MAAWG

To: Mr. Andrew Miller, Chair, Science and Technology Committee, House of Commons
From: Messaging Anti-Abuse Working Group (MAAWG)
Date: September 6, 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 publicly to advance your work.

2. *Declaration of Interests*: The Messaging Anti-abuse Working Group (http://www.maawg.org – hereafter "MAAWG") is an international non-profit industry-led organization founded to fight online abuse such as botnets, phishing, fraud, spam, viruses and denial-of service attacks that can cause great harm to both individuals and national economies. 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 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 follow 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 specify a precise numerical or associated financial cost in response to this question, we would 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 caused by malware infections*. Each system that is surreptitiously compromised by malware is, *ipso facto,* an example of a cyber-crime in its own right. Thus, turning the Committee's question around, one could say, "All malware infections are, by definition, cyber-crimes." Unfortunately, however, since there are many common types of cyber-crimes other than malware infections, we cannot simply report a 1:1 relationship between cyber-crime and malware. We must consider other transgressions that also constitute "cyber-crime."

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

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 become somewhat less precise. 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 this does not make those crimes, by definition, "cyber-crimes." Furthermore, if a country's legal system lags behind its Internet development, and thus malicious computing acts and conduct simply has not yet been made illegal, are we to exclude accounting for such crimes due to their legality? We think not.

c) *Epidemiological fieldwork 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 industry experience has shown that it is difficult to meaningfully extrapolate from an estimate based on a specific point to broader populations and future times. This is further complicated because 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*. These undetected, unreported and uninvestigated cyber-crimes represent "known unknowns." We anecdotally know that such cyber-crimes exist, but since those cyber crimes are largely undocumented, and are at best anecdotally reported, we have no way of knowing if they did (or did not) involved malware. We must also concede that there are other "unknown unknowns" whose mode of action and parameters we cannot even begin to sketch out at this time.

5. Methodological considerations notwithstanding, there is little question that malware remains the cyber-criminal's "tool of choice." Malware gives cyber-criminals access to the cyber infrastructure they need to do their misdeeds and at no incremental cost. For example, the vast majority of all spam is sent via botnet networks of infected home computers. Those botted hosts are created by malware that is surreptitiously installed without the owner's knowledge. Thus most spam, including unwanted messages containing phishing text or malware payloads, is very closely linked to both bots and malware.

6. There are, however, some types of cyber-crime that are not malware-mediated, so even if malware were to disappear tomorrow, that would not guarantee a cyber-crime-free world. By way of example, a "carder"[2] 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. However, this same carder may then sell the purloined information online in one of the infamous, covert "Carder Forums." Cyber-crime or not? It is difficult to determine.

[2] A practitioner of carding, in the context of credit card fraud - ref. Wikipedia http://en.wikipedia.org/wiki/Carder

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

7. Malware is created by specialized programmers who are an integral part of the Internet underground economy. They create malware because they have the professional skills and tools to do so, there is a demand for malware, and they can make a profit by meeting that demand with little personal risk of prosecution. While most of malware programmers focus on developing malware to steal identity or financial-related data, there also are nation-states or their contractors who create malware for non-monetarily motivated purposes.

8. 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 have the sponsor's code installed on user systems; for each installed system, the affiliate program participant is promised a small payment. While legitimate participants in reputable PPI programs may use strategies such as bundling a PPI-based advertising module with a free game – while clearly disclosing the relationship between obtaining the game for free in exchange for putting up with some ads – so-called "blackhat" PPI programs often have affiliates who use more nefarious methods (including malware) to unknowingly install the sponsor's executable code on a large number of systems. Their motivation in doing so is clear: if you do not ask permission, you will be able to install more PPI code than if you do, and the more PPI code you install, the more money you 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 spy on private policy exchanges and government funded R&D projects or to sabotage strategic industrial facilities. The Stuxnet[3] 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 Microsoft Windows user 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 USD.[4] However this estimate does not include the market for *hardware* security appliances, which are hugely popular, expenditures on security-related *staff or consultants*, or loss of productivity associated with patching and other security maintenance activities.

11. This 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 USD[5] five years ago.

---

[3] http://en.wikipedia.org/wiki/Stuxnet

[4] "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

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

For this 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."

12. Viewed from a macroscopic perspective, national authorities should also consider other major costs engendered by malware malfeasance. This includes 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.[6]

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 now 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 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, at most. The malware author is thus guaranteed a "window of vulnerability."

14. In spite of the "window of vulnerability," consumers (or indirectly their ISPs) routinely purchase and install antivirus software on their Windows computers, and in truth, while marginally effective, that software does block some malware. The cost of that software may vary from $0 out-of-pocket (for open-source, 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 a-la-carte. Security software suites that bundles antivirus software with other functionality such as antispyware software, antispam software, a software firewall, application patch status monitoring, and other features are typically higher.

15. *The cost of antivirus software (effectively, malware "insurance") is dwarfed by the cost to end-users of trying to clean up a malware infection should an incident actually occur*. Once infected, most security experts believe the only way to 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.

16. Unfortunately many users do not have trustworthy backups of their systems nor can they reinstall all the programs and other applications that may have resided on their machines. As a result, they are left to try to "disinfect" a system that may be fundamentally difficult or impossible to remediate. End-users usually do not have the tools or expertise to affect such clean-ups themselves and often turn to specialty service providers for help. Pricing varies depending on if the user is able and willing to try to disinfect online, if they need to bring their system into a service location, or if they want the help service to make a "house call." Overall, the pricing typically can range up to USD $300. For comparison, if the user does not need to recover content that is only stored on the contaminated system and the system does not have special features or functions, a basic replacement desktop system can be purchased for a few dollars more. It is often less expensive to replace an infected system than disinfect it.

---

[6] 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

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, Joe St Sauver, a MAAWG Senior Technical Advisor, presented a talk entitled, "We Need A Cyber CDC or Cyber World Health Organization."[7] In that talk, Dr. St Sauver considered four parties that might potentially have responsibility for cleaning 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 malware-infected systems. The Government is the only interested party left when all these other parties fail to take effective action. It effectively becomes the "party of last resort," just as it is for disasters such as floods, hurricanes or earthquakes.

19. Others have suggested a similar approach at the international level: Eugene Kaspersky, CEO of Karpersky Labs, recently put forth a call for the creation of an "Internet Interpol"[8]; such an entity could play a similar role to the United Nation's World Health Organization in terms of coordinating strike-teams to deal with (computer) virus outbreaks. Mikko H. Hyppönen, the Chief Research Officer of anti-virus company F-Secure, recently made similar comments in his CNN[9] column, Sharing intelligence among international law enforcement agencies has never been more critical. We encourage you to review any roadblocks to such data exchange and remove them entirely, if at all possible.

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

20. In allocating responsibilities for dealing with malware and cyber-crime, three distinct roles must be filled:

a) A criminal law-enforcement agency with primary responsibility for investigating use of malware in non-national security contexts

b) An agency from the UK intelligence community that can provide leadership on the problem of malware in national security contexts

c) Not involved with either law enforcement or the intelligence community, an agency which can be charged with helping UK citizens and businesses 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).

21. We recommend separating the law enforcement and intelligence community roles because operational goals and evidentiary or procedural practices often differ between those two groups. Keeping

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

[8] AusCERT 2011: Eugene Kaspersky calls for Internet Interpol - Online ID needed to verify people, says Kaspersky founder http://www.computerworld.com.au/article/386790/auscert_2011_eugene_kaspersky_calls_internet_interpol_/

[9] Fight cybercrime, but keep the net free http://www.cnn.com/2011/OPINION/08/06/hypponen.cybrcrime.ted/index.html

them separate minimizes the potential for confusion or conflict. Likewise, we believe it is important to keep the third "helper" role separate from these other two functions so that citizens can ask for assistance with an expectation of privacy, much as they might receive confidential professional advice from a barrister, physician, clergyman, chartered accountant or other sanctioned professional.

22. In conclusion, thank you for the opportunity to address these questions and to potentially assist in some small way with the Committee's work. Please do not hesitate to contact 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

MAAWG PPC2011-10