

# Global cybercrime ring targeted by Microsoft and FBI

June 6 2013, by Glenn Chapman

---



Microsoft logo is seen during the Electronic Entertainment Expo in Los Angeles, California, on June 7, 2011. Microsoft says it has teamed with the FBI to disrupt armies of hacked computers used to commit more than a half-billion dollars in financial fraud around the world.

Microsoft said it teamed with the FBI to disrupt armies of hacked computers used to commit more than a half-billion dollars in financial fraud around the world.

A strike coordinated with police and [financial institutions](#) disabled more

than a thousand "botnets" used by a global cybercrime operation to steal people's [banking information](#) and identities, according to the software colossus.

Botnets are networks of computers infected with viruses that let them be controlled by hackers.

"Crimes used to happen through stickups, but today criminals use mouse clicks," said former US [Department of Homeland Security](#) cyber official Greg Garcia, a consultant who spoke for financial industry associations.

"This action aims to stop the ongoing harm of these Citadel botnets against people and businesses worldwide."

An investigation launched early last year led Microsoft and its allies to [malicious software](#) called Citadel, which monitors keystrokes on infected machines and sends information such as account names and passwords to hackers.

Cybercriminals used stolen passwords to take money from online bank accounts, according to Microsoft.

Citadel 'malware' has infected millions of computers in more than 90 countries, with the highest numbers of infections found in Europe, Hong Kong, India, Singapore, Australia, and the United States, Microsoft said.



A crest of the Federal Bureau of Investigation is seen inside the J. Edgar Hoover FBI Building in Washington, DC, on August 3, 2007. Microsoft says it has teamed with the FBI to disrupt armies of hacked computers used to commit more than a half-billion dollars in financial fraud around the world.

"The harm done by Citadel shows the threat that botnets, malicious software, and piracy pose to individuals and businesses around the world," said Microsoft general counsel Brad Smith.

"We're going to continue to work together to help put these cybercriminals out of business."

Last week, Microsoft filed a lawsuit against the unknown and unnamed cybercriminals in a [US District Court](#) in North Carolina and got legal authorization to sever communication between 1,462 Citadel botnets.

On Wednesday, Microsoft and US Marshals seized data and other evidence from botnets, including [computer servers](#) at hosting facilities in New Jersey and Pennsylvania, the software company said.

Microsoft and the FBI also shared information with international authorities in the hope they will take action against machines outside the United States used to control Citadel botnets.

"Today's actions represent the future of addressing the significant risks posed to our citizens, businesses, and intellectual property by cyber threats and malicious software," said FBI executive assistant director Richard McFeely.

"Creating successful public-private relationships—in which tools, knowledge, and intelligence are shared—is the ultimate key to success in addressing cyber threats."

Microsoft and its allies did not believe the threat from Citadel was eliminated but were confident they were able to "significantly disrupt" the criminal operation.

Microsoft urged people to rid Citadel from infected computers, providing free tools online at [support.microsoft.com/botnets](http://support.microsoft.com/botnets).

© 2013 AFP

Citation: Global cybercrime ring targeted by Microsoft and FBI (2013, June 6) retrieved 22 June 2024 from <https://phys.org/news/2013-06-global-cybercrime-microsoft-fbi.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.