Corporations, agencies infiltrated by 'botnet'

(AP) -- Security experts have found a network of 74,000 virus-infected computers that stole information from inside corporations and government agencies. The unusual thing about the incident is not that it happened but that it was discovered, and it is a reminder of the dangers of having computers with sensitive data connected to the open Internet.

More than 2,400 organizations, including financial institutions and energy companies and federal agencies, were infiltrated by the "botnet," according to the NetWitness Corp. security firm, which discovered it.

NetWitness didn't name the companies or agencies whose computers were compromised. The Wall Street Journal said the affected companies included Merck & Co., Cardinal Health Inc., Paramount Pictures and Juniper Networks Inc. Merck and Cardinal Health said in statements Thursday that one computer in each company was among those in the botnet but no sensitive information was taken. The other two companies didn't return messages from The Associated Press seeking comment Thursday.

The victims don't appear to have been specifically targeted, unlike the recent computer attacks on Google Inc. that prompted the Internet search leader to threaten to pull its business out of China. That's an important distinction, because it shows how online secrets can fall into the wrong hands even when criminals aren't necessarily looking for them.

"This kind of stuff is out there and it's pervasive," said Amit Yoran, CEO of NetWitness and former cybersecurity chief at the U.S. Department of Homeland Security. Parts of the botnet discovered by his firm likely are still active. He said the network appears to be run from computers in Eastern Europe and China, but it's not certain the perpetrators are there.

Botnets are networks of poisoned PCs that are remotely controlled by hackers and behave like their criminal robots. The PCs are often infected when their owners visit bad Web sites or open malicious e-mail attachments.

Botnets are a major tool for cybercrime. They help criminals amass troves of stolen data that they can sell on the black market or use for their own schemes, such as yanking money from victims' bank accounts.

The biggest on record is the one created by the Conficker worm. That infected anywhere from 3 million to 12 million PCs running Microsoft Corp.'s Windows operating system and is still active.

The botnet NetWitness discovered used malicious software called "ZeuS" that steals passwords and other online credentials. It's primarily focused on poaching Internet

banking credentials and is well known in the security community.

The fact that so many companies and government agencies were hit generally appears to have been incidental. Yoran said the attackers were targeting specific information rather than specific organizations.

Still, they were very successful, snatching more than 68,000 credentials over four weeks. Most of those credentials were login details for Facebook and Yahoo and other personal e-mail services. On the face of it those aren't the most sensitive pieces of information, but they can hold the keys to unlocking other types of online accounts and private data.

Security experts who weren't part of the NetWitness report said the findings illustrate the growing risk from the ZeuS software, whose authors are constantly updating it to evade detection by antivirus software and other security measures.

Don Jackson, researcher with the Counter Threat Unit of SecureWorks, said millions of computers are infected with ZeuS. Perhaps half a million of those are being milked by professional operators running the latest versions of the software.

He said the botnet NetWitness found was a "major threat" but added that the criminals behind it appeared to be using an older version of the software that is easier to detect.

"There are dozens of these types of operations ongoing every day that just aren't named," he said.

A bigger concern, Jackson said, is a new version of ZeuS that has appeared in the last few months and is more powerful and even harder to detect.

One of its features is that it gives a hacker the ability to conduct financial transactions directly from a compromised computer. Otherwise the criminal would have to steal the login credentials and use them on another computer. Some banks have put up extra security measures to detect and stop that.