White Paper

Emergency Incident Response: 10 Common Mistakes of Incident Responders

intel Security

This white paper was written by:
Michael G. Spohn
Principal Consultant
McAfee® Foundstone®
Professional Services
Incident Response and
Forensic Practice

Table of Contents

Introduction

As a senior investigator on the McAfee® Foundstone® incident response and forensic team—part of the Intel® Security product and service offering—I have handled my share of incidents. In the last few years I have been on site at more than 100 organizations helping them deal with serious security breaches. These engagements range from common malware infestations, employee misconduct incidents, and even high-profile breaches by groups such as Anonymous and LulzSec. Most of these incidents involve partial or total business disruption, the theft of intellectual property, trade secrets, financial information, and/or sensitive personal information.

In every one of these engagements, I have learned something I did not know before. This is what makes security breach investigations so exciting for me. Over time, I began to recognize patterns of behavior of incident response teams I worked with and, in almost all cases, these incident responders were incapable of dealing with the threats they were facing in an efficient and repeatable manner. Of course. If this were not the case, why would they need a company like ours to respond?

In this brief white paper, I summarize the top 10 incident response mistakes I see in the field. My purpose is to highlight these issues so you can review your incident response practices and determine whether you suffer from these shortcomings.

Engagement Scenario

In a typical engagement, a client will call us and request immediate assistance in helping contain a security breach, and, in almost all cases, we have an investigator on the customer site within 24 hours.

When it comes to successful incident response practices, I have found the following to be consistently true:

- The size of the organization is not relevant. In larger organizations it may take longer to contain an incident, but the process is the same.
- The industry is not relevant. The specifics of handling a security breach are not dependent on what the client does. Sure, there are privacy and regulatory issues specific to certain industries, but we handle all incidents according to the strictest standards. So should you.
- The crisis management skills of a client vary. For example, federal government agencies generally have more mature crisis-handling capabilities than a mid-sized law firm. Even so, I have found the difference is not relevant enough to make a big difference.
- The technical skills of a client vary. This does make a difference. Clients that have a high level of technical skills, particularly in the area of network management, are generally more successful in efficient containment of security incidents.
- All organizations exhibit a consistent pattern of behavior under stress.

The point of this list is to convince you that a mature and disciplined approach to incident response will work in your organization.

The Top 10 Mistakes

1: Nobody is in charge
I cannot emphasize how important it is to have one person assigned to manage an incident response undertaking. Over the last decade, organizations have moved to more decentralized management structures. Lines of authority are soft. Geographic boundaries have disappeared.

The person assigned as incident manager has the ultimate responsibility for containment of an incident. I am sometimes asked to serve in this role, but I prefer that role to be filled by an insider. A senior manager or director is usually the best choice. C-level executives rarely serve in this role. Whoever is assigned this role does not have to have advanced technical skills. Communication, organization, and delegations skills are more important.

2: Failure to establish a command center
It is quite common for organizations to try to manage serious incidents using conference calls, mobile phones, and email. Trust me—this does not work. It is critically important that a single conference room or office be established as a command center.

The chosen location should be large enough to handle a dozen people, have large whiteboards or post-it-note easels, a conference/speaker phone, and be securable. Access to the command center should be limited to those individuals responsible for managing the incident. The command center will serve as a central hub for all communications, containment planning, task delegation, and status updates.

3: Failure to find and know the enemy
If you ask our clients what they value most from our emergency incident response services, they will usually say: crisis management skills and threat management. Threat management is a skill that requires the ability to find a threat source and understand its modus operandi (MO). We call it 'know the enemy.' This effort is not particularly difficult, but most clients are not very good at it.

The 'enemy' varies depending on the incident type. The important thing is to identify the threat and clearly understand how it operates. For example, in a serious malware outbreak, our process for finding and knowing the enemy consists of the following steps:

- Identify the attack vector.
- Perform live forensic analysis.
- Isolate hosts and obtain samples.
- Profile the malware and understand how it communicates.
- Submit malware samples to the antivirus vendor.
- Leverage enterprise antivirus tools.

Trust me—you cannot create an effective incident containment strategy unless you understand your enemy.

4: Failure to create a containment plan

When I arrive on site at a 'hot' incident, I am always intrigued by the elevated level of chaos. Most organizations do not have an established and documented crisis management plan in place. So, we have to do it for them. Usually within the first four hours of battling a security breach, I produce a concise (one- to two-page) incident containment strategy document. This containment plan is a critical component of the McAfee Foundstone incident response methodology. We always create one.

In short, the methodology consists of the following steps:

- Determine the attack vector and scope of incident.
- Know the enemy—identify their tools and tactics.
- Collaboratively design a containment strategy and document it.
- Create a task list based on containment plan.
- Delegate and monitor tasks until containment is achieved.

5: Failure to document

I admit it. I am an old-timer from the old school that still uses investigative notebooks. Things have changed. Young people today have never known a world without electronics. The use of text messaging and email has changed the meaning of documentation. This has caused many incident responders to forget the importance of good documentation.

You cannot rely on your help desk ticketing system to document your incident. We encourage all responders to keep a notebook with them at all times and document their actions. All events and delegated tasks should be documented and kept in a centralized and secure location.

6: Failure to create an incident timeline

In my view, the creation of an incident timeline is one of the most important tasks when battling an incident. Essentially, this means you must document events and sort them by date/time from oldest to newest. Your list does not have to be fancy—just complete and accurate.

A detailed incident timeline provides you an investigative 'compass' to direct your containment strategy. It also adds clarity to complex investigations and helps you focus on the big picture. Finally, it creates a terrific briefing tool for senior leaders.

7: Confusing containment with remediation

A very common incident response mistake organizations make is to confuse containment with remediation. To be effective, you must focus on containment first and deal with remediation efforts later. Why? Containment focuses on stopping a threat, whereas remediation focuses on fixing vulnerabilities. Think of an emergency incident response as a building fire. You want to spend all your initial efforts on dousing the fire. Repairing the roof comes later.

Emergency incident response is a containment process. It is critically important that everyone on your incident response team understands the importance of containment first. Any task that is not critical to your containment efforts should be set aside for later.

8: Failure to monitor and secure network perimeters
It amazes me how many organizations have not implemented network monitoring technology. Without the ability to know what kind of traffic is moving across your networks, you are powerless to defend against network-based threats. I cannot emphasize enough the importance of securing your network perimeters and monitoring outbound network traffic.

Why outbound traffic? Because your enemy must transport your sensitive data from your network to theirs. During an incident involving a security breach, we always focus on securing the network perimeter and then working inward. Securing the perimeter will handcuff the enemy's ability to communicate. Once this is done, you can then work inward from the perimeter finding and destroying their tools.

9: Inadequate logging
Plain and simple, the vast majority of organizations we deal with do not have adequate logging mechanisms in place. For a reason that escapes me, the resistance to effective logging is still alive and well. We must change this mindset. Logs are the most effective source of evidence in most incidents. The most valuable logs in my experience are network perimeter logs.

Effective incident response teams must have quick access to log files including, but not limited to:

- Syslogs or other centralized logs.
- Firewall logs, IDS/IPS.
- Web proxy logs.
- Microsoft Windows event logs.
- VPN logs.
- DHCP logs.
- DNS logs.
- Microsoft Active Directory (AD) logs.
- Enterprise AD logs.

10: Orphaned enterprise antivirus systems
This mistake may surprise you. There is a strong feeling in the security community that modern enterprise antivirus systems are no longer effective against today's sophisticated and polymorphic threats. I concede we are losing the battle on this front—but your enterprise antivirus system is still a key component of your defense arsenal. In fact, in most malware or APT incidents I have handled in the last four years, an enterprise antivirus system was used to counter the threat.

Organizations get in trouble when they fail to leverage their antivirus tools. Common mistakes in this area include:

- Failure to monitor and/or enforce antivirus compliance.
- Outdated agents.
- Outdated signature files (.DATs).
- Failure to provide daily oversight of antivirus systems.
- Failure to created automated event alerts.
- Failure to monitor antivirus vendor alerts.

Summary

There you have it. The top 10 most common mistakes I see incident responders make. As you can see, none of these mistakes are difficult to correct. In fact, your organization can use this list as a gauge of the effectiveness of your current incident response practices. At McAfee Foundstone, we are passionate about security. We strive to help organizations increase their security posture. This is best accomplished by proactive efforts. We encourage you to spend time ensuring your incident response plans are current and effective.

About the Author

Michael Spohn is a principal security consultant at McAfee Foundstone, where he provides incident response (IR) and digital forensic services to clients. His duties include creating IR management programs, analyzing and testing existing IR plans, conducting forensic investigations, and providing IR and forensic training. He is also a member of the McAfee Foundstone Emergency IR Team, which provides emergency services to clients when an elevated security breach occurs.

About McAfee Foundstone Professional Services

McAfee Foundstone Professional Services, a division of McAfee, part of Intel Security, offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, McAfee Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.
http://www.mcafee.com/us/services/mcafee-foundstone-practice.aspx

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com