First Response: Guide

Overview

This document is for system administrators or owners who believe they have discovered an information security incident — a compromised computer or unauthorized access to digital data.

Critical steps are outlined at First Response Checklist, with more explanation following.

When you discover an incident

Discovering a compromised host can be stressful but first and foremost, remember not to panic: The Office of the CISO is here to help guide you through the incident response process and determine whether sensitive data was accessed. In order to do so, we will need you to take some important first steps.

Throughout the entirety of this process, remember to **take notes.** Write down everything you observed and what you did, with timestamps. Here are some examples of what to record:

- Who reported the incident, and exactly what time?
- How was it discovered?
- If you did your own investigation, exactly what did you do? Include: logged into where at what time, ran what commands, etc, as best you can recall. (Knowing this can help us sort out what was you and what was the attacker.)
- If you took any remedial action, what did you do and what time? Reset account passwords? Shut down computers? Times may be critical.
- For desktops, who is the primary user? Are there others who have logged into it? Have their passwords been changed?
- What other computers or servers does the affected one normally talk to? File servers, web servers, database servers?
- Write down IP addresses of the affected device, and other servers that it talks to, if you know them. The sooner we have that information, the sooner we can start looking for network evidence.
- Any other information that might be useful, particularly anything that has changed recently. (Has someone begun working remotely? Has any related hardware or software changed recently? Seemingly nefarious activity may occasionally be traced to something as simple as a change in behavior or a new mouse.)

If you interacted with affected devices in any way, it may be critical for us to know what you did and when. The reason is that we're frequently asked to determine with high confidence what an adversary did and what data they touched. It can sometimes be difficult or impossible to distinguish between your actions and the adversary's, especially if you have interacted with the device since discovery of the incident.

It is equally important to document only information that has been substantiated. No speculation or inference should be included in your notes; only actions and observations.

Important steps

We understand that circumstances vary and taking the following steps may not always be possible. These are best practices; if you need to modify them, remember to make a note of what you have done.

1. **Disconnect the device from the network**
    - **Disable both wired and wireless network access.**

Disconnecting the device from the network will help prevent further spread of any malware or malicious activity from a compromised device. Remember that if your device has both wired and wireless capabilities, both should be disabled.

If the host is part of a critical service, it will be up to you and the service owner to determine whether or not it can be taken offline. If malware is involved, it is important to isolate the device as quickly as possible in order to prevent other systems from being infected.

2. **Preserve state**
    - **Do not turn off the computer, log off, or use the computer.**

Do not make any changes to the state of the computer such as powering it down, logging off, or otherwise using the computer. Turning the power off could destroy key pieces of forensic evidence that will later be needed to help determine root cause and the full extent of the compromise.

If we have to do a forensic analysis, it might be really important to know, for example, that the last time a file was accessed was before the initial compromise occurred. If you've copied, moved, restored, deleted, or otherwise touched that data, then we may not know whether it was you or the adversary that did the touching, and that reduces our confidence that it wasn't compromised.

3. **Preserve evidence**
    - **If you do any centralized logging, immediately preserve all the logs you have from the log server. *Do not attempt to collect logs directly from possibly compromised devices, or from other affected devices, until you talk with us.***
    - **Identify all systems, departments, and people that connect to the affected system.**
    - **Leave all possibly affected computers or devices running and untouched, but isolate them if possible. ("Step 1: Disconnect the device from the network" should be enough to accomplish this task.)**

It's nearly universal that, at the very least, we're going to need to examine logs from every system that might be affected, but there are caveats.

In the best case, you're sending all the right logs to a central server, so you can easily preserve them without having to even log into the affected systems. It is always safe to do this, and this is one of the few things we'd encourage you do to even before you talk with us.

If you don't have central logging, then it's a little trickier. You'll have to collect logs from individual hosts, and this may be less reliable, not only because some actors will delete or

modify logs, but also because it risks trampling evidence if we end up doing a forensic analysis. That still might be a good trade off, but it's not always clear cut. For those reasons, if you don't have central logs, it's best to contact us before preserving them directly from affected hosts.

Also, note that "affected hosts" doesn't just mean the one that is compromised; it means any host on which there may be evidence. For example, a lot of workstations connect to file servers, and a compromised workstation may have accessed files on the file server, even if the file server itself is not compromised. If your logging on the file server is sufficiently verbose, that may be where we find our best evidence. In extreme cases, we may even be able to answer the question "was this data compromised?" by doing disk forensics on the file server, even if it was not compromised, and that kind of evidence is easily trampled by disk accesses.

Finally, if you're not very careful how you interact with untrusted computers, it may be trivial for an attacker who has compromised a computer to steal the credentials of the first administrator who logs in to investigate. Don't do it! (And if you already did it, change your password immediately.) Sometimes, in fact, this is precisely what the attacker wants and expects; they may compromise a workstation, then just wait for a domain administrator to log in, and steal their credentials to gain new privileges. You don't want that to happen.

If you have already shut down or disconnected computers or taken other remedial actions, that's ok; just leave them as they are and do nothing else to them. Most importantly, record exactly what you did and exactly what time, as best you can remember. (See the previous section.)

To recap: talk to us before doing anything. However, one exception to the "don't touch anything" rule is that it's nearly always ok and desirable to preserve logs from a central logging server, as soon as you think there might be a compromise (unless, of course, the central logging server itself is believed to be compromised).

4. **Contact us**
    - **It is critical to ensure that all potential information security incidents are reported to the correct delegated authority.**
    - **Call the Office of the CISO at 206-685-0116 with a brief summary and a phone number for a technical person with knowledge of your computing environment.**
    - **We encourage the use of the phone, not email, to communicate sensitive details.**
    - **If you get voicemail, leave a detailed message and then email us to let us know.**

Depending on the type of data involved in the incident, there may be one or more delegated authorities to whom the incident needs to be reported. The Office of the CISO can help assist you in determining which delegated authority you need to work with or you can review Administrative Policy Statement 2.5: Information Security and Privacy: Incident Reporting and Management (https://www.washington.edu/admin/rules/policies/APS/02.05.html).

Even if the Office of the CISO is not the delegated authority for the type of information involved in the incident, we may still be involved from a forensics perspective. We would ideally like to get a technical person from your group in contact with an analyst in our office as quickly as possible. Delay can affect our ability to understand what happened and respond effectively.

We also have threat intelligence analysts who have insight into current attack trends which can help guide our response and help us know what to look for. Again, the best course of action may be situational and fluid, so getting technical heads together as quickly as possible helps a lot.

When reporting an incident, we encourage the use of the telephone over email to convey sensitive information. Also, limit information sharing to only those individuals directly involved in the incident management process.

Other things to consider

Do not contact or retaliate against the individual(s) who may have caused the event/incident.

- **Under no circumstances should you ever reply to or contact individuals who you think may have been behind a malicious attack.**
- **Under no circumstances should you ever take action or retaliate against individuals.**

First and most importantly, attribution (the process of determining who is responsible for an attack) is not nearly as easy or straightforward as some people believe. Attackers can and do take a number of measures to implicate others in a crime, either to avoid accountability or to instigate conflict with their own adversaries.

Any contact with, or action against, the attacker must be left to law enforcement. For any UW employee or representative to do so may not only be counterproductive by increasing risks of all types, but may in some cases be a crime. It is absolutely critical to not do this.

Do not conduct your own forensic analysis

- **Never attempt to conduct your own forensic analysis on any potentially affected computer or device until you have consulted with us.**

Forensic analysis itself involves risk. Evidence is easily corrupted if not handled correctly, and incorrect or premature conclusions may have unforeseen and damaging consequences. It is critical to understand the process of preserving evidence and correctly scoping and conducting an investigation, and what will be done with the results of the investigation.

If you have staff trained in forensics who understand the process and risks, it may be fine for them to assist or conduct additional analysis after consultation with us; however, this should never be attempted at the outset. Preserving evidence is time-critical, but analysis can usually wait until enough facts are understood to scope the work appropriately.

Why are we asking for all of this?

In many cases, we are dealing not with black-and-white answers, but with degrees of confidence. Evidence is the key to increasing the confidence level of our findings, and that usually means:

1. Logging as much as possible of the right kind of data before an incident occurs (a topic for a different document), and
2. Preserving as much evidence as possible when an incident occurs. What you do immediately after discovering an incident can have a huge impact on the confidence level of our analysis.

After an incident, while we're in reactive mode, the best way to minimize the impact is to collect quality evidence that can help us determine with high confidence what did and did not happen.

We hope these few steps can help further that goal.