensics largely in the context of identifying and catching the perpetrator of a digital crime. After we catch the suspect, we use digital forensics to put a case together for prosecution. Many investigators believe that that's all there is. Digital forensics and digital investigations, however, can take either of two directions. They can be focused upon the legal and law enforcement aspects of a digital incident or they can be used to determine the root cause that permitted the incident.

If we examine forensic science in general, we find that it is, at its core, the science of finding out why something failed. It could be a dead body, a collapsed building or a penetrated computing system. When we use a branch of forensic science that is not, explicitly, targeted at drawing that conclusion (such as handwriting analysis, ballistics, etc.) we find, ultimately, that we are dealing with sub branches of a larger science. While I would not want to imply that this is a hard and fast definition, functionally it works. We become interested in ballistics when someone has been shot, for example.

In the case of digital investigation, the "why something failed" approach can be quite pure. In a digital incident or crime the "something" that failed was the countermeasures protecting the victim. By conducting a "system autopsy" we can, in many cases, determine the "cause of death". Of course the metaphor is not perfect – metaphors seldom are – but the idea is clear and the science can be quite well-defined.

That, by the way, is an important distinction. In a digital post mortem we have the opportunity to use the scientific method to arrive at a conclusion. If we slip into pure technology we will find that our results are ambiguous and may not be defensible. Computer forensic practitioners often rely more upon technology than upon science. The application of science to the problem can be an important differentiator between a successful and marginally fruitful investigation. Nordby, Writing in Forensic Science, Introduction to Scientific and Investigative Techniques (pub CRC Press, 2002) tells us that reliable methods of inquiry are the common ground between theoretical and forensic science. He lists the characteristics of such methods:

- Integrity
- Competence
- Defensible technique
- Relevant experience

The use of a structured approach to forensic evidence collection, analysis and management allows us, as practitioners, to support our work based upon Nordby's principles.

Finally, the scientific method demands that we develop theories and then attempt to prove or disprove them. When performing an incident post mortem we develop many hypothetical theories of what happened and then attempt to disprove them by collecting and applying facts. If the facts don't support the theory, we chuck it

Copyright © 2003 Elsevier Advanced Technology

and move on to the next. The process is iterative. New facts may suggest new theories to prove or disprove until the final conclusion is the only one fully supported by fact.

The digital investigative process (DIP) that we have discussed in past columns lends itself nicely to this approach. It also holds us to the rigor demanded by Nordby. With that as preamble, let's move on to process.

The Incident Post Mortem Process

Incident post mortem is not incident response. In fact, one of the driving factors behind conducting an analysis may be the failure of the incident response process. In the case of SQLSlammer, the typical incident response approach failed in a great many cases. An important part of incident response is containment. 'Slammer was nearly impossible to contain if it got a toe-hold within an enterprise.

Early detection was the key since the worm tended to start slowly and, at some point, spread very rapidly – too rapidly at that point to contain. Theoretical calculations of worm-spread within a large enterprise gave the early detection approximately an hour decreasing to less than five minutes for the worm to infect the entire enterprise once it started. In that case the evidence pointed to an early conclusion: early detection mechanisms were not sufficiently in place. The key word in that statement is "pointed". It did not establish, by itself, that the root cause of the infection was lack of early detection. To do a complete post mortem we need more.

Some old mystery stories tell us clearly why taking the first, most obvious, conclusion is not always the best approach. We all have read stories or watched mystery films where the victim appeared to have died of some trauma such as a gunshot. Upon completing the autopsy, we find that, in fact, the victim was poisoned first. In a digital post mortem the obvious answer is not always the right one. More often it is correct but not complete. It is not the whole story as in our mystery story example. That is our first caution. Just because you find an answer doesn't mean you've found the whole answer. Complex problems, it is said, tend to generate complex solutions.

The converse of that is Ocam's Razor: the simplest solution is often the best. That leads to our second caution: don't over-complicate the process. Look, initially, for the simple answers. It is possible that you will find your final conclusions to be a combination of simple underlying problems. Complex, perhaps, but not necessarily complicated. In most of the post mortems I have conducted I have found that a suite of fairly simple remedies would have prevented the problem entirely. In a poorly architected enterprise it is fairly simple to cause havoc with limited resources. It is equally simple to put straightforward countermeasures in place that would have prevented the problem entirely.

The general process for conducting an incident post mortem is:

- Get the lay of the land. Examine network maps, interview key witnesses, learn what appeared to have happened from those who were there and watched it happen.
- Collect evidence. Get every log you can find whether you think it will be useful or not. At this stage you are casting a very wide net. You don't yet know what happened so you don't yet know what to look for. If the incident suggests that imaging some computers is necessary, get them imaged as fast as you can before precious evidence is lost. Contact Internet service providers that may have been in the path and get logs preserved pending subpoenas. In short, as you would in an investigation that you expect to lead to the identification of a suspect, freeze time.
- Collect a set of incident hypotheses. At this point quantity is more important than quality. Don't get silly – the hypothesis that space aliens caused the incident may be a bit far out to take up valuable time proving or disproving.
- Conduct detailed interviews. Gather as much detail about what happened as you can. A good tool for conducting interviews is to prepare, with the help of a knowledgeable person, a timeline of observed events. This timeline can include events as seen by various groups such as network operations, security, users, etc. It should also include any meetings that were held by

Copyright © 2003 Elsevier Advanced Technology

response teams or other involved persons and the purpose and conclusions of those meetings. Include when various involved individuals were notified of the incident and all other information that helps you create a picture of events as they occurred. This will be very difficult because during an incident a certain amount of chaos rules. Do the best you can. Take the timeline and use it as the basis for interviews of all involved parties. Note carefully the discrepancies and, through repeated interviews attempt to resolve them. Remember, in a serious incident cover-ups are common.

- Process your physical (digital) evidence. Use the correlation techniques discussed in earlier columns plus some analysis techniques we will discuss in coming months to reduce your data (there will be huge amounts of it) to information and, ultimately, to knowledge.
- Refine your hypotheses, rejecting those not supported by facts as they emerge. You also will find that as facts emerge they suggest new theories. Don't be shy about considering them.
- When you get down to a couple of likely theories (they may be combinations of several earlier ides) test them rigorously against the facts. Look for counterexamples and alternative explanations that might discredit your explanation. Make sure you haven't missed anything or any interview that could shed additional light on the problem. Use whatever data analysis tools you can to validate the impact of your data upon your final theories.

Use the Digital Forensics Research Work Shop's DIP matrix (see last month's column for an explanation) to ensure that you have followed good digital forensic process and haven't left out any controls. Even though this is not, on its face (or may not be) an investigation that will lead to an individual suspect, maintain chain of custody for all documents, logs, etc.

You never know, at the outset, where investigations will lead or how they will be used. The overarching purpose of an incident post mortem is to generate a strong, provable set of lessons learned and recommend appropriate countermeasures. Most organizations are more concerned with that than they are with catching the bad guy. However, that does not preclude criminal, civil and administrative actions based upon the outcome of the investigation. Be sure that you have followed all of the normal rules of conducting a proper investigation.

Post Mortem Quality

There are many groups and individuals who claim to be able to conduct a post-incident analysis. A true analysis follows digital forensic principles. However, the use of the term "forensic" conjures crooks and witch hunts in the minds of many people, especially those in an organization who may have been negligent in their duties. While gross misconduct should never be tolerated, organizational politics are a fact of life. The golden rule of post-incident analysis is that if you cannot, for whatever reason, perform a full and complete post mortem, wherever the facts may lead, don't bother.

It is unethical to compromise an investigation for political reasons. If law enforcement were conducting an investigation there would be little choice except to cooperate with the investigators. When a non-police organization, internal or external, conducts the investigation you may expect varying degrees of cooperation, stonewalling and outright lies. People often lose their jobs over the results of such investigations. That can subject the organization to wrongful termination suits and such suits may name individuals involved in the investigation.

If you cannot conduct a full and impartial analysis, nobody benefits. The object of the analysis is to uncover root causes that permitted an attack to be successful. That leads to the imposition of appropriate countermeasures. It should not lead to finger pointing. Where groups or individuals have contributed to the vulnerabilities and process failures that allowed the event, training, improved countermeasures, better processes and awareness are the answers. Move heaven and earth to conduct the investigation in that spirit. If you can't, move on. Nobody will gain.

The second issue to contend with is the quality of the investigation from a capability perspective. Skilled incident investigators are masters of the digital forensic process, users of sophisticated data management tools, skilled in

Copyright © 2003 Elsevier Advanced Technology

network analysis and interview techniques, and capable of managing politically sensitive issues. That narrows the field of available investigators significantly.

Because vulnerability or penetration tests have been conducted, or a risk assessment run, doesn't mean that the outcome of a post mortem is a foregone conclusion. There are temporal issues that come into play. For example, in the SQLSlammer incident, many organizations had not patched their SQL servers for business reasons. A vulnerability assessment would show that up and the owners would, simply, seek a waiver on the grounds of business necessity. A risk assessment would show that the servers were unpatched and that might be considered acceptable risk.

Unfortunately, a post mortem is reactive in nature. All of the waivers and acceptable risks have resulted in catastrophe. Now the investigator needs to pick up the pieces and find what happened. A skilled investigator will do exactly that, but will do it in the context of business requirements. He or she always will be looking for ways that the event could have been prevented without placing undue hardship on the business processes of the organization. That, too, requires a special set of skills.

Finally, expect to deploy an investigative team. No one person has all the skills. My team consists of seven people:

- A quality manager. This person manages all evidence, chain of custody, ensures that there are copies of the investigators' notes in the record, schedules interviews, etc.
- Network specialists. I have two. One specializes in TCP/IP networks the other in Microsoft and other operating system specific networks. Both specialize in firewalls and intrusion detection systems as well.
- Code specialist. This person analyses rogue code involved in the incident and is a specialist on operating systems and their behavior. He also hacks special analysis tools and scripts if we need them on site.
- Business process specialists. I have two. They specialize in standards such as BS7799/ISO17799, banking regulations, etc. Their job is to uncover process failures, especially those that are counter to regulatory requirements if any. They also attempt to calculate the cost of the incident to the organization.
- Team leader. Specializes in the investigative process, forensics, data reduction and analysis and investigation management.

Organizations like post mortems to be completed rapidly and correctly. These engagements, whether by outside consultants or inside staff (most organizations don't have qualified internal staff to conduct a proper post mortem, however) are very expensive and should be reserved for only the most catastrophic occurrences. A recent analysis determined that the client lost in the tens of millions of dollars to SQLSlammer, for example, and 'Slammer was the third worm that had affected seriously the organization. Clearly, a detailed post mortem, regardless of cost, was in order.

Incident post mortems are expensive, difficult and require highly skilled practitioners to perform. In order to get full benefit of that investment, they must be conducted thoroughly and openly with positive approaches to the results. The results are never pleasant, of course. Catastrophes never are, and if there was no catastrophe there would be no need for the post-incident analysis.

Smaller post-incident analyses are always appropriate for any digital incident, of course, and such analyses are rarely as complex or expensive as that described here. They can, generally, be conducted internally and will have nowhere near the potential impact of a major post mortem. However, if the time comes to respond to a catastrophic event with a full-blown post-incident analysis, do it right, do it positively and do it quickly.

Copyright © 2003 Elsevier Advanced Technology