The US Government is the target of some of the most sophisticated and current cyber attacks. It is therefore in the greatest position to analyze the very latest attack vectors, Remediate them, and prevent further exploitation of them.

This information, if made widely available in a standard format, could dramatically improve not only private sector prevention of further attack - but attacks in other sectors of the Governement itself!

Currently this information is rarely shared. And when it is, the distribution is very narrow. One must go outside the Government to elite intrusion detection firms and security hardware/software tool providers to have access to this information which is often too expensive for many agencies and private sector companies.

Given that this critical intelligence information already exists in parts of the Government AND the Government has good reason to share this information with others, I would like to propose the following.

1. A standard process in which all Government intrusions and incident responses should - at completion of their investigation create a standard format set of indicators of compromise. All contractors hired to do incident response and remediation must provide this as a deliverable upon completion.

2. The Government should provide, free of charge, these indicators. So that other Government and private industry security tools (as well as internally developed custom made tools) could easily import that data to help them protect their systems.

3. The information should be in a simple format that any program could easily read. For instance a comma separated file that contains: Type of indicator, Indicator, Description Of Indicator. An example would be:

FileContent, eval('hackerx'), This indicator was found in a web shell back door
FileName, htran.exe, This is a known backdoor file
MD5Hash, 000102030405060708090D, This is an MD5 of a hacker backdoor
etc...

4. This data should be available as a simple HTTP feed, so that any program can download it in real time and import the data. A central repository of this information should be developed so that the data does not have to be sent out via email. Rather, security software could automatically GET it without the need for human intervention.

Thanks for your consideration of this idea.
David Porco