Cyber Response Exercise – April 2021

Date: Saturday, 24 April 2021   *Mission Number:* 21-T-1181

Time: 9:00 AM   *Exercise Title:*   Cyber Spring

Exercise Scenario:

Malicious cyber actors have developed a computer worm which has been dispersed widely via the Internet and has escaped early detection. This worm is a zero day exploit targeting Windows operating system computers and is set to activate on Earth Day.

Thursday, 22 April (Earth Day):
Major simulated outages affecting cloud services, government infrastructure, businesses, and individuals are reported around the world. Expunging the worm may take weeks. Phones are not affected, but quickly become overloaded.

Friday, 23 April:
CRESA contacts Clark County ARES/RACES to request data communications stations be set up the following day at critical locations around the county.

Saturday, 24 April:
Portable field stations with digital data capability are deployed. Members practice sending and receiving simulated messages.

Activation Methods:

Notification will take place the day <u>before</u> the exercise (Friday). The EC notifies the TLs via phone and asks for field stations to be in place and operational by 9:30 AM the following day (Saturday). TLs then notify team members.

Deployment Locations:

As assigned by the EC as part of exercise play. Because of COVID-19 precautions, response locations will only be <u>outside</u> of served-agency and other venues.

_____

Objectives:

1. The Emergency Coordinator develops an ICS-205 (Incident Radio Communications Plan) for the exercise and distributes it to Team Leaders, and Team Leaders distribute it to team members, on Friday, 23 April 2021.
2. Members, or small groups of members, are able to deploy and set up digital data capable field stations using either Orange Kits or personal equipment.
3. All stations are in place and operational by 9:30 AM.
4. Overcome communications obstacles and deliver accurate and timely digital messages.
5. Each participant sends an After Action Report (AAR) to their Team Leader by Monday, 26 April 2021.
6. Each Team Leader sends their team's Form EMD-078 and all team member AARs to the EC by Wednesday, 28 April 2021.

Ground Truth:
1. Infected systems (*unavailable for exercise play*):

   Winlink CMS (Content Message Server) systems, Windows computers which have been connected to the Internet at any time since March 19, 2021.
2. Uninfected systems (*available for exercise play*):

   Windows computers isolated from the Internet and those reinstalled after the worm hit, non-Windows systems (Mac, Linux).
3. Even though some computers are not affected, there are few uninfected systems left on the Internet which can communicate with each other.
4. Communications capabilities available to uninfected computers include Winlink Peer-to-Peer, Packet, and NBEMS.

Operations:
- The Net Control Station (NCS) will operate on CLRK 2, and/or on Secondary and Tertiary repeater(s) as necessary.   *(Operating Aid, Tab 7, Attachment A)*
- <u>Team Leader</u> tasks:
  - *Before the exercise:*
    - Determine how many portable digital data stations the team can stand up and report this to the EC at least a week prior to the exercise.
    - Upon receipt of the ICS-205 form from the EC, distribute it to team members.
  - *At the beginning of the exercise:*
    - Deploy with the team. Establish voice communications with all team portable stations on a team simplex frequency.   *(Operating Aid, Tab 7, Attachment A)*
  - *After the exercise:*
    - Complete the Form EMD-078 time and mileage report for the team and send it to the EC.   *(Operating Aid, Tab 10, Attachment A)*
    - Ensure that all team members submit an After Action Report for the exercise and forward those to the EC.   *(Operating Aid, Tab 12, Attachment A)*
- <u>Member</u> tasks:
  - *Before the exercise:*
    - Check your personal gear for portable digital data communications capability.
  - *At the beginning of the exercise:*
    - Deploy with your team and have the portable digital station active by 9:30 AM.
  - *During the exercise:*
    - Send and receive digital data messages by at least two different methods.
  - *After the exercise:*
    - Complete an After Action Report.   *(Operating Aid, Tab 12, Attachment A)*
    - Send your completed AAR to your Team Leader by Monday, 26 April 2021.

Hot Wash:

At the end of the exercise, all members should participate in an on-the-radio "hot wash" (exercise debriefing, other feedback) which will be conducted by the EC on CLRK 2.