Deploying to an Already Infected Environment

Background

Cyber Crucible customer deployments routinely result in discovery of previously unknown infections. Networks are normally not infection-free, even if existing cybersecurity defensive tools have given the all-clear.

A ransomware attack provides a highly visible point of demarcation, or, pivotal point, for a company to measure how often hackers successfully re-attack, and how successful they are.

- Open Source reporting and threat intelligence reveals a re-attack rate of non-Cyber Crucible customers of around 80%.
- Cyber Crucible observed around 10% of endpoints have at least one identity theft attempt, such as passwords, keys, or tokens, per 90 day period.
- Cyber Crucible observes attackers attempting to re-gain a foothold in an environment approximately monthly.

From an incident response or forensic standpoint, Cyber Crucible is an excellent tool to regain control of the network. Especially for victims of attack, we suspect that the attackers are maintaining visibility to the victims' state of recovery and financial health, to better time when to strike again.

What Happens Immediately Upon Install

Cyber Crucible automatically begins suspending running programs that are observed to be behaving maliciously.

Roll-out of Cyber Crucible product can result in multiple programs across multiple machines being suspended as the environment is cleaned up.

At times, a partial roll-out of Cyber Crucible can result in the hacker attempting to regain control through the machines that do not have Cyber Crucible protection.

For example, Cyber Crucible was once installed on just a portion of the desktops, of a recent data breach victim. The hackers attempted to uninstall Cyber Crucible by connecting from the unprotected machines, then eventually started shutting the protected machines off.

What Happens to Dormant Malware, Waiting for Future Tasking?

Malware that is not taking action on behalf of attackers, is triggered after the malware starts to access data.

Let’s run through a scenario:

Two machines have malware on them. Let’s call them Machine A, and Machine B.

Both samples of malware are currently undetectable by your favorite security tools.

Machine A’s malware does nothing, but waits for instructions. Cyber Crucible does not detect the malware. The malware is also not yet detectable by other security tools.

Machine B’s malware being attempting to access data or identity data. Immediately after a successful attack, the most common behaviors we see, of attackers tasking their malware, is to ensure they have fresh identity data such as passwords or tokens, and to enumerate new data. So, part, “get the new passwords after the administrators reset passwords”, and, part, “keep tabs to look for new data”.

On Machine B, Cyber Crucible immediately suspends the application.

After anywhere from a month to a year, Machine A’s malware is caught after enough victims have reported the malware to security vendor databases. The more disciplined the attackers are in the distribution of that sample, the longer that particular malware will go undetected.

Machine B’s malware has been neutralized, frozen in place.

Machine A’s malware is trapped. The second (well, 100 milliseconds) it tries to access any data or identity information, Machine A’s malware is suspended. The client is protected, even though the malware exists for days, up to years, without the malware being detected by other tools.

Additional Details - Reboots Can Be Valuable

Some of our analytics are most accurate when the lifecycle of the process is able to be tracked from start of application to the present state.

Rebooting a machine after install can be advantageous.

Programs already running prior to install will not have full analytical inspection from Cyber Crucible. Rebooting forces those programs to re-start, thus providing full inspection to all programs.

Revision #4
Created 2026-05-18 20:27:39 UTC by Dennis Underwood
Updated 2026-07-20 19:21:51 UTC by Dennis Underwood