To: Mr. Andrew Miller, Chair, Science and Technology Committee, House of Commons
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 1, 2011
Subject: Malware

Dear Mr. Miller:

1. *Purpose of This Communication:* We understand that the Science and Technology Committee of the House of Commons is collecting evidence as part of its inquiry into malware.[1] We ask that you consider the following response from the Messaging Anti-Abuse Working Group (MAAWG) as part of that work. You have our permission to use the following material in any way that may advance your work.

2. *Declaration of Interests*: MAAWG is an international non-profit industry-led organization founded to fight online abuse such as phishing, botnets, fraud, spam, viruses and denial-of service attacks. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet Service Providers and Network Operators representing over one billion mailboxes, and from key technology providers, academia and volume sender organizations. The multi-disciplinary approach at MAAWG (http://www.maawg.org) includes education, advice on public policy and legislation, development of industry best practices, guidance in the development of industry standards and the facilitation of global collaboration.

3. *Organization of This Response:* Our responses to the questions you asked follows, in the order those questions were raised in your request.

Question 1. What proportion of cyber-crime is associated with malware?

4. While the Committee may receive submissions that blithely offer a precise numerical response to this question, we'd urge you to review such responses skeptically. Let us briefly explain why.

> a) *All malware infections are cyber-crimes, but not all cyber-crimes are malware infections*. Each system that's surreptitiously compromised by malware is, *ipso facto,* an example of a cyber-crime in its own right. Thus, if we could turn the Committee's question on its head, we could say that "all malware infections are, by definition, cyber-crimes." Unfortunately, however, since there *are* types of cyber-crimes other than malware infections, we cannot simply report a 1:1 relationship between cyber-crime and malware. We must consider what else constitutes a "cyber-crime."
>
> b) *What one considers to be "cyber-crime" can vary from person-to-person or jurisdiction-to-jurisdiction*. Most would certainly include "distributing malware" or "hacking into someone else's computer or network without authorization" as classic examples of cyber-crimes, but beyond that, the definition may get somewhat fuzzier. Some unquestionably illegal offenses, such as the dissemination of child pornography, the sale of pirated software, or the illegal marketing of narcotics and other dangerous drugs, may use computers or networks, but does that make those crimes "cyber-crimes?" Or what if a country's legal system lags its Internet development, and thus some very bad conduct simply hasn't yet had the time to be made officially illegal there?

---

[1] http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news/110719-new-inquiry---malware/

c) *Epidemiological field work on the rate of malware infections worldwide is still imprecise at best, and the rate of malware infection is neither constant nor uniformly distributed*. At best, one might be able to offer a statistical estimate for one particular locale at one particular time, but it would be difficult to meaningfully extrapolate from such a point estimate to broader populations, and to future times, since we have no control over what malware authors, or the populations they target, may do in the future.

d) *Many cyber-crimes go undetected, unreported, or uninvestigated*. Paraphrasing Mr. Donald Rumsfeld, former US Secretary of Defense, those undetected, unreported, and uninvestigated cyber-crimes represent "unknown unknowns." We anecdotally know that such cyber-crimes exist, but since those cyber crimes are undocumented, we have no way of knowing if they did (or didn't) involve malware.

5. Those methodological considerations notwithstanding, there is no question that malware remains the cyber-criminal's "tool of choice." Malware gives cyber-criminals low or no-cost access to the cyber infrastructure the criminal needs to do their misdeeds. For example, virtually all spam, MAAWG's particular focus, is sent via bots. Those botted hosts get made by malware. Thus spam, including unwanted messages containing phishing messages or malware payloads, is very closely linked to bots and malware.

6. There are, however, some types of cyber-crime that may not be malware-mediated, so even if we could make malware go away tomorrow, that would not guarantee a cyber-crime-free world. By way of example, a "carder" does not need malware if he or she is stealing debit card information from an automatic teller machine (ATM) using a realistic-looking fake card reader and keypad overlaid on top of a real ATM.

Question 2. Where does the malware come from? Who is creating it and why?

7. *Most malware is created by specialized programmers who are part of the Internet underground economy. They create malware because they have the professional skills and tools necessary to do so, there's a demand for malware, and they can make a profit by meeting that demand with little personal risk of prosecution. Some malware, however, may be created by nation states or nation state contractors for non-monetarily motivated purposes.*

8. Let's consider an example of a mainstream malware creation and distribution scenario: "pay-per-install" (PPI) affiliate programs. Pay-per-install affiliate programs solicit participants ("affiliates") who will arrange to get the sponsor's code installed on user systems. For each system on which the sponsor's code is installed, the affiliate program participant is promised a small payment. While legitimate participants in reputable PPI programs may do things like bundle an advertising module with an otherwise free game (clearly disclosing the relationship between obtaining the game for free in exchange for putting up with some ads), so-called "blackhat" PPI programs may have participants who use more nefarious methods (including malware) to get the sponsor's executable on a large number of systems. Their motivation in doing so is clear: if you don't ask permission, you'll be able to install more PPI code than if you do, and the more PPI code you're able to install, the more money you'll make.

9. While most malware is economically motivated, there are exceptions. For example, some nations (or nation-state contractors) may employ malware to surreptitiously monitor the communications of peaceful religious or political dissidents. Others may use malware to sabotage strategic industrial facilities. The Stuxnet malware is a well-known example of this later category of malware.

Question 3. What level of resources are associated with combating malware?

10. Every enterprise, and every user of Microsoft Windows who wants to remain uninfected, has to devote substantial effort to avoiding malware infections. Well-regarded industry sources recently estimate the total worldwide security *software* market at US$16.5 billion,[2] however that estimate does not also include the market for *hardware* security appliances, which are hugely popular, nor expenditures on security-related *staff or consultants*, nor loss of productivity associated with patching and other security maintenance activities.

11. That cost estimate also does not include the costs related to dealing with malware that has gained a toehold notwithstanding everyone's best efforts to keep it at bay. Turning to another study, we see that the worldwide cost of economic damages from malware exceeded $13.3 billion[3] five years ago.

12. Viewed from a macroscopic perspective, national authorities should also consider and include estimates of law enforcement and prosecutorial costs associated with combating malware authors, the economic impact of malware-enabled corporate and industrial espionage on national competitiveness, and the cost of counterintelligence programs needed to respond to malware-related national security cyber-security threats.[4]

Question 4. What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

13. Traditionally, antivirus programs have relied on "signatures" to identify and block malware. Contemporary malware authors know this, and have come to check "draft" versions of their malware against popular antivirus products, tweaking and repacking their malicious code until it avoids detection by at least the most popular antivirus products. The malware authors have a difficult-to-overcome advantage in this arms race: they can continually modify their code at a pace that the antivirus vendors cannot match. As a trivial example of this, *envision a malware author who automatically releases tweaked versions of his or her code hourly, while antivirus vendor customers might download updated signatures only once a day. The malware author is thus guaranteed a "window of vulnerability."*

---

[2] "Gartner Says Less Than Half of Security Software Market Belongs to Top Five Vendors," July 2011, http://www.gartner.com/it/page.jsp?id=1752714

[3] "Annual Worldwide Economic Damages from Malware Exceed $13 Billion," June 2007, http://www.computereconomics.com/article.cfm?id=1225

For that study, " direct costs are defined as labor costs to analyze, repair and cleanse infected systems, loss of user productivity, loss of revenue due to loss or degraded performance of system, and other costs directly incurred as the result of a malware attack. Direct costs do not include preventive costs of antivirus hardware or software, ongoing personnel costs for IT security staff, secondary costs of subsequent attacks enabled by the original malware attack, insurance costs, damage to the organization's brand, or loss of market value."

[4] The public will likely never know the total cost of incidents such as the USB-born infection that totally disrupted U.S. Army networks in 2008. That malware was described by William J. Lynn, U.S. Deputy Secretary of Defense, as "the most significant breach of U.S. military computers ever," see "Defending a New Domain," *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

14. In spite of that "window of vulnerability," consumers (or their ISPs, indirectly), routinely purchase and install antivirus software on their Windows computers, and in truth, while not perfect, that software does successfully block some malware. The cost of that software may vary from $0 out-of-pocket (for open-source or other freely available antivirus products, or commercial antivirus products licensed by the user's ISP), to $20 or more per system per year for antivirus products purchased ala-carte. Security software suites that bundles antivirus software with other functionality (such as antispyware software, antispam software, a software firewall, application patch status monitoring, etc.) are typically higher.

15. *The cost of antivirus software (effectively malware "insurance") is dwarfed by the cost to users of trying to clean up a malware infection should an "accident" actually occur*. Once infected, most security experts believe that the only way you can be sure you once again have a secure and stable system is by "nuking and paving" the system -- formatting it and reinstalling from scratch, or at least formatting and reinstalling from trustworthy backups predating the infection. Unfortunately many users do not have trustworthy backups of their systems, nor can they recreate all the programs and other applications they may have installed. As a result, they're left trying to "disinfect" a system that may be fundamentally difficult or impossible to remediate. Because they don't have the tools or expertise to do so themselves, they turn to specialty service providers for help. Pricing typically varies, depending on whether the user is able and willing to try to disinfect online, or they need to bring their system in to a service location, or they want the help service to make a "house call," but pricing typically runs in the US$150-300 range. For comparison, if the user doesn't need to recover content that's only stored on the contaminated system, and the system isn't one that has special features or functions, a basic replacement desktop system can be purchased for roughly US$300 on sale, and a basic replacement laptop can be purchased for roughly US$350 on sale. Considering the fact that the (still-infected) old system may be able to be sold some unsuspecting 3rd party, its often cheaper to replace an infected system than disinfect it.

16. *Other users may avoid Windows (the most malware-targeted operating system) entirely, purchasing a system that uses a less-aggressively targeted operating system instead. This comes with costs of its own*. For example, while Windows desktops often can be had for as little as US$300, the least expensive Apple Mac desktop, the Mac Mini, cost roughly twice that, US$599. Similarly, while a Windows laptop can be had for as little as US$350, the least expensive Mac laptop costs US$999, nearly three times that amount. Dealing with multiple operating systems also increases the complexity of supporting users for ISPs, higher education institutions, enterprises, government agencies, software vendors, etc.

Question 5. Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

17. Yes, we believe such a responsibility exists. The Government has a compelling national interest in the protection of its citizens and businesses online, and in the protection of their networks and systems. An attack on United Kingdom citizens' networks and systems, whether blatant or insidious, is an attack on the UK as a whole, and properly deserves national attention and response.

18. At the May 2007 Anti-Phishing Working Group (APWG) Counter E-Crime Summit in San Francisco, one of MAAWG's senior technical advisors presented a talk entitled, "We Need A Cyber CDC or Cyber World Health Organization."[5] In that talk, Dr. St Sauver considered four parties that might potentially have responsibility for cleaning up a malware-infected systems: the system owner, their ISP, their software vendor, and the author of the malware. He then explained why, in each case, those parties would many times fail to clean up malware-infected systems. When all these other parties

[5] http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf

fail to take effective action, the Government's the only one who's left. It effectively becomes the "party of last resort," just as it is in real life for disasters such as floods, hurricanes, earthquakes, etc. We do not have room to recapitulate St Sauver's full presentation here, but we will provide a copy of that presentation for your consideration along with these remarks.

Question 6. How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

19. We recognize the fine cyber-security/anti-cyber-crime work that has been done by many government agencies in the U.K., including New Scotland Yard,[6] the Serious Organized Crime Agency (SOCA),[7] the Center for the Protection of National Infrastructure (CPNI),[8] the Communications-Electronics Security Group (CESG),[9] The Security Service (MI5),[10] the Secret Intelligence Service (SIS/MI6),[11] the Information Commissioner's Office (ICO),[12] the British and Foreign Commonwealth Office (FCO),[13] and many others. The United Kingdom also contributes and benefits from its work with Europol,[14] Interpol,[15] the Council of Europe,[16] and international law enforcement agencies such as the FBI.

20. However, if we rely on Google as an impartial arbiter of online influence, when we search for

malware cyber-crime site:uk

we do not see a single UK government site that strikes us as the "go-to" site for *operational* issues related to this topic -- ironically, in fact, the top result returned when we did this search was to this very Parliamentary Committee! This may be a matter of online documentation lagging boots-on-the-ground capabilities, but our impression, right or wrong, is that users might have a hard time figuring out who in the UK government or UK law enforcement to contact regarding the fight against cyber-crime involving malware. We urge you to rectify that.

---

[6] http://content.met.police.uk/Home

[7] http://www.soca.gov.uk/

[8] http://www.cpni.gov.uk/

[9] http://www.cesg.gov.uk/

[10] https://www.mi5.gov.uk/

[11] https://www.sis.gov.uk/

[12] http://www.ico.gov.uk/

[13] http://www.fco.gov.uk/en/

[14] https://www.europol.europa.eu/

[15] http://www.interpol.int/

[16] http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

21. In allocating responsibilities for dealing with malware and cyber-crime, we urge you to note that three distinct roles need to be filled:

> a) You need a criminal law-enforcement agency with primary responsibility for investigating use of malware in non-national security contexts,
>
> b) You should also have an agency from the U.K. intelligence community which can provide leadership on the problem of malware in national security contexts, and
>
> c) You also need an agency that is NOT involved with either law enforcement or the intelligence community, an agency which can be charged with helping U.K. citizens and businesses to cope with malware, including acting as a resource of last-resort for dealing with malware-infested UK systems and networks (as recommended in our response to Question 5., above).

22. We recommend separating the law enforcement and intelligence community roles because often evidentiary and procedural practices, and operational goals, differ between those two groups. Keeping them separate minimizes the potential for confusion or conflict. Likewise, we believe it will be important to keep the third "helper" role separate from the other two roles, so that citizens can ask for help while maintaining an expectation of privacy, much as they might receive confidential professional advice from a barrister, physician, clergyman, chartered accountant or other professional.

23. In conclusion, thank you for the opportunity to address these questions and to potentially help in some small way with the Committee's work. Please don't hesitate to get in touch with us if we can clarify any of the above points, or address other questions you may have.

Sincerely,

/signed/

Jerry Upton, Executive Director
Messaging Anti-Abuse Working Group
jerry.upton@maawg.org

[2,744 words including footnotes]