Testimony of

Paul Vixie, Chairman & CEO
Farsight Security, Inc.

before the
Subcommittee on Crime and Terrorism
United States Senate Committee on the Judiciary

Hearing on
Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks

July 15, 2014

I. INTRODUCTION

Good afternoon Mr. Chairman, Ranking Member Graham, and Members of the Subcommittee. Thank you for inviting me to testify on the subject of botnet takedowns.

My name is Paul Vixie, and I am the Chairman and Chief Executive Officer of Farsight Security, a commercial Internet security company. I am speaking today in my personal capacity based on a long history of building and securing Internet infrastructure. I am also here at the behest of the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), a non-profit Internet security association whose international membership is actively working to improve Internet security conditions worldwide.

I have first-hand knowledge of these matters from my experience in the Internet industry since 1988. My background includes serving as the Chief Technology Officer for Abovenet/MFN, an Internet Service Provider (ISP); serving as the founder and CEO of MAPS, the first anti-spam company; and acting as the operator of the "F" DNS root name server. I have also been involved in Internet standards work in the Internet Engineering Task Force (IETF) and policy development work in the Internet Corporation for Assigned Names and Numbers (ICANN). In addition, I served for nine years on the board of trustees of ARIN, a company responsible for allocating Internet address resources in the United States, Canada, and parts of the Caribbean. I presently serve on the ICANN Security and Stability Committee (SSAC) and the ICANN Root Server System Advisory Committee (RSSAC). I am the author of several Internet standards related to the Internet Domain Name System (DNS) and was for eleven years the maintainer of BIND, a popular open source DNS software system. It was for my work on DNS and BIND that I was inducted earlier this year into the Internet Hall of Fame. My remarks today reflect my ongoing goal of fostering improvements in botnet takedown activities by the non-profit, for-profit, and law enforcement sectors.

II. LESSONS FROM CONFICKER AND GHOST CLICK

I would like to start by reviewing several successful botnet takedown efforts in recent years, since commonalities among these successes may prove instructive.

In 2008 the Conficker worm was discovered and by mid-2009 there were over ten million infected computers participating in this botnet. I had a hands-on-keyboard role in operating the data collection and measurement infrastructure for the takedown team[1], in which competing commercial security companies and Internet Service Providers – most being members of M[3]AAWG – cooperated with each other and with the academic research and law enforcement communities to mitigate this global threat.[2]

In 2011 the US Department of Justice led "Operation Ghost Click" in which a criminal gang headquartered in Estonia was arrested and charged with wire fraud, computer intrusion, and conspiracy. The "DNS Changer" botnet included at least 600,000 infected computers and the mitigation task was complicated by the need to keep all of these victims online while shutting off the criminal infrastructure the victims at this point depended on[3]. My employer, Internet Systems Consortium (ISC), was the court appointed receiver for the criminal's Internet connectivity and resources, and I personally prepared, installed, and operated the replacement DNS servers necessary for this takedown.

Each of these examples shows an ad-hoc public/private partnership in which trust was established and sensitive information including strategic planning was shared without any contractual framework. These takedowns were so-called "handshake deals" where personal credibility, not corporate or government heft, was the glue that held it together and made it work. And in each case the trust relationships we had formed as members of M[3]AAWG were key enablers for rapid and coherent reaction.

Each of these takedowns is also an example of modern multilateralism in which intent, competence, and merit were the guiding lights. The importance of multilateralism cannot be overemphasized: We have found that when a single company or a single agency or nation "goes it alone" in a takedown action, the result has usually been catastrophe. The Internet is hugely interdependent and many rules governing its operation are unwritten. No amount of investment or planning can guarantee good results from a unilateral takedown action. Rather, takedown actors must work in concert and cooperation with a like-minded team representing many crafts and perspectives, in order to maximize benefit and minimize cost – and I refer specifically to the collateral costs borne by uninvolved bystanders.

For example, Conficker's second major version generated 50,000 (fifty thousand) domain names per day that had to be laboriously blocked or registered in order to keep the control of this botnet out of the hands of its criminal authors. Complicating the situation, these 50,000 domain names were split up across 110 different "country code" top-level domains that are each the property of a sovereign nation. The registries for these domains are a mix of private and public institutions, some with national government oversight and many without. Almost all of the 110 registries agreed to cooperate, which involved sharing technical plans and data, as well as strategic plans and calendars.

Similarly, Operation Ghost Click required cooperation between United States and Estonian national law enforcement agencies, as well as competing national and multi-national ISPs and Internet security companies, and an eclectic collection of Internet researchers and adventurers. This diverse team worked together for a single common cause which was to protect the Internet's end users and restore the Internet's infrastructure after an extraordinary breach.

Privacy deserves a special mention. In any takedown of criminal infrastructure, it is vital that end user privacy be protected according to the greatest common denominator of the laws or rules governing each participant in the coordinated takedown effort. So it was in Conficker, where victim event data that showed time stamps and unique IP addresses were only made available on a trusted, need-to-know basis. This information was only shared either with responsible scientists for studies conforming to international ethical guidelines for human subjects research, or with ISPs and anti-virus companies for the narrow and specific purpose of identifying and notifying victims with the end goals of cleanup and remediation.

Privacy protections during Operation Ghost Click were even more rigorous. The court-appointed receiver who operated the replacement DNS servers deliberately gathered the minimum possible data about each victim, which included the IP address, time stamp, and port number – but no end-user DNS lookup names. Furthermore, the FBI and DOJ team members declared themselves unwilling to hold or even receive victim specific data, so the court-appointed receiver delivered the victim records directly to the researcher and clean-up teams, subject to non-disclosure terms.

The ad-hoc nature of these public/private partnerships may seem like cause for concern, but I hope you will consider the following: First, this is how the Internet was built and how the Internet works; second, this is how criminals work with other criminals. We would not get far by trying to solve these fast-evolving global problems with top-down control or through government directives and rules. Bot-masters are constantly innovating, both by devising new ways to penetrate networks and new methods of avoiding detection. Effective response to, and remediation of, botnet attacks requires a coordinated effort that is flexible, nimble, and capable of quickly identifying and adapting to a dynamic and changing threat landscape. While government has a role to play in the takedown of criminal infrastructure such as botnets, it can be most effective by continuing to support the participation in ad-hoc public/private partnerships by agencies such as Justice (for example, see the FBI's involvement in the National Cyber-Forensics and Training Alliance [NCFTA]) and Homeland Security (for example, see the United States Computer Emergency Readiness Team [US-CERT] and the SEI/CMU CERT).

As another takeaway, I note that these two successful takedown exercises were both zero-fee events – no one was asked to "pay to play." The shared goal of protecting Internet end users and restoring the Internet's infrastructure requires a perfectly level playing field, and the only money which changed hands in Operation Ghost Click was a modest contract for technical services between the DOJ and the court-appointed receiver.

III. EFFECTIVE ACTION REQUIRES UNDERSTANDING HOW BOTNETS ORIGINATE AND PROLIFERATE

I'd like to take a moment to explain where botnets come from and what makes them so attractive to criminals and also what makes them possible.

A botnet is literally a "network of robots," where by "robot" we mean a computer that has been captured and made to run software neither provided by the computer's maker nor authorized or installed by its owner. The Internet now reaches billions of end users, as well as tens of millions of unattended "servers" including alarming growing number of industrial control systems. Every Internet-connected device has some very complex software including an operating system, installed applications, and ephemeral "plugins." The only hard and fast requirement for any of this software is "interoperability," meaning, it merely has to work.

From its humble academic origins in 1969 to the present planetary-scale digital fabric interconnecting most humans and facilitating almost all commerce, the Internet has seen continuous wildcat growth. As a platform for innovation, the Internet is unequaled in all of human history for the value it has created and the tools it has made available to every person in every nation. The level of freedom allowed to innovators on the Internet is unprecedented – pretty much any smart person or team can try out almost any idea, with a built-in global audience and perhaps an immediate global market as well.

The invisible cost of this growth and innovative value creation is that much of the software we run on many of our connected devices was given wide exposure and perhaps forgotten by its maker without receiving "red team" testing to check for vulnerabilities. The challenge for the Internet is that today there is perhaps more assurance that a U.L. Listed toaster oven will not burn our house down than there is that some of our vastly more expensive and powerful Internet-connected devices are insulated from becoming a tool of online criminals.

The economics of this situation also can be challenging, since in the fast-changing, high-growth Internet-enabled economy the winners are characterized by short time to market, low cost, and high volume. Innovators may not always have the time or resources to address potential security issues, so we live in a culture of "patching it later." During the preparation of these remarks, I read news reports of an Internet-enabled light bulb, part of the "Internet of things," that was found to be vulnerable to a simple attack in which it would expose the local wireless network password to anyone who asked. It is extremely unlikely that any of these flawed light bulbs can be patched or that their owners can or will be informed of the need to return the product for a refund or exchange. So while the world needs the Internet and the Internet's powers of economic growth and innovation, the cost to the world is that many tens of millions of connected devices can easily and quite often do become tools for criminals. Some companies know this and are addressing it, but much work remains.

But the pace of innovation and adaptation on the Internet is being matched by the pace of innovation and adaptation by criminal bot masters. After a software flaw leading to

vulnerability is found and circulated, it is quickly exploited for criminal purposes. The first step is to use the flaw to install software used by criminals to manage the new computer as part of a botnet. Later steps will be to install specific software tools to facilitate various kinds of online crime like DDoS attacks, spamming, key logging, credential theft, or identity theft. The most important role of every member of a botnet is: *find and infect more victims*. Thus virtually all software flaws are exercised indirectly, using other infected computers. Criminals can operate their infrastructure through so many layers of proxies and middle-men that it's almost impossible to trace most criminal acts back to their actors. As corollaries, it's safe to say two things: (1) Most Internet crime could not exist without botnets; and (2) Botnets could not exist absent a never-ending series of software flaws in Internet connected devices.

This is not a call for regulatory relief. The Internet's success has come organically; that is, not just without a plan but precisely because there was no plan. No national government or super-national governance body could, or should try to, put this genie into a bottle. Rather, we must take stock of some long-invisible costs and make informed decisions as a nation and as a society on which of the Internet's costs we should just live with versus which costs are high enough that we should seek out cheaper alternatives. The primary ways to lower these costs are no different than any non-Internet field: (1) Understand our situation; (2) Make our choices with eyes wide open; and (3) Invest or front-load wherever it will reduce costs in the long run.

Finally, I'd like to quote an ICANN Security and Stability Advisory Committee (SSAC) report from 2002:

> With the advent of high speed "always on" connections, these PCs add up to either an enormous global threat, or a bonanza of freely retargetable resources, depending upon one's point of view.[4]

Regrettably, the major trend in the twelve years since that report was written is growth – more Internet connected devices, more software flaws, more botnets, and more crime.

IV. STEPS FOR THE FUTURE

Next, I'd like to describe what I think are some practical and effective next steps we can take toward some short and medium term goals. As you'll see, I believe that we can get the most traction by going after the causes, enablers, and attractions of botnets, rather than just beefing up our ability to take down botnets.

Awareness campaigns have played a notable role in slowing the spread of human diseases such as tuberculosis and HIV. Given the danger that an unpatched and undefended Internet connected device can pose to the world's economy as well as to the privacy and safety of its owner and other humans, why would we do less to stop the spread of botnets? I hope to see the day when every user of the Internet knows that if their device is out of date and terribly slow, it is probably infected with malicious software that makes the device steal their identity, send spam, and participate in DDoS attacks.

The US Government is one of the world's largest buyers of Information Technology (IT). Any technical requirement that becomes part of the Federal Information Processing Standards (FIPS) stands a good chance of becoming a de-facto standard for the world. Since DDoS attacks often rely on the lack of Source Address Validation (SAV) by an ISP, perhaps we should investigate requiring SAV by date-certain for all ISPs and hosting or cloud service providers who wish to sell services to the US Government.

Ensuring the security of critical infrastructure is a high priority for both government and industry. It may be useful to explore empaneling a blue ribbon committee to identify and recommend best practices for securing network and server architecture operating industrial control systems, especially as it relates to connected devices, connections between the hot side and the outside, and software testing and patching protocols for those systems. Some of the Conficker-infected computers we tracked in 2008 and 2009 turned out to be industrial controllers for medical equipment including in some cases human life/safety monitors used in surgical operating theatres. While there may be some subtleties involved in getting these embedded computers patched without triggering full recertification, there's no question that these computers should not be connected to the open Internet, or that the staff's first clue that they have a problem should not be a phone call from the Conficker Working Group. We are now a connected society, and we need to find more ways to front-load security protections into Internet-connected services and offerings. To this end, government should continue to support and encourage industry-led groups like M^3AAWG – which has been active in publishing reports and developing voluntary practices aimed at strengthening and facilitating botnet detection and remediation – and public/private partnerships like NCFTA.

V. CONCLUSION

I've given a very brief overview of the botnet problem, its causes, its impact, and its likely future assuming we allow nature to take its course. I'd like to leave you with the following thoughts:

1. The Internet is the greatest invention in recorded history, in terms of its positive impact on human health, education, freedom, and on every national economy.
2. We have necessarily cut some corners on device and software safety and quality in order to innovate at breakneck speed from 1969 to now – time-to-market, not resistance to takeover, has often been our overriding engineering principle.
3. The Internet is also therefore the greatest invention in recorded history in terms of its negative impact on human privacy and freedom, as evidenced by the massive and continuing illicit transfer of wealth from productive people and countries toward unproductive people and countries.
4. Our democratic commitment to the rule of law has very little traction on the Internet compared to how the rule of law works in the real world. The Internet is borderless and lawless, but carries more of the world's commerce every year.
5. These problems manifest as "botnets" which are networks of robots, where the robots in question are using our connected devices in ways we never agreed to.
6. Takedown of criminal infrastructure including "botnets" must be approached not just as reactions after the fact but also as prevention by attacking the underlying

causes.

7. Takedown is no single agency's or any single company's job, and unilateralism never ends well in any case – so, cooperation and multilateralism must be our guiding lights.
8. The US Department of Justice is the envy of the world in its approach to takedown and its awareness of the technical and social subtleties involved, with a special shout-out to NCFTA, a public/private partnership with strong FBI ties.
9. No legislative or regulatory relief is sought in these remarks – the manner in which government and industry have coordinated and cooperated on botnet takedown efforts have underscored the effectiveness of public/private partnerships that afford all affected parties the necessary degree of flexibility and adaptability to face and eliminate botnet threats.

Mr. Chairman, Ranking Member Graham and Members of the subcommittee, this concludes my written statement. Thank you again for this opportunity to speak before you today on this important topic, and I would be happy to answer your questions.

---

[1] *Conficker Working Group*, http://confickerworkinggroup.org/wiki/
[2] *Worm: The First Digital World War*, Mark Bowden, 2011, ASIN B005IGBHU8
[3] *DNS Changer Working Group*, http://www.dcwg.org/
[4] *Securing the Edge*, Paul Vixie, 2002, https://archive.icann.org/en/committees/security/sac004.txt