

Botnet Preparedness

The scary reality for organizations that house confidential and sensitive data, including the personal information of employees and citizens, is that there is no end to cybersecurity threats such as botnets, worms and hacking. The Department of Homeland Security, which sponsors October's National Cybersecurity Awareness Month, offers a helpful "Stop. Think. Connect." mantra for the millions of governments, businesses and citizens that connect to the Internet every day.

Botnets are perhaps the most frightening cybersecurity threat. Like ghosts, these highly sophisticated, vulnerability-seeking threats manufactured by cyber criminals are nearly invisible. Unlike the disk-crashing, network-freezing worms and Trojan horses of a few years ago, bots are designed to leave networks and computers running seamlessly by all outward appearances while they siphon data out to their "bot masters" and avoid detection.

Most government agencies are already pursuing a handful of tactics to minimize the chance of network penetration and, if an attack occurs, to isolate the threat and eliminate it. However, the effort is often inadequate or uncoordinated. An optimal strategy can be created using a combination of the CDW Government (CDW-G)-developed approaches below, dependent upon the size and type of agency, budgets and the sensitivity of the information that must be secured. Please feel free to use any or all of this content as you wish, with appropriate attribution*:

- **Install a Windows Firewall.** Though sometimes tempting for users to disable, a Windows firewall can block many network-based exploits when properly configured. This measure is especially appropriate for large agencies with many similarly configured machines
- **Disable AutoRun.** The autorun feature, which automatically installs software, should be disabled as operating systems should never blindly launch commands from foreign sources
- **Break Password Trusts.** Judicious control over local accounts, especially the local administrator account, is critical to isolating and eliminating a threat. Disabling computers' ability to automatically connect to each other closes the path that botnets take to spread to the internal network. This is particularly critical in environments where certain populations of machines store highly confidential data
- **Consider Network Compartmentalization.** In most computing environments, workstations do not need to communicate with each other across departments. Shutting down this capability goes a long way toward preventing the spread of botnets. IT managers should establish private virtual local area networks (VLANs), or access control lists (ACLs) between subnetworks to limit exposure. This strategy is not a good fit, however, in environments that mix voice and data communications, as it tends to break the ability to negotiate virtual circuits on the fly
- **Provide Least Privilege.** When users are not administrators of their own workstations, it is much harder for malware to propagate via drive-by download or for AutoRun methods to take hold on a system. Preventing users from being administrators also makes it more difficult for their user account credentials to spread malware, should the computer become infected
- **Install Host-Based Intrusion Prevention.** To keep botnets from taking root in a system, IT managers should concentrate additional protections on specific network layers based on vulnerability, such as at points of contact between specific hardware and software. This approach does not fix technical flaws or holes in operating systems or application software, but it can reduce the chances that exploits will be successful. These tools are highly effective, but they are expensive and challenging to deploy
- **Enhance Monitoring.** The more that is known about how users and the network operate in normal activity, the easier it will be to determine in real-time when a botnet infestation causes slight anomalies. Agencies can employ a range of products to obtain information about the network's health by collecting data on network traffic, training devices to monitor abnormalities with a central analysis system and deploying intrusion detection and intrusion prevention systems (IDS/IPS). The key to success is around-the-clock monitoring. Even with remote managed security services filling the gap, this might be beyond the capabilities of many government agencies

Botnet Preparedness

- **Filter Data Leaving the Network.** Botnets typically establish communication with one or more remote servers that hackers use to retrieve private information. To stop these communications, and the threats associated with them, agencies can prohibit unwanted traffic from leaving the network, a tool known as egress filtering. Agencies should force Internet traffic through proxies or content filters (see below), or deploy a data loss prevention (DLP) solution
- **Use a Proxy Server.** While it is impractical to block all potentially hostile outbound traffic, forcing outbound traffic through a proxy server will give agencies a secondary choke point for monitoring and controlling Web access and for defeating some attempts to tunnel around security measures. Content filtering is appropriate for almost any agency
- **Install Reputation-Based Filtering.** Tools like IronPort and WebSense can help block e-mail from and requests to addresses that have reputations as potential malware sources
- **Monitor DNS Queries.** The way that a workstation responds to domain name system (DNS) queries is often an early warning sign that the workstation may be infected. Specifically, responses from workstations that contain very low time-to-live (TTL) values should be monitored, as low TTL can indicate infection. By spotting infections early, system administrators can act before the infection spreads too far

*Source: CDW-G