Scenario 15: Cyber Attack

Casualties	None directly
Infrastructure Damage	Cyber
Evacuations/Displaced Persons	None
Contamination	None
Economic Impact	Hundreds of millions of dollars
Potential for Multiple Events	Yes
Recovery Timeline	Months

Scenario Overview:

General Description –

This scenario illustrates that an organized attack by the Universal Adversary (UA) can disrupt a wide variety of internet-related services and undermine the Nation's confidence in the internet, leading to economic harm for the United States. In this scenario, the UA conducts cyber attacks against critical infrastructures reliant upon the internet by using a sophisticated C^2 network built over a long period of time.

Detailed Attack Scenario –

The UA seeks to cause internal, untraceable disruptions in the United States to distract the populace and decision makers for months. The UA believes a cyber attack can effectively meet the goals of information extraction, undermining user confidence in the internet. Disrupting the underlying internet infrastructure will have significant economic impact by severely reducing the public's confidence in the U.S. financial infrastructure and affecting online banking, e-commerce, and other internet-based services.

The UA has spent several years to assemble a joint military and intelligence team. This team includes groups that discover and exploit computer vulnerabilities, create attacks related to those discoveries, conduct reconnaissance and battle damage assessments, and conduct actual cyber operations. The primary target is the confidence of the American people.

The attack campaign is conducted in three phases.

Phase 1 – Attack Preparation

Objective: Construct an attack network with underlying encrypted C^2 mechanisms with which to launch future attacks. This phase will initiate about 2 years prior and continue until approximately 1 week prior to the D-Day event. It will continue until several hundred thousand bots[1] are populated in the attack network.

[1] A **bot** is common parlance on the internet for a software program that is a software agent. A bot interacts with other network services intended for people as if it were a real person. One typical use of bots is to gather information. (www.wikipedia.org)

Event 1.1: Deploy mole software

Attack Mechanism: Write a personal firewall and distribute it via a trusted computer security software provider, such as ZoneAlarm. The software would include an auto-update function. With auto-update, software can be morphed on-command but will appear benign to anyone initially inspecting and approving it. Even on well-run systems, people rarely check old software. The auto-update function will check if its time to start the attack, or just get the latest version. When conducting auto-updates, the software will only connect to known addresses and servers, reserving communications with the botnet[2] until it is time for the actual attack. When loaded onto a victim's computer, the software will participate in the botnet.

Event 1.2: Design and build a bot

Attack Mechanism: Write a bot to scan and deploy using a wide variety of vulnerabilities as they are identified. (Vulnerabilities and the ability to exploit them have a very short life span, relative to a 2-year planning cycle.) The bot will communicate using the same C^2 technology as the mole software but will not do so until it is time to launch the attack.

Event 1.3: Trading and bartering

Attack Mechanism: The internet underground has its own culture for trading and bartering for almost anything, including compromised systems. Compromised hosts (including routers) will be acquired from the underground, and the new bot will be installed. The hosts will also be repaired to prevent other unwanted infiltration.

Event 1.4: Build the C^2 network using traditional, widely available tools and techniques

Attack Mechanism: Use traditional scanning and probing techniques in addition to the newly created tools to build the C^2 network and botnet**.**

Phase 2 – Overwhelm Network Security Personnel

Objective: This goal of this phase is to wear down the first-responder capabilities of the Internet Service Provider (ISP) community just prior to D-Day. The attacks will occur for 2 to 3 hours during periods when first responders are normally not at work (e.g., 2:00 a.m. or holidays). Attacks should repeat randomly across the ISP and the core internet services community with the intent of demoralizing the first responders. These events will all take place in the last few days before D-Day.

Event 2.1: Forge Address Resolution Protocol (ARP) replies

Attack Mechanism: Forge ARP replies with random Internet Protocol (IP) and Mandatory Access Control address information. This is done using the widely deployed zombies. Poison ARP caches causing failures that are very difficult to trace and troubleshoot.

[2] Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. (www.wikipedia.org)

Event 2.2: Undermine Dynamic Host Configuration Protocol (DHCP)

Attack Mechanism: Randomly generate DHCP release requests on behalf of other systems on networks that have zombies deployed. Randomly generate DHCP requests with the intent of consuming network addresses. This will cause local system and network administrators to spend valuable time tracking down problems on local networks.

Phase 3 – Massive Network Outages

Objective: Attack major internet services to undermine consumer and government confidence in the functionality of the internet. This phase will also last only days.

Event 3.1: Attack DNS functionality

Attack Mechanism: Conduct Distributed Denial of Service (DDoS) attacks against the websites and their upstream providers. These attacks will use zombies from both inside and outside organizations. Unleash the botnet built over the past 2 years in a massive DDoS attack.

Planning Considerations:

Geographical Considerations/Description –

The problems are experienced across the Country, as well as internationally. Overseas trade could be affected due to the mistrust in the U.S. internet infrastructure and the problematic U.S. economy.

Timelines/Event Dynamics –

A year or two is needed for preparation. The attack is executed over a period of months to ensure extended press coverage and undermine confidence in the internet.

Assumptions –

- Initial reconnaissance is either undetected or detected but not effectively acted upon.
- The UA can avoid tipping off U.S. intelligence by using U.S.-based hosting companies as it gathers resources for the attack.
- C^2 issues of timing several nearly simultaneous attacks can be worked out by UA's organizational structure.

Mission Areas Activated –

Prevention/Deterrence:

The strength of private sector companies will be tested in regard to prevention and deterrence.

Infrastructure Protection:

Although physical infrastructure is not at great risk, internet software deteriorates, and numerous systems must be repaired. This requires software expertise, time, and money to correct. If not already impacted, numerous systems would have to shut down.

Emergency Assessments/Diagnosis:

The attack will be difficult to recognize. Each attack will end before anyone would have enough time to completely diagnose the problem.

Emergency Management/Response:

Emergency response will be split between technically bringing systems back online and instituting business continuity process, and controlling the public perception of the situation to restore confidence and prevent panicky behaviors.

Hazard Mitigation:

All ISPs, Domain Name Server/System (DNS) operators, and other organizations will need to evaluate their network topologies, diversity, integrity of backup processes, and other methods of attack prevention. Companies will also have to consider methods to improve the first-responder capabilities.

Victim Care:

Primarily, victim "care" will be based on economic assurance. Citizens will look for Government assurances that the internet is a stable and viable method for conducting business and other financial operations.

Investigation/Apprehension:

Using intelligence and law enforcement sources and methods, the investigators will need to determine the likely technical source and the identity of the perpetrators.

Implications:

Fatalities/Injuries –

No significant fatalities or injuries are expected, although collateral effects (e.g., involving hospitals, emergency services responses, and control systems) may have limited fatal consequences.

Property Damage –

No property damage is expected, although those control systems that are dual-homed may cause physical damage.

Service Disruption –

Service disruption would occur across many sectors with possible loss of confidence in the internet and services offered such as online banking and e-commerce.

Economic Impact –

The greatest impact will be intermittent and unpredictable disruptions to the internet, which will affect online banking, other e-commerce services, and general public confidence.

APPENDIX: Scenario Working Group Members

The Homeland Security Council receives interagency guidance via a number of Policy Coordinating Committees (PCCs). One of them is the Domestic Threat, Response, and Incident Management (DTRIM) PCC; the Scenarios Working Group (SWG) supports the DTRIM. The members of the SWG are as follows:

CHAIR: Janet K. Benini, Director of Response and Planning, White House Homeland Security Council

Arkin, Richard	Department of Energy
Avato, Steven	Department of Justice, ATF
Bar-shalom, Tali	White House Office of Science and Technology Policy
Biersack, Walter	Department of Energy
Broun, Laurence	Department of the Interior
Companion, Tod	National Aeronautics and Space Administration
Conklin, Craig	Department of Homeland Security, FEMA
Daly, Kevin	Department of Justice, FBI
Dickson, Howard	Department of Homeland Security
Dolce, Robert	Department of State
Edelman, Phil	Department of Health and Human Services
Fancher, Raymond	Department of Justice, FBI
Finan, William	Environmental Protection Agency
Fuller, Gordon	Department of Justice, FBI
Gillin, MAJ Jeff	Department of Defense
Gosnell, William	Department of Defense, USACE
Gruber, Corey	Department of Homeland Security, ODP
Guffanti, Marianne	Department of the Interior, USGS
Hastings, Thomas	Department of State
Hatchett, Richard	Department of Health and Human Services
Havens, Kathryn	National Aeronautics and Space Administration
Ippoliito, David	Department of Labor, OSHA
Irwin, William	Department of Defense, USACE
Jones, Gregg	Department of Defense
Jorgensen, Andy	Department of Defense
Kadlec, Robert	White House Homeland Security Council
Kerr, Larry	White House Office of Science and Technology Policy
Kevern, Thomas	Nuclear Regulatory Commission
Krueger, Steve	Department of Justice, FBI
Landry, Steve	Department of Homeland Security, ODP
Lim, Kent	Department of Commerce
Lowe, Tom	Department of State
Lustig, Teresa	Department of Homeland Security
Lystra, Clark	Department of Defense
MacKinney, John	Environmental Protection Agency
Maddox, Justin	Department of Energy
Malak, Patricia	Department of Homeland Security, ODP

Martin, Mark	Department of Justice, ATF
McClenney, Lucretia	Department of Veterans Administration
McCreight, Robert	Department of State
McGarry, Sherri	Department of Health and Human Services, FDA
Metzler, John	Department of Energy
Michling, Suzanne	Department of Defense
Mjoness, Mark	Environmental Protection Agency
Mize, W. Keith	Department of Energy
Morzinski, Gregory	Department of Defense
Mullin, Jonathan	National Aeronautic and Space Administration
Newton, Robert	Terrorist Threat Analysis Center
Nicholas, Paul	White House Homeland Security Council
Noji, Eric	Department of Health and Human Services, CDC
Park, Tom	Department of Homeland Security, FEMA
Pavetto, Carl	Environmental Protection Agency
Peluso, Francis	Department of Transportation, FAA
Pond, Robert	Department of Homeland Security, USCG
Pratt, Britt	Department of Agriculture
Siebert, Mark	Department of Justice, ATF
Sizemore, R. Tom	Department of Veterans Administration
Smith, Alan	Department of Agriculture, APHIS
Steele, Scott	Department of Justice, FBI
Stephens, David	White House National Security Council
Taborn, Michael	Department of Transportation, FTA
Thomas, Lori	Department of Agriculture
Tupin, Edward	Environmental Protection Agency
Venkayya, Rajeev	White House Homeland Security Council
Webster, James	Department of State
Weidner, John	Department of Homeland Security
Williams, John	Department of Agriculture
Williamson, Suzanne	Department of Justice, FBI
Winters, Stephen	Department of Defense
Young, Bruce	Department of Veterans Administration