Group shows botnet threat in the future may come from the sky

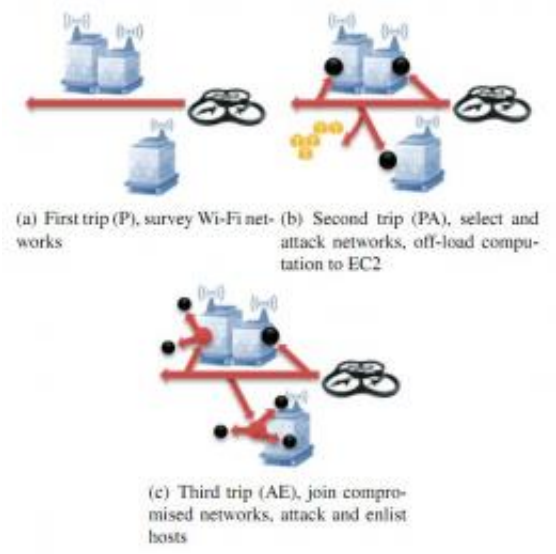
September 9 2011, by Bob Yirka

SkyNET drone prototype.

(PhysOrg.com) -- Sven Dietrich, an assistant professor in computer science at the Stevens Institute of Technology, and two of his students have given a demonstration of an aerial drone, that they say could be used to spy on wireless networks, at last month's USENIX Security Conference. In their presentation, and paper, they say that such drones could be used to move close enough to WiFi connections to eavesdrop or potentially serve as a control unit in a botnet.

The drone, essentially a toy quadricopter (helicopter with four rotors) purchased from a store and configured with a small computer, cameras, software and wireless technology cost the team just $600 to put together, which they say means that almost anyone could construct one and begin using it to listen in on private networks.

While certainly the threat of such a drone eavesdropping on a private or corporate wireless network is rather unsettling, worse is the ease with which such a “toy” could be used to serve as the control unit of a botnet (large numbers of computers infected with code that allows them to be controlled by an outside source.) Because they would be free from tethers on the ground, law enforcement would find it exceedingly difficult, if not impossible to track them down to stamp out the botnet. And that’s a very bad thing, because botnets exist primarily to steal valuable information (such as credit card and bank numbers) off of personal computers, though in some cases they are used more as a tool to bring down web portals via denial of service attacks.



Diagrams showing the PAAE (pilot, attack, attack, enlist) procedure used by the SkyNET drone. Black dots represent targets. In b the targets are networks. In c the targets are both networks and hosts.

Dietrich says such a drone could also be fitted with a solar panel to keep the battery charged, which would allow it to park near a vulnerable site

and do its dirty work almost indefinitely. To make things even easier for the shady characters who wish to quietly plug in to a weakly protected site, the drone can be directed to its target using a 3G smartphone.

This is not the first time that someone has shown that wireless networks could be compromised by remotely controlled aircraft. A demonstration of a reconfigured Army drone following a cell phone signal was shown at the recent Black Hat security conference for example.

The point in these demonstrations is not to scare people, though they most certainly might do just that, but to highlight the risks people and companies take when they don't properly secure their WiFi networks, and to hopefully incite others to find ways to make future systems more secure so that users won't be so vulnerable to such attacks.

More information: SkyNET: a 3G-enabled mobile attack drone and stealth botmaster, www.usenix.org/events/woot11/t … final_files/Reed.pdf

Abstract

SkyNET is a stealth network that connects hosts to a botmaster through a mobile drone. The network is comprised of machines on home Wi-Fi networks in a proximal urban area, and one or more autonomous attackdrones. The SkyNET is used by a botmaster to commandtheir botnet(s) without using the Internet. The drones are programmed to scour an urban area and compromise wireless networks. Once compromised, the drone attacks the local hosts. When a host is compromised it joins both the Internet-facing botnet, and the sun-facing SkyNET. Subsequent drone flights are used to issue command and control without ever linking the botmaster to the botnet via the Internet. Reverse engineering the botnet, or enumerating the bots, does not reveal the identity of the botmaster. An analyst is forced to observe the

autonomous attack drone to bridge the command and control gap. In this paper we present a working example, SkyNET complete with a prototype attack drone, discuss the reality of using such a command and control method, and provide insight on how to prevent against such attacks.

via Technology Review