How We Plan to Respond: A Facilitated Discussion Using Scenario

Bradford J. Willke
Jason Rafail

19 September 2007

Software Engineering Institute | Carnegie Mellon

The Problem - Part 1

A bad actor (designated BG1) from an unknown country has compromised a computer system (designated CnC) in Country “A” to act as a command and control point for their malware.

The same bad actor (BG1) has, over a period of months, infected tens of thousands of computers around Europe with malware. The characteristics of the malware that we know to be true are as follows:

- The malware contacts another computer via the Internet once per hour with encoded/encrypted traffic.
- Computer users (corporate, government, academic, and home users) have reported to CSIRTs (via phone and email) that machines use dial-up to the Internet OR have been shut down (for periods over 2 hours) and rebooted… can no longer connect to the Internet.
- The virus payload is unknown, but it is assumed to corrupt files associated with the TCP/IP stack and network configurations.

For Discussion of Part 1

1. Is this a multinational problem? For whom is this a problem?
2. Where would this fall on your internal “metrics” for incident severity and urgency? How big of a problem is this? What is your threshold?
3. What steps would you take to investigate, triage, and respond to the problem, if any?
4. What would you do, if anything, to coordinate the problem throughout the European community? Throughout the world CSIRT community?

The Problem - Update 1

Another set of bad actors (BG2) have purchased time on a large, distributed botnet, and plan to focus a denial-of-service attack against CnC.

These bad actors have sent messages to national governments, coordinating councils, corporations, and academic institutions in Europe asking for money not to attack the CnC computer.

For Discussion of Update 1

1. *Is this now a multinational problem? For whom is this a problem?*
2. *Has this changed the value of your internal “metrics” for incident severity and urgency? How big of a problem is this? What is your threshold?*
3. *Are there new steps you would take to investigate, triage, and respond to the problem, if any, beyond the initial steps taken?*
4. *What would you do, if anything, to coordinate the problem throughout the European community? Throughout the world CSIRT community?*
5. As the technical experts, what would you recommend to your national governments, corporations, and academic institutions? Do you recommend they pay the ‘ransom’ demand?
6. What actions do you recommend for home users and small businesses?

The Problem - Update 2

Companies have started to report more instances of the malware.

Government agencies have started to hear reports that the malware is showing up on process control system and supervisory control and data acquisition (SCADA) networks, in manufacturing, water treatment and supply, electrical power, and air transportation sectors.

Anti-virus companies have started working on the problem, but do not have a solution. They recommend that users “NOT Quarantine” or attempt to remove the malware.

For Discussion of Update 2

1. Is this now a multinational problem? For whom is this a problem?
2. Has this changed the value of your internal “metrics” for incident severity and urgency? How big of a problem is this? What is your threshold?
3. Are there new steps you would take to investigate, triage, and respond to the problem, if any, beyond the initial steps taken?
4. What would you do, if anything, to coordinate the problem throughout the European community? Throughout the world CSIRT community?
5. As the technical experts, what would you recommend to your national governments, corporations, and academic institutions? Do you recommend they pay the ‘ransom’ demand now? Would you ever recommend this?
6. What actions do you recommend for home users and small businesses?
7. What will the distribution method of patches and anti-virus signature, given the self-inflicted denial of service is likely if that the infected systems are removed from the Internet?

Scenario Debriefing

What did we do well / good / efficiently?

What did we do poorly / inefficiently?

How likely are our actions to be effective?

How could we have done this more efficiently?

What tools, resources, personnel, and capabilities did we use?

Was there a logical process to the way we responded?

- Could we repeat the same steps in our response?
- Could we have done some of the steps in parallel?

Was there a critical decision path?

Who made the decision (for CSIRT, for government, for corporations)?

Who should have made the decision?

Check: Did We Identify Requirements to Do this Efficiently and Effectively?

Requirements:

- Common risk framework (risks based on the potential negatives impacts to critical information infrastructures caused by threats and vulnerabilities)
  - Common or comparable definitions and risk articulation
  - Valuation of the CII
  - Common understanding of negative impact and areas of impact (economy, psychology, safety, …)
- Understand how mature your CII program is, what goals have been met, and what capabilities exist
- Understand ‘trusted’ sources of information and mutual capabilities/functions