Cybercrime fighting group takes down Beebone botnet

April 9 2015, byRaphael Satter

Raj Samani, chief technology officer of Intel Security's Europe, Middle East and Africa division poses for a photograph in front of a screen after speaking during an internet security conference in Madrid, Spain, Thursday, April 9, 2015. A new group of international cybercrime fighters claimed one of its first kills Thursday, pulling the plug on malicious servers that hijacked at least 12,000 machines, most of them in the United States. The move is a big step for the Cybercrime Action Taskforce, set up in September in a bid to go after top-level Internet crime. A host of internet security groups, including Intel Security, Kaspersky and Shadowserver, provided assistance. (AP Photo/Paul White)

A new group of international cybercrime fighters claimed one of its first kills Thursday, pulling the plug on malicious servers that hijacked at least 12,000 machines, most of them in the United States.

The elimination of the Beebone botnet is an early success chalked up by the Joint Cybercrime Action Taskforce, a coordination body created last year by the FBI, Britain's National Crime Agency, Europol and host of other international law enforcement agencies.

It's also an illustration of the lengths many hackers go to defeat investigators. Beebone's masters deployed shape-shifting software that updated itself up to 19 times a day.

"From a techie's perspective, they made it as difficult as they possibly could for us," said Europol advisor Raj Samani, who spoke to The Associated Press on Wednesday, only an hour after authorities wrested the last rogue server from the criminals' control.

Botnet is the term applied to networks of hijacked machines which criminals or security agencies use to spread malicious software, empty bank accounts and launch attacks.

Beebone was modest by botnet standards, but Samani—the chief technology officer of Intel Security's Europe, Middle East and Africa division—said it was state-of-the-art. Beebone relied on a pair of malicious programs that re-downloaded each other, an insurance policy should one of them be removed. Regular tweaks to the software's code made it difficult for experts to blacklist the programs.

"In terms of size this is obviously small, but in terms of sophistication . we're talking about an investment by the criminals," he said.

Raj Samani, chief technology officer of Intel Security's Europe, Middle East and Africa division speaks on his cell phone after giving an internet security conference in Madrid, Spain, Thursday, April 9, 2015. A new group of international cybercrime fighters claimed one of its first kills Thursday, pulling the plug on malicious servers that hijacked at least 12,000 machines, most of them in the United States. The move is a big step for the Cybercrime Action Taskforce, set up in September in a bid to go after top-level Internet crime. A host of internet security groups, including Intel Security, Kaspersky and Shadowserver, provided assistance. (AP Photo/Paul White)

The move is a big step for the Cybercrime Action Taskforce, set up in September in a bid to go after top-level Internet crime. A host of security groups—including Intel Security, Kaspersky and Shadowserver—provided assistance.

Europol would not name any of the victims of the botnet. Europol's Paul Gillen said there had not yet been any arrests.

Raj Samani, chief technology officer of Intel Security's Europe, Middle East and Africa division speaks during an Internet security conference in Madrid, Spain, Thursday, April 9, 2015. A new group of international cybercrime fighters claimed one of its first kills Thursday, pulling the plug on malicious servers that hijacked at least 12,000 machines, most of them in the United States. The move is a big step for the Cybercrime Action Taskforce, set up in September in a bid to go after top-level Internet crime. A host of internet security groups, including Intel Security, Kaspersky and Shadowserver, provided assistance. (AP Photo/Paul White)

More information: U.S. Computer Emergency Response Team: www.us-cert.gov