

ONE HUNDRED TWELFTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
Minority (202) 225-3641

August 10, 2011

Mr. Dmitri Alperovitch  
Vice President, Threat Research  
McAfee, Inc.  
12010 Sunset Hills Road, Fifth Floor  
Reston, VA 20190

Dear Mr. Alperovitch:

As you may know, I have held several hearings into data security breaches affecting Americans. I have also introduced legislation -- H.R. 2577 -- to create a national standard for data security and breach notification requirements for businesses that hold consumer information. I read with great interest the report McAfee released last week, entitled "Revealed: Operation Shady RAT," detailing the activities of one particular bad actor engaged in a widespread pattern of intrusion. The details of this report are alarming at the least.

The Subcommittee on Commerce, Manufacturing, and Trade has jurisdiction over cyber security and data security and has engaged in a multi-year oversight effort into the effects on consumers, our international competitiveness, and the economy as a whole. As the Subcommittee continues its oversight in this matter, I request a briefing from your security threat research team to inform our efforts.

Specifically, I would like more information on the following questions:

1. While the report suggests the high-profile intrusions of recent months that garnered significant media attention are neither sophisticated nor novel, are they representative of intrusions we should expect to continue? How do these unsophisticated intrusions differ from the intrusions that were the focus of your report? Are such intrusions something the government and private sector can effectively prevent or mitigate on a continuing basis?
2. If these intrusions can be classified as more "unsophisticated" and "opportunistic," what is the threat of the more "insidious" intrusions on which McAfee has focused in recent years? How can we effectively prevent or mitigate these more insidious intrusions?

3. The report suggests that the more insidious intrusions are more likely to occur without public disclosure. Would more public disclosure help or harm industry efforts to fight this type of cybercrime?
4. The report states that McAfee's security threat research team was "taken aback by the audacity of the perpetrators." Did the logs analyzed by McAfee reveal novel techniques or patterns that would be helpful in our efforts to combat cybercrime?
5. While the report concludes that most of the hacker's targets were government agencies, quasi-government agencies, or government contractors, did the logs analyzed by McAfee reveal whether any consumer's sensitive or personal information was exposed or obtained by the perpetrator? If so, what types of data were potentially acquired by the cyber criminals?
6. The report suggests intellectual property and national secrets were the primary targets of the attacks. In terms of trends, what is the greater target: intellectual property and national security information, or consumer information that can be used to perpetrate identity theft?
7. The report describes "a historically unprecedented transfer of wealth" over the last 5 to 6 years. Is McAfee aware of any estimates that quantify the financial impacts on U.S. businesses, consumers, and our economy at large?

We appreciate any assistance that you may provide as we continue our efforts to protect American consumers and our economy from the threat of cyber attacks. Please contact Shannon Weinberg of the Committee staff at 202-225-2927 to schedule this briefing.

Sincerely,



Mary Bono Mack  
Chairman  
Subcommittee on Commerce, Manufacturing,  
and Trade

cc: The Honorable Fred Upton, Chairman

The Honorable Henry A. Waxman, Ranking Member

The Honorable G.K. Butterfield, Ranking Member  
Subcommittee on Commerce, Manufacturing, and Trade