An Open Letter to Congress
from
Andrew Lee, CEO, ESET North America

November 15, 2011

To Members of the United States Congress:

I am the chief executive officer of North American operations for ESET, a world leader in proactive Internet threat protection. As a CEO working to create well-paid jobs in America, I urge you to reject HR 3261, the Stop Online Piracy Act (SOPA) as well as S.968, the PROTECT IP Act (PIPA). Based on my work, and that of my team of researchers, I have to say that this legislation, if passed as currently written, would have a chilling effect on the economy of the United States.

More than 100 million Internet users in over 180 countries rely on ESET products to protect their personal and enterprise data systems. This gives ESET a unique perspective on the DNS filtering proposed by SOPA and PIPA. There is hardly any part of the United States economy today that does not depend upon the smooth operation of the Internet, which in turn relies upon the integrity of the Domain Name system (DNS). The DNS filtering proposed in SOPA and PIPA would seriously undermine that integrity.

While ESET fully supports the goals of protecting IP and reducing piracy, our experiences combatting cybercrime for more than 20 years suggest that SOPA and PIPA will do little to advance these goals. What we are sure they will do is undermine valuable efforts to improve the security of the Internet. Without those improvements, expansion of the global digital economy, of which the United States is clearly a leader, as well as a leading beneficiary, will falter.

Furthermore, the DNS filtering proposed in SOPA and PIPA appears to be at odds with the sterling efforts of United States law enforcement agencies that are leading the world in the fight against cybercrime. I would like to share the perspective of our research team on this, as expressed on our Threat Blog by our Security Evangelist, Stephen Cobb, CISSP:

November 10, 2011 – Today the world woke up to DNS changing and something called DNSChanger. First we had the excellent news of a major FBI bust, taking down a cyber-ring that had infected about four million computers in 100 countries. The operators of this fraud had used a type of malware called DNSChanger to redirect infected computers to rogue websites. For example, Mr. Consumer would type itunes.com into his web browser but end up somewhere other than itunes.com, namely a website chosen by the crooks who had altered the way Mr. Consumer's computer found its way from site to site. (There are plenty of details in the FBI announcement.)

The crooks generated at least $14 million in ill-gotten gains by redirecting traffic to manipulate online advertising schemes. And Mr. Consumer was not the only person affected. Systems within some large enterprises were infected as well as some government agencies, including NASA. Busting this operation was a big win for the feds: 6 arrests made, a huge botnet taken over by the good guys, numerous bank accounts frozen, and

hard drives seized from more than 100 rogue servers. If this action can be followed by a successful prosecution and stiff penalties for those convicted then the risk/reward ratio for cybercrime will be nudged a little closer to "not worth it."

The sheer scale of this DNSChanger scam is likely to increase the momentum for technology that makes it harder to subvert DNS for illegal purposes namely DNSSEC, short for DNS Security Extensions. The goal of DNSSEC is to protect the Internet from certain threats, such as DNS cache poisoning, man-the-middle attacks, and the kind of DNS changing that the FBI has so dramatically brought to light.

How disappointing then, to get an email later the same day, also about DNS changing, but this time the DNS changer is the U.S. government itself, acting at the behest of a coalition of interests looking for ways to defeat online piracy of music, movies, and other intellectual property. This state-sponsored DNSChanger is part of the PROTECT IP bill in the Senate, and it's House counterpart, the "Stop Online Piracy Act (SOPA)." These bills would require DNS server operators in the US to replace the correct IP address for a website with an alternate address provided by the Attorney General's office, if the website was "infringing". The definition of infringing is distributing illegal copies, counterfeit goods or anti-DRM technology.

While we are all in favor of stopping piracy, messing about with DNS and legalizing state-controlled DNS changing seems like overkill. Furthermore, it is fundamentally incompatible with DNSSEC, a technology that will, if it is allowed to proceed, make many parts of the Internet more resistant to abuse, and expand the possibilities for lawful and profitable business in cyberspace. While the FBI and other law enforcement are working hard to stop the bad guys making millions by infecting our computers and subverting DNS it seems unwise to give private companies the ability to go ahead and change DNS armed only with court orders.

In short, these bills will be devastating to the Internet and America's leadership in the global digital economy. They will undermine plans to make the Internet more secure and needlessly complicate the fight against cybercrime. I urge you to reject them.

Sincerely,

Andrew Lee
CEO
ESET North America