Disloyal Armies

Abstract
Your computer may be part of a network of zombie devices called a botnet, enabling criminals more easily and cheaply than ever.

Text by Justin Levinson
Illustration by Miguel Arias

"Hi, I'm with the census, and I have a few questions. Do you have a minute?"

Every decade, thousands of workers knock on doors across the US to find out who's living there. Between June and October 2012, someone came knocking on your computer's door for the same purpose, and you probably didn't even notice.

The Internet is a staggeringly massive entity. Every computer, printer, and security camera accessible online has a numeric identifier, or IP address. One anonymous researcher decided he wanted to know if anyone was home at each of the 4.2 billion possible addresses. This task needed an army. So he conscripted one.

Many Internet-connected devices still use their default passwords—the electronic equivalent of leaving the front door unlocked. A simple program invisibly transformed these machines into census troops and gave marching orders to check thousands of addresses. This standing force is known to security professionals as a "botnet", and most are used for more nefarious purposes than counting computers. The researcher was not available for comment.

Right now, unsuspecting users are happily browsing cat videos while their computers work behind the scenes to send spam, flood sites with disruptive traffic, or generate clicks to inflate advertising revenue. Once infected by malware, these zombie computers report to a central command-and-control server and await instructions. The largest ranks number in the millions, but their amorphous nature makes counting imprecise.

These digital shenanigans were originally the domain of curious hackers and pranksters. Now it's big business. "Online fraud has long since moved from being a mere hobby to a means for cybercriminals to earn a living," writes Max Goncharov, a security researcher at Trend Micro.

In a report exploring the sprawling network of underground Russian hacking marketplaces, Goncharov detailed a few available botnet services. Botnet owners rent out their herds for a few dollars per hour. Consultants help nontechnical criminals get up and running. Even botnet software itself is for sale to DIYers—but the underground being what it is, pirated copies are readily available to those who balk at the USD 100+ price tag.

Sometimes, payments come from the unwitting soldiers themselves. One popular botnet toolkit, Zeus, snatches victims' banking logins. Security researchers and law enforcement discovered an international fraud ring, dubbed Operation High Roller, that took the game to the next level: it targeted primarily high-net-worth victims and attempted to siphon nearly USD 78 million from accounts in Western Europe, the US, and Colombia, while stealthily rewriting the users' bank statements to hide the crime.

Law enforcement and software companies have worked in tandem to strike back against the biggest cells. In June, Microsoft coordinated surgical strikes with the FBI against the vulnerable command-and-control servers that kept the Citadel botnet operational, liberating more than a million infected computers. Yet the underground has responded by adopting more guerrilla tactics: smaller botnets to avoid detection and peer-to-peer controls to eliminate command-and-control servers. Among the 730 million inhabited addresses out in the ether, a war between unwitting soldiers of fortune rages on. ●