



AccessData Group

# The Importance of Integrating Host and Network Forensics

White Paper

TABLE OF CONTENTS

Introduction .....1

Traditional Incident Response (IR).....1

Network-based Incident Response .....2

Host-based Incident Response .....2

Using Each IR Technique to Complement the Other .....3

Tool Integration .....3

Conclusion .....4

## Introduction

Historically, the disciplines of host-based and network-based incident response have been separated by very separate areas of operation with little or no collaboration between those who focus on the network and those who specialize in host analysis. The gulf between these two disciplines can be attributed to number of reasons, including different technical knowledge requirements, differing procedures and processes, the administrative/political realities faced by every organization, and finally, the tool sets involved.

This unfortunate disparity has resulted in inefficiencies in the way organizations secure their networks. To put it bluntly, we are getting our heads handed to us by targeted attacks originating from brilliant children. With increased cyber attack and espionage breaches, increasingly savvy perpetrators, as well as a growing number of sophisticated exploits, this will only get worse if we sit on our collective hands. This lack of response capability is a deep rooted problem that must be acknowledged and must be addressed by corporations and government entities alike.

We have to get smarter, better, faster.

## Traditional Incident Response (IR)

To get where we need to be, we need to have an understanding of where we are at now. We can do this by examining the traditional process of IR.

**In the traditional methodology, an incident can be identified by many different sources, including the following:**

1. Antivirus alerts (AV)
2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
3. Firewall (FW) and/or Security Information Management Systems (SIMS) Logs
4. Trouble Tickets (slow or erratic performance)
5. Unexplained or Unauthorized Account Modifications
6. Denial of Service User Reports (DoS)

A quick glance at this list reveals that these sources can be split into two broad categories—network-based and host-based. The AV, IPS, Trouble Ticket, Account Modification and DoS all source from the host. The IDS, FW and SIMS all have the network as their source, and therein lies our problem.

For our network sources, the network IR team is tasked with response and investigation. For the host-based sources, a completely separate team, with correspondingly separate tool kits, skills and procedures goes into action. Rarely, if at all, do the two teams intersect.

This lack of integration has resulted in the failure to completely manage most incidents. The ball is dropped as it is passed between teams. This is almost unavoidable with current methodologies simply because both host- and network-based IR each have their own strengths and weaknesses.

## Network-based Incident Response

### Strengths

Sophisticated perpetrators are well aware of the artifacts that result from host-level exploitation. These artifacts are found in memory (volatile data), page or swap files, hard drives, USB drives, CDs/DVDs and other static media. Just as easily as these artifacts are detected, they can be obscured to a level of practical uselessness or even be completely erased. The techniques are well known—any simple Google search for “anti-forensics” will yield a treasure trove of easily used scripts and techniques that can be followed with trivial effort. Even the most unsophisticated attacker can make finding and evaluating host-level artifacts difficult if not impossible. All the attacker needs to do is “own” the attacked host to deploy and use these methods.

This is precisely the strength of network-based IR. The attacker can never precisely know where the network-based data is being gathered (“sniffed”) or where it is being stored. As such, the attacker is blind to this data. It is inviolate.

### Weaknesses

There are two primary weaknesses to network-based IR. The first is that it is easily “spoofed”, (i.e. faked or altered) to appear to be something it is not. Unless there are very strict source tagging efforts made on the packet streams, it is nearly impossible to say with certainty exactly where something came from and when it arrived.

The second weakness is the sheer amount of data involved. Huge amounts of packets traverse even the most sparsely populated networks. In order to monitor this data it is often mandatory that some sort of tuning or filtering be implemented on the mass sea of data. Tuning and tweaking poses its own set of problems, with tuning down too low missing important data and tuning too widely resulting in still more data to be assimilated.

## Host-based Incident Response

### Strengths

Host-based IR is as solid as a rock—provided the data is still there. Technology is very mature when it comes to finding, filtering, isolating and reporting on deleted files, swap space, paging artifacts and otherwise tampered or altered files. Large volumes of canned “digital fingerprints” (hashes) are published that provide irrefutable evidence that a file is what it is. There is little fooling it if the data is actually there.

Host-based IR is also rapidly maturing in the arena of resident memory analysis (RAM). Processes that are hidden in memory, hooked or injected dlls are also easily detected. Examination of the host memory reveals these hidden processes readily.

### Weaknesses

At times, the offending artifact is completely scrubbed. The scrubbing action can be as simple as a disk defragmentation (rarely completely effective) or as complex as a Federal Information Processing Standard (FIPS) multiple overwrite of the disk space.

Incriminating artifacts can also be encrypted. Encryption has now progressed to the level that simple brute force (trying many possible key combinations) can take longer than the projected age of the universe, even with ALL of the computers in existence today working simultaneously. This is often an insurmountable problem. You may have the data, but it is encrypted and so it is useless to your investigation.

## Using Each IR Technique to Complement the Other

Just as in Combined Arms tactics, where infantry covers the weakness of artillery, and cavalry covers the weakness of infantry, we can use the same relative technique to utilize the strengths of each IR strategy to complement and cover the weaknesses of the other. This is best explained by following the path of one of the most threatening network exploitation techniques found in the wild— the EPROM rootkit.

### EPROM Rootkit Example

A rootkit is a specific type of malware that, once installed, hides itself, other processes and specific sectors of the hard disk, and it typically opens network sockets for backdoor connections from the network. In the case of the EPROM rootkit, this malware is installed within the Erasable Programmable Read-Only Memory of a peripheral device in the target computer. This peripheral device is most commonly a network interface card or a sound card. The EPROM rootkit has also been found in the wild installed within the memory of a video card.

What makes this particular rootkit so dangerous is that it survives a rebuild of the infected machine. Since its code resides within the peripheral device's memory, a complete wipe of the Operating System (OS) is ineffective for remediation. As soon as the new OS is installed, the OS calls the drivers for the peripheral, the EPROM serves up the rootkit into RAM and the nefarious, hidden process is active again, opening hidden connections to the outside. Since it only resides within memory (RAM) during the active running of the infected machine, it is extremely hard to detect. Since rootkits themselves are not exploits, they require a vector to infect the target host. This is typically the first opportunity to detect this malicious action.

In our example, the Network IR team detects the exploit vector of the rootkit. For example, a Microsoft exploit, MS08-067, Windows Server Service Code Execution, is launched against one of the internet-facing servers. The IDS detects the exploit. Or perhaps not...

The IDS may not have the latest signature update, the signature may not even exist yet (as in a zero-day exploit) or the IDS has been tuned down and this signature is not active. We MUST ensure that all network traffic is recorded and stored for future playback, regardless of whether we know it is malicious or not at the time of passage.

Even if we detect it in transit on the wire, how do we know if the exploit was successful and the target host is exploited? Quite simply, we do not until we examine the target host.

Now the host IR team gets involved. This team examines the target host using a variety of network tools. They may have open source rootkit detectors, trusted binary boot disks or use OS native tools to perform their examination. If they do not use rootkit detection technology or examine volatile memory before powering the host down, they will miss the infection. If the infection rootkit hooks its backdoor socket listener to an existing, valid port, such as http (web), even a remote port scan will not detect it.

By following this simple example, we can see the numerous opportunities for the ball to be dropped, tools to fail, miscommunication to between teams, delays and latency.

So, how can we do this better?

## Tool Integration

If we select a set of tools that provide BOTH host-level and network-level IR functionality, we eliminate all of the points of failure involved in "passing the ball" from one team to the other. We also eliminate the latency involved in these hand-offs. By including remediation within the integrated tool set we also allow for a more immediate

remediation of the infection. We can also compress training and thus reduce costs. This is a genuine win-win strategy.

### **Requirements for our Integrated Tool Set**

1. Must record all network traffic
2. Traffic must be capable of being played back
3. Payloads must be extractable (carved out) into native format
4. Carved network payloads must be integrated into the host-level examination tool
5. Host-level examination must be capable of live memory analysis
6. Remote process kill and parent file must be able to be wiped
7. All evidentiary artifacts must be exportable in a forensically sound manner (complete and unaltered) and sharable with other tool elements

## **Conclusion**

It is against this list of requirements and with the objective of solving this exact problem that AccessData has integrated its host- (AD Enterprise) and network- (SilentRunner Sentinel) based forensic technologies into a single incident response solution. A single investigator can now utilize these tools together to tackle the most elusive and complex incident response problems.

Furthermore, the Incident Response solution enables organizations to integrate their incident response and computer forensic processes to streamline their investigations and significantly reduce response and remediation time. Using a single investigative solution allows an organization to consolidate its technology training requirements and to be more effective without having to hire additional resources. Ultimately, the integration of network-based and host-based forensics will save an organization time and money, while significantly reducing risk.

### **About AccessData**

AccessData has pioneered digital investigations for more than twenty years, providing the technology and training that empower law enforcement, government agencies and corporations to perform thorough computer investigations of any kind with speed and efficiency. Recognized throughout the world as an industry leader, AccessData delivers state-of-the-art computer forensic, network forensic, password cracking and decryption solutions. Its Forensic Toolkit® and network-enabled enterprise solutions allow organizations to preview, search for, forensically preserve, process and analyze electronic evidence. AccessData's solutions address criminal and internal investigations, incident response, eDiscovery and information assurance. In addition, AccessData is a leading provider of digital forensics training and certification with its much sought after AccessData Certified Examiner® (ACE®) program. For more information on AccessData visit [www.accessdata.com](http://www.accessdata.com).