A Broader Look at Web-Based Malware: Mapping the Threat to Better Fight It

The Chain of Trust Initiative
May 2010

Boris Jamet-Fournier
Harvard Kennedy School of Government – Advisor: Professor Nicco Mele

Acknowledgments

I would like to thank the many individuals who have contributed to my understanding of web-based malware. The first and most important is my professor and mentor, Nicco Mele, who sparked my interest in the Internet. Nicco encouraged me to find out more about the consequences of digital technology for politics, journalism, communications, and many other areas of human life. This report is my attempt at understanding a dimension of the Internet I knew little about before I started my research, and at proposing a fresh insight on the world of web-based malware. I am extremely grateful to Nicco for providing food for thought to a growing community at the Kennedy School and offering his unlimited support.

I would also like to sincerely thank Professor Jeeyang Rhee Baum and Mayor Bill Purcell, my Policy Analysis Exercise seminar leaders, whose advice and challenging questions have been particularly helpful.

Of course, I am also very thankful to all the people I have interviewed for this report and the Chain of Trust Initiative and its staff. I also want to extend my very sincere thanks to Maxim Weinstein, who has been an exceptionally helpful and accommodating client.

Contents

Executive Summary

What can the Chain of Trust Initiative do to advance the cause of a safer Internet for all users?

Most observers point out that in the field of web-based malware, actors are constantly faced with uncertainty, blurred expectations, a lack of standards, and the absence of a general framework that would facilitate comprehension by individuals and action by communities. The main challenges of web-based malware (the barriers to awareness, the adaptive nature of the threat, the opposition between virtual threats and material losses, the opposition between the creation of a public good and business objectives, the difficulty to assigning responsibility) make it a very complex issue to deal with.

How to take a broader look at web-based malware? Can a comprehensive map of web-based malware be established? Who are the main actors and their influencers? What are their interactions, and what can we learn from them? What specific recommendations can help the Chain of Trust Initiative better "stem the rising tide of malware"?

This report is my attempt at answering these questions.

MAIN FINDING # ONE:
An extremely large number of individual and collective actors have an interest in or an influence on web-based malware. Their preferences are not always aligned, even when they are theoretically trying to achieve the same goal. Expertise and motivations vary wildly among these groups. In this system, the number and the diversity of these stakeholders makes it is extremely hard to assign responsibility in any clear or constructive way.

MAIN FINDING # TWO:
Using the chain of trust concept, it is possible to make sense of the comprehensive list of malware stakeholder categories presented in this report. The web security chain of trust shows major actors, influencers and interactions in the world of web-based malware and gives helpful insight into what parts of the chain can and should be reinforced (user-ISP and web host-website owner links in particular).

MAIN FINDING # THREE: A large number of web-based malware stakeholders, especially end-users, lack expertise on the subject. This lack of familiarity with web-based malware leads actors to understate the threat that it creates.

Recommendation 1: Recognizing the fact that not everyone can become an expert, the COTI should maintain and further its educational outreach, extending the chain of trust findings to all types of stakeholders:

- Who are the actors?
- When do they interact?
- What is my role in the chain of trust?
- How to establish responsibility?

MAIN FINDING # FOUR: A major obstacle to fighting web-based malware is that it is not concrete enough. Different aspects of the malware threat (for instance, the fact that a large number of

intermediaries and influencers can make the chain of trust weaker, or the fact that web-based malware are "silent" attacks) make it too abstract for some actors to realize the risks with which it is associated.

Recommendation 2: The COTI should make both the reality and the perception of web-based malware more concrete.

MAIN FINDING # FIVE: Large improvements are needed at an institutional level to enhance awareness, willingness to cooperate, dialog, and coordination.

Recommendation 3: The COTI should lead several initiatives to promote institutional improvement in the anti-malware community, on threat names, coordination, and standards, especially.

MAIN FINDING # SIX: The reality of the world of web-based is still far from the ideal set by the web chain of trust.

Recommendation 4: The COTI should work to reinforce the chain of trust by eliminating weak links and increasing transparency.

Introduction

Three lessons from the Google v. China feud

On Tuesday, January 12, 2010, Google, Inc. announced on its blog that the company "should review the feasibility of [its] business operations in China" (The Official Google Blog, 2010) after discovering that malware attacks had targeted their corporate infrastructure and that of more than a dozen of large western companies based in China. The sophisticated cyber attack was said to originate from within China and was described by the Mountain View company as a major breach of trust between Google and the Chinese. Google said it had also unearthed evidence that phishing scams or malware attacks had been targeting some Gmail users, including human rights activists.

Since launching Google China in 2006, the American multinational had worked closely with Chinese authorities, offering only limited access to services they fully provide in other countries in the hope that providing the Chinese people with the possibility to use their powerful search engine, even if censored, represented a net gain in terms of freedom—of course, the prospect of China and its 300 million users (by official count) were also extremely attractive to the search engine giant. In the same press release, Google stated that it was considering pulling out of the country. The announcement triggered significant coverage (the search "google" on Google News returned twice as many entries in January 2010 as in October and December 2009, the two months of the year in which Google received the most coverage) and the claim by Hillary Clinton that American could not "stand by while people are separated from the human family by walls of censorship" (Clinton, 2010) a few days later, in a speech on Internet freedom given in Washington DC, only added to the buzz. The Secretary of State, whose remarks openly commented on the hostilities between Google and Chinese authorities, insisted on the idea that "an attack on one nation's networks can be an attack on all." Two months after the incident, Google started redirecting all google.cn traffic towards Hong Kong.

The interruption of a conversation about malware on major news outlet is extremely relevant to this research. From my perspective, the conflict offers three major lessons.

The first is that computing is relevant to public policy. While this is old news to some experts and a fringe of the population with an interest in cyber security, the fact that computer attacks can be directly related to international relations in general, and the American interest in particular, was certainly not clear to the larger public before the beginning of 2010. After January of this year, many more people became aware that cyber attacks can be used *by* governments *against* other governments or large entities (like Google) to accomplish policy goals. This is one of many steps in the collective realization that the physical and the virtual are in fact part of the same world. The 2008 Barack Obama campaign, which used the Internet to mobilize millions of supporters and raise record-setting contributions, led to the same kind of collective understanding in the realm of politics.

The second lesson is that the world of computer security is infinitely vast and complex. Google, a company that usually provides services to Internet users, was the *target* of cyber attacks. The Chinese authorities could be the perpetrators of these strikes, while in other countries and in a different context, governments actually fight this kind of aggression. Specific individuals were also targeted in ways that might pose a threat to their freedoms, and eventually, their lives. How did the criminals (whoever they are) attack their victims, and through what channels? How does one make sense of this large number of actors and these intricate relationships?

The third lesson is a consequence of the first two. If computer security is a vast and complex realm that is relevant to an increasing number of actors in a growing number of areas, should not the general public have at least a basic understanding of these phenomena? Research data from Zogby International shows that an overwhelming majority of connected Americans feel safe online (88 percent) and that a similar number of US web users think they have the adequate tools to protect themselves on the Internet (84 percent). Commenting on these results from April 2008, online safety expert and executive director of the National CyberSecurity Alliance, Ron Teixeira,

stated, "the perception of users is that they are safe, but the reality is they are not" (SCMagazine). Prior research conducted by McAfee and the National CyberSecurity Alliance shows that 78 percent of the computers that users thought were safe were in fact inadequately protected. StopBadware's Maxim Weinstein reinforces Teixiera claim by insisting on the changing nature of malware, most of which used to be "annoying, pop-up-laden pieces of software that attracted a user's attention. Now, drive-by downloads silently install spyware and bots that run in the background, often without the computer user's knowledge. Thus, users may feel safe even while their machines are compromised" (2008, SCMagazine). Because we know that these threats are not only relevant to policy, but also applicable to their private computers and their private lives, should not all computer users understand malware better?

Defining web-based malware

Since the purpose of my research is to take a broad look at the world of malware, I have chosen to use a broad definition of the concept. In this report, malware is defined as any application that does not let individuals use their computer or their network as they intend, that is deceptive or irreversible, or that limits the user's freedoms with regard to his or her computer on and offline. I should add that the term "malware" itself is subject to debate—while some institutions, like the Anti-Spyware Coalition, often use the phrase "Spyware and Other Potentially Unwanted Technologies", other organizations, like StopBadware, more frequently use the word "badware;" different organizations use different terms to represent a similar (but not identical) reality. In this report, "malware" should be interpreted as a synonym of what StopBadware defines as "badware" in its guidelines (StopBadware, 2010). Using a broad definition of malware is also useful because it is more consensual among experts than these more specific, competing interpretations.

According to this definition, "malware" includes viruses, trojan horses, false updates, worms, spam bots, and many other types of harmful software. The differences between these varieties are

sometimes slight, sometimes substantial; yet, given my actor-focused approach, I have chosen not to delve into the distinctions between the different breeds of malware. However, I will focus on malicious software that is distributed through the web, for instance, via drive-by downloads (downloads the user is not aware of). Research from 2008 (Greenstadt et al.) suggests that drive-by downloads from trusted websites are "the most common form of malware distribution on the Internet." My research thus centers on web-based malware[1], as opposed to malware that reaches the victim's machine through e-mail (spam), mobile media, social engineering, or other types of malware transmission techniques.

Although I will come back to malware creators later in the report, it is important to say here that when using malware, cybercriminals are typically hoping to steal other users' Personally Identifiable Information (PII)[2] or other confidential information, sell a product the users do not need, send spam, or spread more web-based malware (botnets). While the overwhelming majority of cybercriminals use malware as a way to steal money directly or indirectly, sometimes in large quantities (Business Week, 2006), other individuals and organizations use malicious software for other (usually political) purposes. The Google incident in China is a prime example of this type of activity.

The Chain of Trust Initiative (COTI)

StopBadware Inc. is one of the many organizations that fight the spread of malware on benevolent Internet users' machines and networks. The project was started at Harvard University's Berkman Center for Internet and Society under the direction of professors Jonathan Zittrain and John Palfrey. In January 2010, StopBadware became an independent non-profit organization and is supported by several large Internet companies, including Google, Mozilla, and PayPal.

[1] In October 2009, more than 640,000 Web sites and about 5.8 million pages were infected with malware, according to Dasient, a web-based malware removal company.

[2] According to Maneesha Mithal, the associate director of the Federal Trade Commission's privacy division quoted in the New York Times on March 16, 2010, privacy is so difficult to maintain online that "technology has rendered the conventional definition of personally identifiable information obsolete."

Executive Director Maxim Weinstein and his staff are dedicated to fighting malware-generating data and analyzing trends thanks to the StopBadware Website Clearinghouse, their searchable database of malware Uniform Resource Locators (URLs). This is the core of the non-profit's work and also its most time consuming activity. Furthermore, StopBadware hosts the online community, BadwareBusters.org, and seeks to influence thinking and behavior through its advocacy arm by publishing guidelines for users and news updates on its blog.

The Anti-Spyware Coalition (ASC) is a consortium of anti-spyware software companies, academics, and consumer groups who share the goal of fostering agreement on definitions and practices in this community. Members of the ASC include AOL, McAfee Inc., Microsoft, and Yahoo! Inc., who gathered in this consensus body at the initiative of the Center for Democracy and Technology in order to discuss the main threats the industry is faced with in terms of malware and to produce documents for both experts and the larger public.

The National CyberSecurity Alliance (NCSA) and its educational website, staysafeonline.com, seek to encourage a culture of online security and to teach all Internet users what online behaviors are the safest. The public-private partnership, which also counts a number of large corporate sponsors, was founded in 2001 and is one of the main promoters of the National Cyber Security Awareness Month (October).

Hoping "to stem the rising tide of malware" (StopBadware, 2009), StopBadware, the ASC, and the NCSA came together in May 2009 and launched the Chain of Trust Initiative, a collaborative effort designed to further each organization's anti-malware work (SCMagazine, 2009).

Mapping web-based malware?

What can these three organizations do together to advance the cause of a safer Internet for all users?

Most observers point out that in the field of web-based malware, actors are constantly faced with uncertainty, blurred expectations, a lack of standards, and the absence of a general framework that would facilitate comprehension by individuals and action by communities. I will describe five challenges of web-based malware that contribute to this uncertain environment in depth in this report.

Once these challenges have been identified, how does one take a broader look at web-based malware? Can a comprehensive map of web-based malware be established? Who are the main actors and their influencers? What are their interactions, and what can we learn from them? What specific recommendations can help the Chain of Trust Initiative better "stem the rising tide of malware"?

This report is my attempt at answering these questions. I will do so in five steps (a through e). Once I have identified and illustrated the main challenges of web-based malware (a), I will present my own inventory of web-based malware stakeholders (b). This list is intended to be a comprehensive index of all categories of web-based malware actors. Next, I will introduce the concept of chain of trust, its underpinnings and its implications (c), and will develop one application of this concept to web-based malware. Although this illustration only applies to malicious software distributed on the Internet, it is meant to be representative of the larger malware phenomenon. I will describe each actor's interaction with the other links of the chain of trust and detail successful or unsuccessful attempts to strengthen this chain (d). Lastly, I will offer four main recommendations based on the findings of this report (e).

With 75 percent of connected North Americans, growing rates of Internet use around the world (Internet World Stats, 2009), and every computer at risk, these questions should not solely concern online security experts, but also the larger public of every country, or at least their governments. Mapping web-based malware is an important step to better understand the nature of the threat and contain it more efficiently.

It is important to note that this report is not meant to be exhaustive. While the list of malware stakeholders categories is my best attempt at compiling a comprehensive inventory of players having an interest in or an influence on the spread of web-based malware, the rest of this report only describes some illustrations of the chain of trust. Although I have chosen these illustrations because either I or the experts I have interviewed have deemed them representative, I do not claim these sections of the report to be .

Another important point to keep in mind is that the actor-focused framework adopted in this report is only one of several possible approaches one can use to better understand malware. Some commentators, including Internet security expert and former Network Solutions Chief Technology Officer (CTO) David Holtzman, whom I have interviewed, suggest that an action-focused framework would be more satisfactory in at least some ways. They contend that an actor-focused model might not be able to capture the nuances in each one of the stakeholders' actions and interactions, but rather definitively categorize them in a class that may reflect only the largest or the most visible parts of their actions. Besides, it is the action, rather than the actor, that defines malware.

While these are fine arguments, I have chosen to work on an actor-focused framework. In theory, any individual or organization, from the COTI to Google, from browser makers to consumer groups, could start spreading malware. In practice, however, enough time has passed and enough knowledge has been gathered since the apparition of malware that we can safely assume that the actor is a good proxy for the action. If we assume that any actor or organization could be the origin of malicious software, we would need to study each actor's actions, which would take considerably much more time and resources. Instead, I am using the actor as a proxy for its actions, a safe and useful compromise to study the world of malware.

When an actor did not belong to a single category (government is probably the best illustration of this), I listed it in all of the categories in which it could fit. Furthermore, an action-focused framework would be dangerously complicated to build and make sense of. In my

opinion, the same type of research conducted a few years ago should have considered using an action-focused model, but as time goes by, the relevance of using the actor as a proxy for the action increases rapidly. Even if web-based malware is in constant evolution, we have now entered a phase in which building an actor-focused framework is the most relevant option- at least, for my purposes.

Methodology

- Review of the current literature on web-based malware (mostly academic papers, news articles and reports). All of these resources were found online;
- Phone, e-mail, and in-person interviews:
    - Dr. Anirban Banerjee, Chief Security Officer, Jaal LLC;
    - Allan Friedman, post-doctoral fellow at the Center for Research in Computation and Society (Computer Science Department—Harvard University);
    - David Holtzman, social technology expert;
    - Tim Malin, New York City Police Department;
    - Jonathan Nightingale, Director of Firefox Development, Mozilla Corporation.
- The February 5, 2010 Chain of Trust Initiative meeting. Earlier this year, a dozen computer security and Internet safety professionals took part in a meeting set up in order to provide me with additional material and feedback for my research. Attendees included:
    - Justin Brookman, Senior Resident Fellow, Center for Technology and Democracy;
    - Robert Bruen, KnujOn;
    - Eric Davis, Head of Anti-Malvertising, Google, Google;
    - Michael Kaiser, Executive Director, National Cyber Security Alliance;
    - Tyler Moore, post-doctoral fellow at the Center for Research in Computation and Society (Computer Science Department—Harvard University);

- Brandon Palmen, Lead Web Developer, StopBadware;
- Mario Vuksan, independant consultant;
- Richard Wang, SophosLabs security expert, Sophos;
- Maxim Weinstein, President & Executive Director, StopBadware;
- Heather West, Policy Analyst, Center for Technology and Democracy.

In addition, I have received very helpful feedback and guidance from StopBadware's Maxim Weinstein.

Mapping web-based malware

The challenges of web-based malware

Once these definitional issues are resolved, one can start approaching the topic itself. Unfortunately, theoretical and practical obstacles to understanding—and fighting—malware are abound. I have chosen to focus on five challenges of malware that I think are particularly relevant to this report.

- The barriers to awareness

I have already addressed the users' lack of expertise with regard to malware. Most Americans do not assess the malware threat adequately, as shown by research data, and most Internet users who feel adequately protected are in fact at risk. This is caused by several barriers to awareness between the user and a safe Internet environment. Even if the wording is a little brusque, one might also think about these barriers as "layers of ignorance."

Although more than eight out of ten users have a security software[3] installed on their computer globally (Symantec, 2010), close to twenty percent of Internet users still do not protect their machines with any type of anti-malware software.

It goes without saying that not all "protected" computers are equally safe. The number of protections installed on the machine and the quality of these protected can vary wildly. It is easy for non-expert users to be confused by the plethora of protection software and services available nowadays.

Even the best anti-malware protection system will not be very useful unless it is used adequately. For example, updating one's AV software is critical to ensuring that one's machine is as safe as possible. It is also important that users not rely solely on anti-malware software to protect their computers from malware—other critical factors include using software that is secure in the

[3] Commonly called AV software, for Anti-Virus software. Even if this designation is technically not correct (virus is not equivalent to malware, since virus are a type of malware), it is used widely, including in this report.

first place, keeping software updated, and adopting appropriate user behaviors.[4] Besides, when an individual is not using his or her own computer- at work, for instance- a moral hazard factor is added to the user's lack of expertise. Even if he or she knows which practice is the safest, the user might avoid it because he or she feels like the risk is borne by somebody else. (This is of course an erroneous intuition, since the more computers are infected, the greater the likelihood that other computers or networks will become zombies, as discussed above.)

Even websites that appear legitimate can be a source of malware. Most commentators claim that government websites are not protected enough against malware and related types of threats. According to Websense, a web security company, between June 2008 and June 2009, "77 percent of Web sites with malicious code [were] legitimate sites that [had] been compromised." (Websense, 2009)

"Safe" is an ideal rather than a reality. A computer or a network cannot be 100 percent safe, because the nature of the threat is constantly changing.

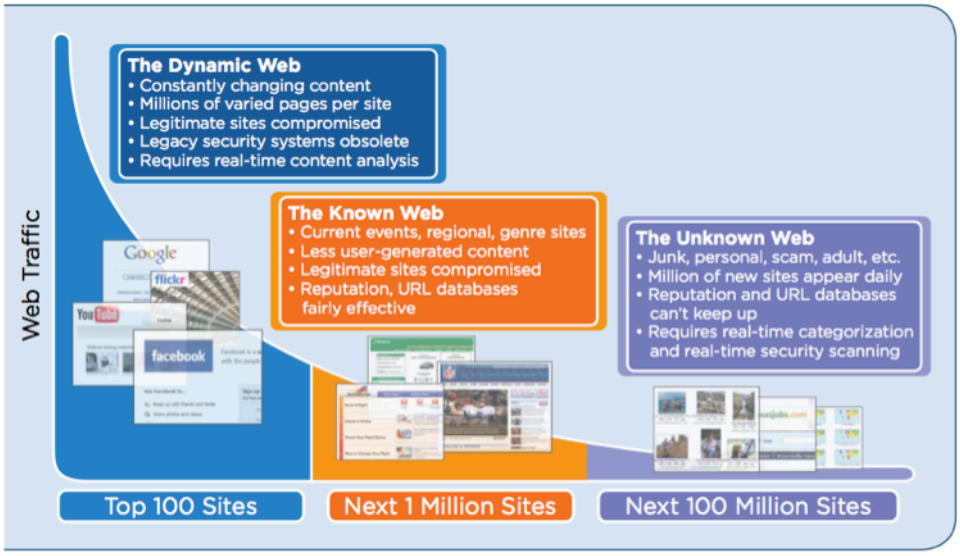
- An adaptive threat

Another important challenge is the fact that as AV software and other detection protection tools get better at fighting malware, cybercriminals come up with different and more sophisticated attacking techniques. This is a common problem in law enforcement, but poses specific challenges to the anti-malware community. If a category of actors, such as Internet Service Providers, decide to make an effort on malware detection, targeting all botnets on their networks, would it be easy for criminals to come up with more discreet web malware? In their 2008 paper, *Reinterpreting the Disclosure Debate for Web Infections*, Greenstadt et al. also describe how cybercriminals have adopted the theory of the long tail (Anderson, 2004), targeting thousands of low or mid-traffic websites instead of injecting malicious code in a few more reactive- and better protected- high-traffic online destinations.

[4] Examples of safe user behaviors include reading and complying with legitimate warnings or downloading content from trusted sources.

Over the last couple of years, a new type of threat has appeared on the web. Instead or targeting independent and isolated users, cybercriminals engage in large-scale data harvesting campaigns. According to the 2009 ScanSafe Global Threat Report, the most common victims of these "vertical threats"[5] are the Energy & Oil, the Pharmaceutical & Chemical and the Engineering & Construction industries.

The result is a fast-increasing number of infections and a growing risk for Internet users. In a survey of more than 440 companies and government agencies published in December 2009, the Computer Security Institute found that 64 percent of users reported malware infections, an increase of 50 percent from 2008. Each security breach represented an average loss of $234,000 for the vulnerable organization (Lohr, 2010). According to Websense, "61 percent of the top 100 sites either hosted malicious content or contained a masked redirect to lure unsuspecting victims from legitimate sites to malicious sites" in the first half of 2009. Over 50,000 new pieces of malware are released every day.



Websense, 2009

[5] These threats are called "vertical" because they target a large number of actors in specific industries.

- Virtual threats, material losses

Yet another problem for the anti-malware community is that it is fighting a virtual threat. It is extremely hard for most users to understand how networks of robots can infect their computers, how malicious code can be injected in legitimate websites, and how this can result in identity theft, and eventually, in material losses. In his essay, *The Psychology of Security*, computer security expert Bruce Schneier defines security as a trade-off, saying, "There is no such thing as absolute security[6], and any gain in security always involves some sort of trade-off." According to the American cryptographer, the main obstacle to a good assessment of a given risk is a lack of information: "The more your perception diverges from reality […], the more your perceived trade-off will not match the actual trade-off. […] A lot of this can be chalked up to simple ignorance."[7] Out of the five explanations for "bad information" listed by Bruce Schneier, three are extremely relevant to web-based malware:

- "People exaggerate spectacular but rare risks and downplay common risks." — Web-based malware is far from being spectacular – sometimes, it is not even noticeable to the user.
- "People have trouble estimating risks for anything not exactly like their normal situation." — Web-based malware, like the Internet itself, is a relatively new phenomenon. End-users have not had time to proceed to a 'cultural shift' and consider online activity as the "normal situation."
- "People overestimate risks that are being talked about and remain an object of public scrutiny" — Because web-based malware is a "silent" type of threat, it does not receive as much media coverage as other types of online (e.g., child pornography) or offline (e.g.,carjacking) threats. Thus, it is less of an "object of public scrutiny" than other menaces.

This is at least part of the reason why a large number of Internet users tend to underestimate online threats, including malware.

[6] I developed the same idea above, in "The barriers to awareness": "'Safe' is an ideal rather than a reality."
[7] Schneier does use the word "ignorance."

Yet, earlier this month, the Federal Bureau of Investigation stated, "online crime complaints increased substantially once again [in 2009]. …The Internet Crime Complaint Center (IC3) received a total of 336,655 complaints, a 22.3 percent increase from 2008. The total loss linked to online fraud[8] was $559.7 million; this is up from $265 million in 2008." According to the same report, " 'law enforcement relies on the corporate sector and citizens to report when they encounter on-line suspicious activity so these schemes can be investigated and criminals can be arrested,' stated Peter Trahon, section chief of the FBI's Cyber Division. 'Computer users are encouraged to have up-to-date security protection on their devices and evaluate e-mail solicitations they receive with a healthy skepticism.'"

- Public good v. business objectives

In addition to these serious challenges is the reluctance of some actors to maximize their anti-malware efforts in order to reduce costs. While most online stakeholders claim to be acting in favor of online security, for-profit entities can only do so to a certain extent. In some cases, the website owner's and the user's preference for less malware on the Internet do align, but Greenstadt et al. (2008) also note that web content providers tend to "conceal the risk that their websites pose to Internet users" and "to inappropriately externalize the costs of malware infection," thanks to the voluntary disclosure policy (Greenstadt et al., 2008). Website owners whose online content is infected have a counter-incentive to disclose that they are spreading malware on the web—doing so would hurt their reputation, their traffic, and eventually, their revenues.

In this version of the tragedy of the commons, companies typically do not invest in online security unless it affects their own profits directly. While it certainly makes sense for corporations to control their costs, this point of view does not help the production of an 'online security' public good and is based on a rather short-sighted rationale. Given the nature of malware and the way it hops from computer to computer, network to network, decreasing the *global* amount of malware is the only way to make a sustainable contribution to a specific website's security.

[8] Online fraud is not always malware-related.

- Assigning responsibility

The fifth challenge of web-based malware is a key element of this report. In just a few pages, I have already mentioned anti-malware NGOs, Government, malware removal companies, cybercriminals, Internet users, researchers, academics, creators of Internet standards, website owners, anti-malware software, and the companies that make them; these are all categories of malware stakeholders, but there are many more.

Given that the field of web-based malware is so vast and complex, what resources can be designed in order to better represent the actors in the world of web-based malware and the interactions between them?

An inventory of malware stakeholders

One of the most important steps of my research was to compile a comprehensive list of all the categories of web-based malware stakeholders—individuals or organizations that have an interest in or an influence on the spread of web-based malware. As pointed out by a recent Internet Corporation for Assigned Names and Numbers (ICANN) draft working group report, "the Internet is a huge and sprawling environment that crosses international borders. It is decentralized by design, and involves millions of parties all exercising ownership of or control over various assets and infrastructure. […] All of these parties are vulnerable to and are often leveraged by criminals. As a result, no one party—and no one type of entity—has the power to solve the problem of e-crime alone. Indeed, security experts agree that e-crime[9] cannot be solved–it can only be fought, and hopefully contained, just like offline crime." (ICANN, 2010)

[9] It is worth noting once again that web-based malware is only a portion of online crime.

Three major groups appear in this comprehensive inventory (appended to this report—page 48):, (a) the actors fighting malware, (b) the channels of malware, and (c) malicious actors.

(a) While some of these actors specialize in cyber activity and are not relevant outside of the Internet world, others, like business organizations or the press, carry an offline role too. While some actors focus exclusively on malware, others do not. Each player's specific motivations might not always be aligned with the rest of the players, or with the global goal to reduce the amount of malware in circulation, especially among private actors—competition between these actors might favor or hinder anti-malware efforts, depending on the context;

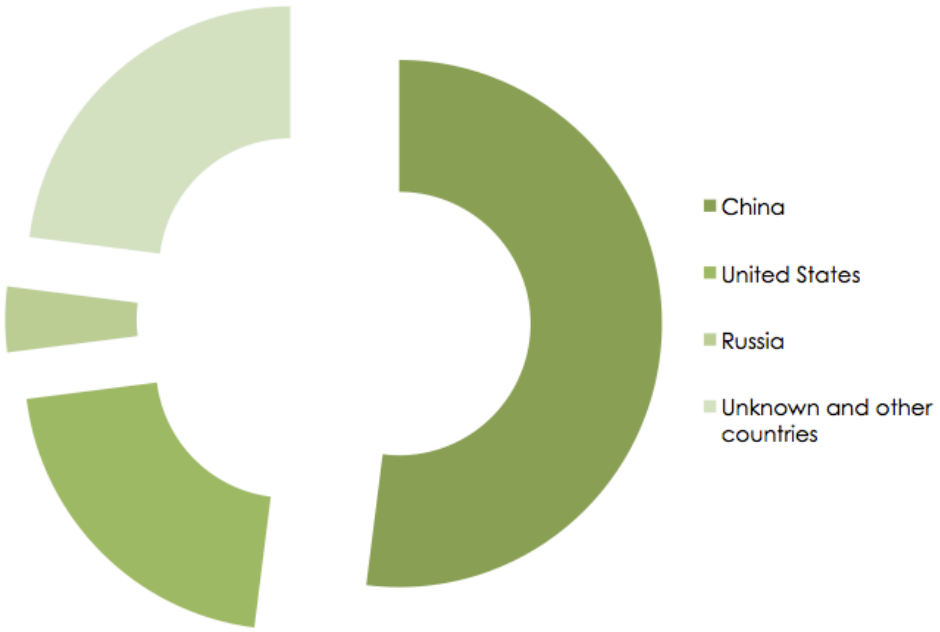
(b) By definition, all actors in this group belong to the computing or Internet world. While my research focuses on web-based malware, it was important to include non-web channels of malware transmission (such as e-mail or portable media) to show that the distinction between web-based malware and other types of malware is porous. Some of the stakeholders in this group were also in group (a), which means that these institutions, including government (whose fundamental purpose is the maintenance of basic security), might be fighting malware and facilitating it at the same time. More inter-agency and inter-department cooperation is thus required to make these actors' situation coherent;

(c) The presence of rogue marketplaces and of black market operators in this group shows that web-based malware is in practice linked not just to other illegal online activities, but also to offline criminal organizations and individuals. Government is also part of this group. This includes rogue governments (to this day, it is still unclear what the role of the Chinese government played in the January 2010 controversy) and governments which have not set a law enforcement structure able to contain and control the activities of cybercriminals. Representing the actions of government in the chain of trust is challenging because its role varies widely, depending on the country, the context, or the specific governmental actor being considered. This goes back to

the actor vs. action dilemma (see *Mapping web-based malware?*, page 15) . While creating a specific category for government in this inventory of malware stakeholders was option, I chose to include in all three categories—actors fighting malware, channels of malware, and malicious actors—in order to show both the multifaceted nature of public institutions with regard to web-based malware and their capacity to be strong influencers. My point is not to say that all governments act like or have close links to malicious actors (clearly, this is not the case), but rather that while the fundamental purpose of government is the maintenance of basic security and public order, it is not always the case that public institutions effectively address public security issues like web-based malware.

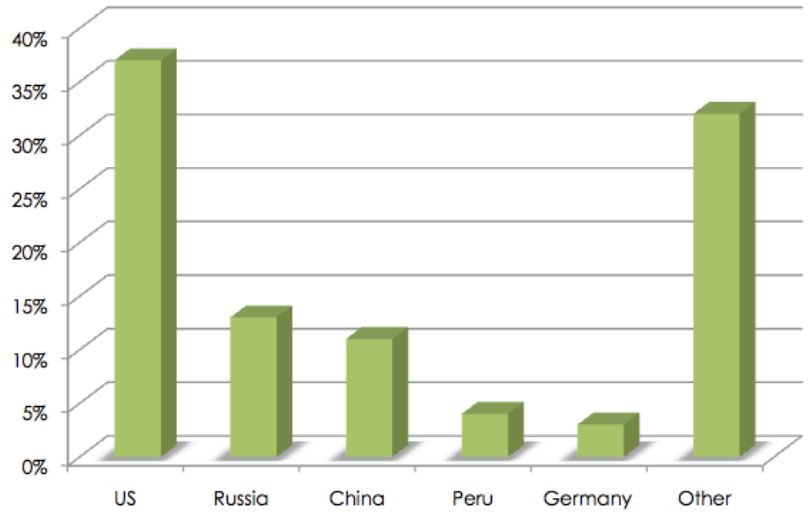
Top Malware
countries in May 2008

StopBadware, 2008



Top Malware countries in 2009

Sophos, 2010



Malware is said to originate from a certain country when the website that distributes malware (either because it is a malicious website or because it is the victim of an exploit) is hosted in that country. Of course, cybercriminals can attack a website that is hosted in a country different form theirs, so the country of origin of malware probably tells us more about the target or the hosting companies' and governments' commitment to taking down and cleaning up malware sites than about the criminals themselves. According Sophos security expert Graham Cluley, "much emphasis is given in the media to cybercrime and hacking attacks originating from China. But you need to remember that just because the malware is planted on the web in these countries doesn't necessarily mean that the hackers themselves are based in the same place" (Sophos, 2010). That is why the sharp increase in the amount of malware originating from the United States between February 2008 and December 2009 (from 10 percent to 37 percent) does not mean that the relative share of US criminals has grown in this 22-month span.

Because of the transnational nature of the threat ("the Internet is a huge and sprawling environment that crosses international borders," says the ICANN, and so is web-based malware), it makes it very hard to use traditional country-specific law enforcement structures to determine who should be in charge and to effectively fight malware.

Once again, it is extremely difficult to assign responsibility to a specific actor or group of actors—except for cybercriminals, of course.

MAIN FINDING # ONE:
An extremely large number of individual and collective actors have an interest in or an influence on web-based malware. Their preferences are not always aligned, even when they are theoretically trying to achieve the same goal. Expertise and motivations vary wildly among these groups. In this system, the number and the diversity of these stakeholders makes it is extremely hard to assign responsibility in any clear or constructive way.

Drawing chains of trust

Given this first conclusion, one has to find alternate ways to comprehend the world of web-based malware. What are we trying to achieve, and what is the main obstacle to this goal?

The early sections of this report insist on the idea that assigning responsibility to specific actors or group of actors is the major problem in containing the spread of this electronic scourge. The following sections will demonstrate how constructing chains of trust (including what I will call the web chain of trust) is a helpful tool to better understand web-based malware.

In this report, I am using the concept of "chains of trust" both as a representation of the current state of web-based malware and as a means of demonstrating what steps need to be taken to reach the common goal of the anti-malware community: a safer web for every type of user.

Before I describe the web chain of trust in detail, let me clarify the implications of a chain of trust. In my opinion, a chain of trust requires four principles: (a) awareness, (b) willingness to cooperate, (c) dialog, and (d) coordination.

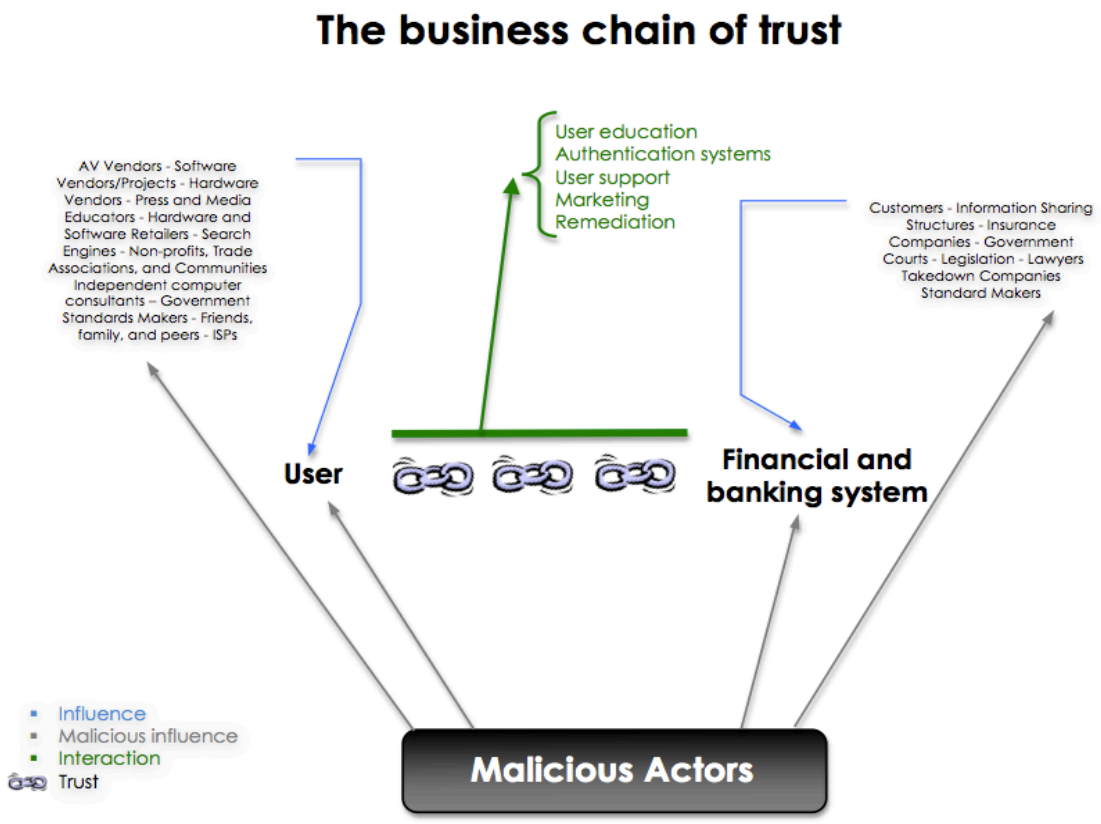
(a) Awareness – each player has to be aware of the existence and of the role of as many other members of the chain of trust as possible, which at a minimum includes those players that are nearby in the chain of trust, within the player's sphere of influence, or that are influenced by the actor in question. I have already shown that this is a huge challenge in the world of web-based malware because of the large number (appendix 2 lists more than 50 categories of actors) and diversity (every user has his or her own online behaviors) of the stakeholders involved;

(b) Willingness to cooperate – once the actors are identified, they have to be willing to working with each other. This is an equally changing piece of the problem, as has been demonstrated above (non-aligned preferences or goals);

(c) Dialog – dialog is critical to ensure that at any point in time, all parties have the maximum amount of knowledge of what the other actors are trying to achieve, both why and how. This is of course not always possible because some actors (for instance, two rival AV software companies) have competing goals and because dialog takes away resources from the actor's primary objective;

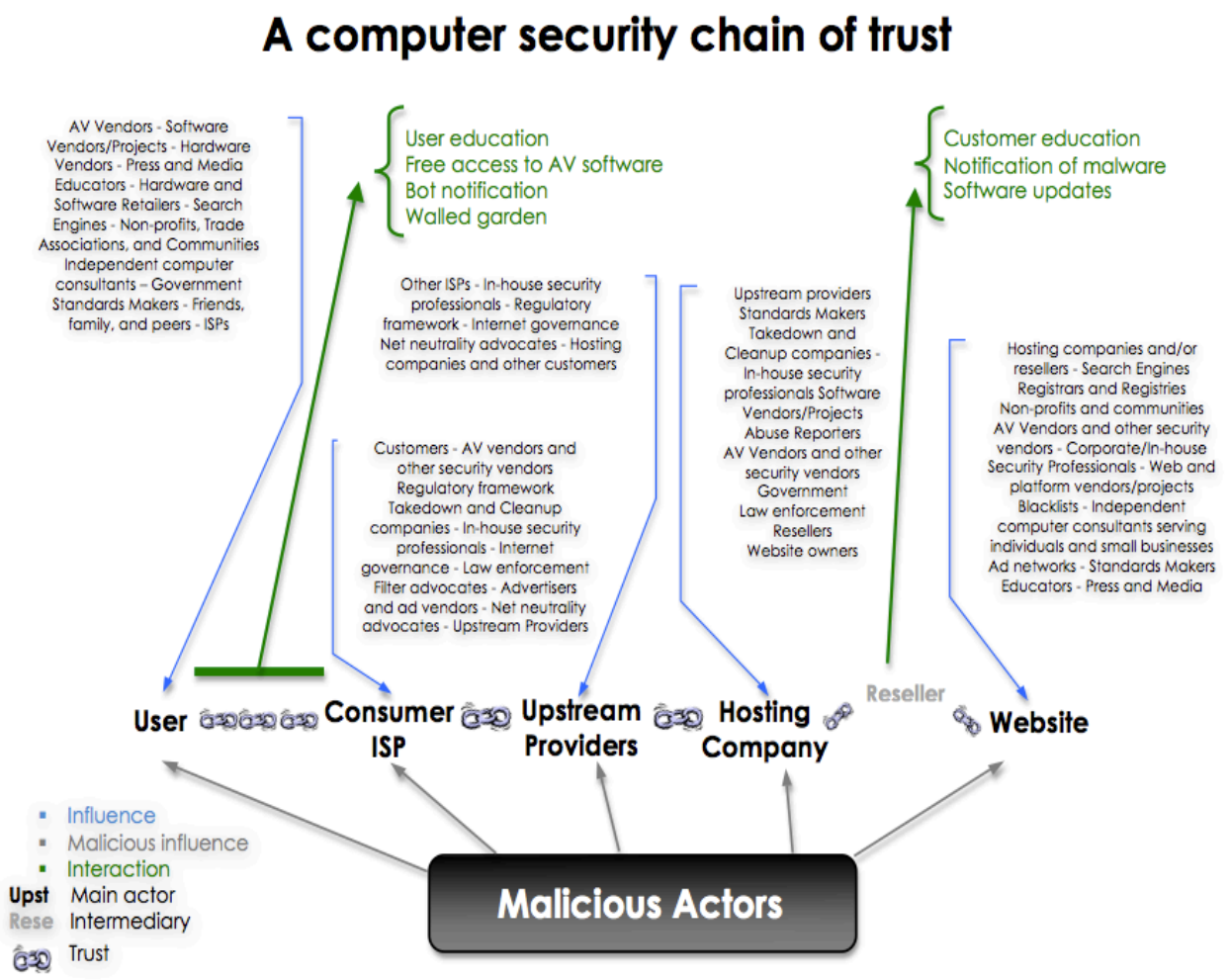
(d) Coordination – in this framework, coordination is different from dialog in that it refers to the exchange of external information (for example, the latest pieces of malware spotted on the Internet) rather than the actors' own goals and activities.

The business relationship between users and the financial and banking system is a straightforward example of a chain of trust. The following visual shows the influencers of both actors and the most relevant interaction between the two for our purposes (user education and authentication systems).



A computer security chain of trust

The same concept can be applied to the entire Internet from the perspective of web-based malware. The following visual makes sense of a large number of actors and shows the interactions between them, insisting on the five most important stakeholders from the point of view of web-based malware: end-users, Internet Service Providers (ISPs), upstream providers, hosting companies, and websites (as well as their owners). The visual itself is a critical part of this section, but in the next few pages, I am going to describe a few specific examples of influences and interactions on the computer security chain of trust.



- End-users

One of the most crucial teachings of the chain of trust framework is that end-users are subject to a tremendous number of influences and can potentially interact with an enormous number of actors. As pointed out above, end-users are "low-bandwidth actors," which means that they easily reach information overload in the context of computer security. One cannot insist enough on the challenges that navigating the available information about malware effectively represents. Beyond this overwhelming number of sources, the technical nature of the information is also a barrier to comprehension for most users, and as I have stated above, the influences at play in the chain of trust often point in different directions, which only adds to the confusion of the

average end-user. Given this state of affairs, each user can adopt one of several behaviors. Some give up and either consider online security a non-issue or regard it as a threat they absolutely cannot fight. Others ask around and search the web for easy-to-understand information with regard to computer security. This category of users could largely benefit from the creation of an "online security culture" and from a certain centralization of information (or the duplication of the same tips and pieces of advice on multiple online locations). Others might look to authorities deemed competent and trustworthy, like Internet Service Providers, to help them improve the security of their machine and network. This specific interaction is studied in detail below.

- ISPs

Internet Service Providers are in the business of their customers with access to the Internet.[10] Connection speed, data transmission technology, and other characteristics of the offer can vary widely from one provider to the other and from one type of customer to the other.[11] Because they want to provide a safe Internet connection to their customers, ISPs work with third parties like takedown and cleanup companies to ensure a satisfactory level of malware protection on their infrastructure.

- Upstream providers

Consumer ISPs are in fact an intermediary between the general public and other ISPs, often called upstream providers, who provide Internet access to consumer ISPs and their clients. The relationship between ISP and upstream provider is extremely complex and often involves more than a mere linear connection between the two, depending on the number of Points of Presence of a given ISP and on the number of upstream providers used by this ISP, among other factors.

[10] In some cases, Internet access is part of a 'bundle,' typically including landline telephone, television, and cable services (triple play.)
[11] Especially between individual and corporate customers.

- Hosting companies and resellers

Instead of storing website data on their own machines, website owners often use web hosting services, whose scope and rates vary widely, depending on the needs of the website owner. Typically, web hosts own (or lease) a large number of servers in a data center, which is connected to the Internet and where the host can easily monitor connections and security systems for a large amount of data.

Because reseller web hosting (a practice in which an individual or an organization purchases the host services and then resells them to other customers for a profit) makes the chain of trust longer, and the responsibility of content harder to establish, reselling is a favorable environment for bulletproof hosting (bulletproof hosts do not apply any sort of filter on the content being hosted—whether it is a serious blog or dubious online gambling—and do not take servers offline even when they receive complaints with regard to the content being hosted) or "negligent hosting," where hosts or resellers do not prioritize security and do not respond to takedown requests or other abuse notices in a timely fashion.

- Website owners

Online security is not a priority for all website owners. In recent years, it has become increasingly easy to start a website to share thoughts and multimedia content or to publicize a project. For all these website owners, the cost (in time and other resources) associated with keeping their websites secure is often quite high compared to the overall resources they devote to their websites. On the one hand, platforms like Blogger and Wordpress,[12] which make creating a blog an option to anyone with an Internet connection for free, are easy targets for malicious actors since most of their users have very little technical knowledge of anti-malware protection strategies and often do not realize their website has been compromised until months after the

[12] See Krebs, B. (2010) Hundreds of Wordpress Blogs Hit by 'Networkads.net' Hack (http://krebsonsecurity.com)

attack. On the other hand, these organizations can provide assistance to end-users, monitoring aggregate traffic on their site and potentially alerting them when they suspect malicious actors have launched an attack.

Individual website owners tend to be influenced by the same types of actors as end-users (it is hard to imagine how a website owner could not be an Internet user as well), but collective website owners, like businesses or government agencies, are also influenced by independent and in-house security professionals. Another important interaction exists between website owners and blacklists, since no company or organization (or even individual website owners, for that matter) wants to see their website blacklisted—end-users would then avoid their site, through search engine warnings or directly through the blacklist (for users who actually consult it)—in some instances, blacklisted websites also get press coverage, thus the media might be an intermediary too.

- The End-user/ISP interaction

The interaction between end-users and ISPs is a critical part of the computer security chain of trust. Over the last few years, ISPs have developed a number of activities and programs in order to strengthen the chain of trust. The case of bot notification is particularly noteworthy. As stated by Leslie Harris, President and CEO of the Center for Democracy & Technology on Comcast's blog Comcast Voices:

> proactive notification is a helpful step on the part of Comcast to address what is often the weakest link in online security: users. Most ISPs monitor their networks for spam and viruses, and some offer their subscribers security software for an additional monthly fee. However, at the time of this writing, Comcast is the first major U.S. Internet service provider to actively reach out to individual users plagued with malware

> as a free, routine part of its subscriber security services. The vast majority of consumers do not even know what bots are; let alone how to fix their computers if they are saddled with one. With initiatives like Constant Guard[13], that could begin to change.

More details on the technicalities of this system can be found in *Example of an ISP Web Notification System*, a draft memo published online by the Internet Engineering Task Force (IETF) on March 5, 2010. Because the authenticity of the notice itself might be questioned by users who take the time to read it, one of Comcast's main challenges is to come up with a way to let the user know that he or she is not being duped by yet another deceiving alert. While the ISP has tried to resolve this challenge joining a "How do I know this notice is from Comcast?" link with the notice, including this information in the user's monthly bill would certainly be a better option (even if a direct consequence of using this course of action is that bot issues are resolved after a few weeks in the best case scenario).

Another encouraging example is the Australian Internet Security Initiative (AISI). Developed by the Australian Communications and Media Authority (ACMA), a governmental agency whose responsibilities include regulating Internet content standards, the AISI was launched in late 2005 as an attempt at controling the spread of malware on Australian computers and networks. The AISI represents a substantial improvement of the application of the chain of trust principles discussed above (willingness to cooperate, dialog, and coordination especially). Through this program, the ACMA collects data about patterns of aggregate online behaviors and provides daily reports to ISPs, who can then notify their customers of the potential presence of malicious software on their machine or network and help them resolve the issue. Over seventy Australian Service Providers participate in the program,[14] which they can enroll in for free.

Two related developments are worth mentioning in this report. First, the Internet Industry Association (IIA), a coalition of Australian Internet businesses, is currently preparing what it calls a

[13] A free Comcast program that promotes online security through people, technology, and education.
[14] According to the ACMA, "over 90 per cent of Australian residential customers of internet services are covered by these ISPs." (2009)

"security code to protect Australians online." Like the AMCA's program, the code focuses on zombie detection, user notification, and malicious software removal, but also adds a fourth dimension: encouraging ISPs to "report repeated or severe instances of suspicious activity to relevant Government agencies, where it is believed the suspicious activity constitutes a serious threat to Australian communications networks" (IIA, 2009). A draft copy of this ambitious attempt at self-regulation suggests that ISPs "*should* attempt to identify the end user whose computer has been compromised, and contact them to educate them about the problem." Of course, the use of the word "should" by Australian ISPs themselves (members of the IIA include major ISPs like Optus, Telstra, Vodafone, AAPT, Virgin and Hutchison 3G) is very meaningful. It seems to indicate that they are committed to taking a very active part in the fight for a "a faster, safer, fairer, more trusted internet in Australia" (which is, according to IIA Chief Executive Peter Coroneos, the mission of his organization). The code, on which users could comment for a couple of months in late 2009 and which is expected to come into effect later this year, also states that ISPs should provide users "with a timeframe in which to take remedial access and, if this is not adhered to, terminate service," although this option would only be chosen in the "most extreme of cases."

Second, it is important to note that this local action inspires other initiatives at the global level. The International Telecommunications Union used the AISI as a base for its Botnet Mitigation Toolkit, which "seeks to raise awareness[15] among Member States of the growing threats posed by botnets and the linkage with criminal activities" (International Telecommunications Union, 2008).

Besides, some ISPs, like Plata in Japan, have used data on the average user's lack of expertise as the starting point of the anti-malware strategies that require a minimal level of improvement from the user by default (most experienced users can customize the service provided by the ISP and take a more active part in the protection of their network and machine). According to Japanese ISP director Katsumi Nagata, in the realm of online security, "a potential solution is useless unless it is made the default or offered free of charge. We wanted to make a system in which our least-experienced users can be protected from the outset" (Cisco, 2010). His

[15] Awareness is the first of the chain of trust principles.

company, Plata Networks, worked with network infrastructure giant Cisco to offer URL filtering and packet filtering service to all users (URL filtering is a core part of network security that prevents access to unauthorized or malicious web sites) making it possible to protect users from network threats regardless of each individual's knowledge or skills.

Other ISPs develop online security user education programs. Besides its extensive partnership with Symantec, proudly presented in the "Get Protected" section of its website (which is not directly accessible through the Comcast.net portal, however), Comcast provides an inventory of the 10 things users should do in order to maximize their information and their computer's protection. This easily printable checklist is quite a helpful resource and is rather condensed compared to Microsoft's gargantuan Consumer Security Support Center. Other organizations, such as AV software vendor Symantec, use easy-to-understand and humorous videos ("Symantec guide to scary Internet stuff") to explain a large number of malware-related concepts in less than three minutes.

- Other influences on end-users

Search engines can also largely influence end users' perceptions and behaviors. Almost four years ago, Google, which now "holds a commanding 65 percent market share and is still the only company whose name is synonymous with the verb *search,*" (Levy, 2010) introduced a warning in search results when it finds a website to be potentially harmful. Google partnered with StopBadware to help educate the end user, as well as the owners of the affected websites, about these harmful threats.

Web browser companies are equally influential partners for end users. Johnathan Nightingale, director of Firefox Development at the Mozilla Corporation, says that the company does not "have the power to unilaterally knock malware off the internet," but that instead it equips its users "with the tools to defend themselves. The single best thing we can do is producing a secure piece of regularly updated software that resists exploitation, and our track record there is

quite strong. Because we do not claim perfection, though, we also ensure that our users get regular updates to in-browser malware and phishing blocklists so that they never visit likely attack sites in the first place." Mozilla has developed a Safe Browsing partnership with Google, creating an anti-phishing extension to Firefox that alerts the user if a web page appears to be asking for personal or financial information under false pretences and anti-malware warnings.

Another extremely important source of influence on end users is the AV software industry. Indeed, the language and concepts these actors use largely shape the users' perceptions of the threat; AV software is thus both an action and an education medium. While the mere existence of an AV industry underlines the reality of the threat, AV software tends to have risk-inducing consequences as well. Most users think it only takes installing anti-malware software on one's computer to be protected against malware, but as I have made clear above, this could not be more wrong. This part of the chain can be reinforced by competent and conscientious hardware and software, whose advice is often extremely helpful.

- Web hosts, resellers, and website owners

Hosting companies are another example of upstream service providers, and one of the best illustrations of their role in the chain of trust- the McColo takedown- occurred in late 2008. McColo, a San Jose-based web hosting provider, served as a gateway for a significant portion of the world's junk e-mail. About half of the spam sent through botnets hosted by McColo were ads for male enhancement drugs and similar kinds of products (Krebs, 2008). Two providers (Global Crossing, a Bermuda-based company with U.S. operations in New Jersey, and Hurricane Electric, a company headquartered in California) cut off McColo's connectivity to the Internet after investigations by the Washington Post shed public light on the web hosting company's activities. "Immediately after McColo was unplugged, security companies charted a precipitous drop in spam volumes worldwide. E-mail security firm IronPort said spam levels fell by roughly 66 percent," stated journalist and computer security expert, Brian Krebs. Yet, in April 2009, Symantec published

a report showing that "levels of spam [were] approaching the dizzy heights they [had reached] before the sudden shutdown of rogue hosting company McColo" (one of the leaders in the bulletproof hosting market) six months before (Harris, 2009). In the long run, a single takedown is sufficient to fix the malware issue.

Bulletproof hosting is also sometimes used by actual malicious actors who actively seek to prevent malicious content from being taken down by moving it from one server or network to another, for instance. Indeed, resellers are typically smaller actors, which means that they may not have the resources to invest in security. Besides, resellers are not always easy to identify by security professionals who may see an upstream provider as the host of record, and upstream providers may not apply as much pressure on the resellers to deal with security threats as if they were storing the data themselves. While some hosting companies do try to engage in some notification and education efforts, reselling provides a weak link in the chain of trust for unscrupulous website owners or bot herders to spread malware.

MAIN FINDING # TWO:
Using the chain of trust concept, it is possible to make sense of the comprehensive list of malware stakeholder categories presented in this report. The web security chain of trust shows major actors, influencers and interactions in the world of web-based malware and gives helpful insight into what parts of the chain can and should be reinforced (user-ISP and web host-website owner links in particular).

Recommendations

Building on the main findings presented above, the last section of this report puts forward the four most critical issues that the Chain Of Trust Initiative (COTI) should address and what course of action should be followed in order to "to stem the rising tide of malware" (StopBadware, 2009). My recommendations are clearly associated with the problem it seeks to resolve and will be introduced in order of increasing feasibility.

MAIN FINDING # THREE: A large number of web-based malware stakeholders, especially end-users, lack expertise on the subject. This lack of familiarity with web-based malware leads actors to understate the threat that it creates.

Recommendation 1: Recognizing the fact that not everyone can become an expert, the COTI should maintain and further its educational outreach, extending the chain of trust findings to all types of stakeholders:

- Who are the actors?
- When do they interact?
- What is my role in the chain of trust?
- How to establish responsibility?

End users:

COTI members have already compiled a large amount of data on user expertise (or lack thereof), specifically regarding the NSCA. The COTI should now publicize the main chain of trust findings, in particular, the answer to the question, "What should I do to protect my information and my computer online?"

- The message should be simple. Extensive data shows that end users have a *very* low bandwidth when it comes to online security advice (or any expert topic, for that matter). The COTI's recommendations should not be more than five in number and might include things such as "update your security software regularly," "back up your hard drive," and "secure your wireless network."
- Those who are messaged should respect four criteria to maximize efficiency: relevance to the users' needs, easily comprehensible, easily applicable, and objective.
- Because the end users' bandwidth is so low, the COTI might focus on answering the question, "What should I do to protect my information and my computer online?" but should provide additional information about the concept of chain of trust and its application to a secure web for interested users.
- The COTI should adopt an aggressive public relations stance and relentlessly try to disseminate this message with the help of its large number of partners and supporters (the specifics of message might be agreed upon with the partners). Although members of the COTI are already working on public relations, this effort should insist on the chain of trust paradigm, should make sure to lead a coordinated campaign with *one* message that satisfies the four criteria above, should take advantage of the increased presence of malware in the public debate, and should increase the idea of responsibility on end users and ISPs, given that some have already investigated ways to make the fight against malware more efficient (especially on bot detection and notification).
- The COTI should work on the creation of a "culture of online security." Fiction works (for instance, YouTube videos) or online games might be used to create an environment in which security on the web feels as intuitive as security on the road. K-12 education should be particularly instrumental in this task. Technology coordinators, school administrators, and teachers (100, 97 and 95 percent, respectively) agree cyberethics, cybersafety, and cybersecurity curriculum should be taught in schools (NCSA, 2010). The goal of this effort should be to make all users ask for security features when they purchase an online service

or software the same way they ask for useful features and attractive prices today. Safety features are one of the major selling points in other industries—one would never buy a car on aesthetic and cost criteria only. Hopefully, this concern for security will develop in the computer hardware and software industry too.

Consumer webmasters:

- The COTI should relay the same message when targeting consumer webmasters. However, they might add additional details about the online security chain of trust and insist on the responsibility of website owners and web hosting companies.

Policy Makers:

- The COTI should not try and stimulate or influence regulatory and legislative production, but rather should educate policy makers, making sure they are familiar with the chain of trust framework and its main findings.
- The COTI should facilitate a public debate on computer security and malware in general. On March 3, 2010, at the annual RSA cryptography and information security conference in San Francisco, Michael Chertoff, former United States Secretary of Homeland Security, declared: "The government can start by talking more openly about cyber issues, thus raising awareness of the dangers that exist; the private sector needs to develop security systems that are easier to use and do not require people to remember twenty different passwords. Biometric devices that recognize a person fingerprint are a step in the right direction" (Wall Street Journal, 2010). Thus, engaging public leaders is only part of the solution, but it is an important element for the COTI.
- Making the threat more concrete will be a determining factor in the COTI's approach to policymakers outreach.

MAIN FINDING # FOUR: A major obstacle to fighting web-based malware is that it is not concrete enough. Different aspects of the malware threat (for instance, the fact that a large number of intermediaries and influencers can make the chain of trust weaker, or the fact that web-based malware are "silent" attacks) make it too abstract for some actors to realize the risks with which it is associated.

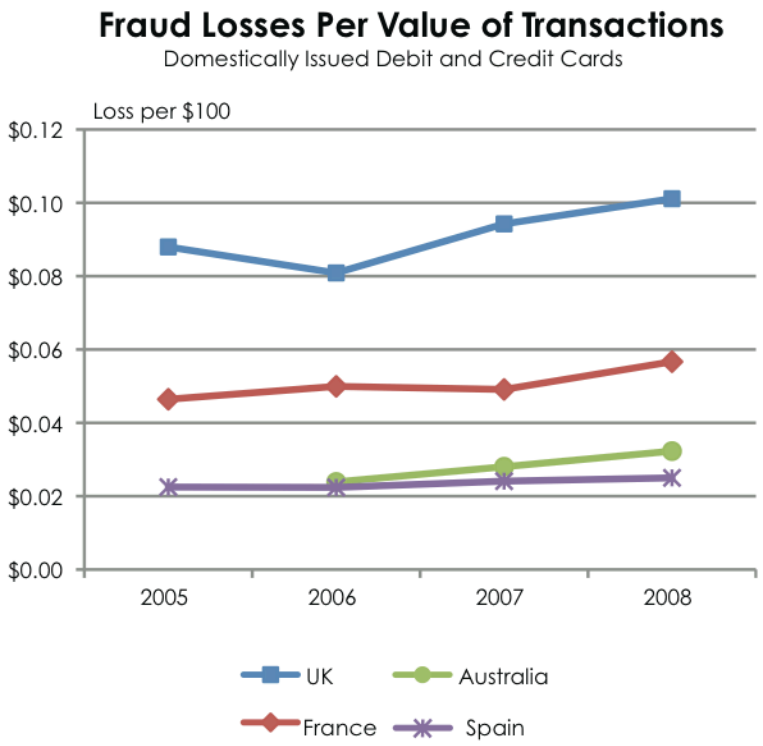
Recommendation 2: The COTI should make both the reality and the perception of web-based malware more concrete.

A fast-increasing number of operations happen online. Today, even in what are called "virtual worlds," users can meet, converse, work, and exchange ideas and money, and replicate so many of the material world's actions that one might question the distinction between "real" and "virtual." Nevertheless, for most users, what happens online is still not perceived in the same way as what occurs in the "real" world. 44 percent of US computer users say the possibility of being cybercrime victim has not changed their online behavior (Zogby, 2009). The COTI needs to increase the relevance and the urgency of the web-based malware threat by making both the reality and the perception of web-based malware more concrete, targeting end users and policymakers in particular.

- On April 21, 2010 StopBadware launched its StopBadware Stories, an extension of the BadwareBusters online community that seeks to put a human face on the malware threat. This effort needs to be deepened. Stories are currently now easily accessible through the BadwareBusters website, but this should eventually be extended to other COTI members and other partners' websites;
- The COTI also actively help and publicize the law enforcement improvement in terms of malware. "The worlds of law enforcement and justice have had about a decade to deal with highly organized and financially motivated cybercriminals. We finally have nearly universal recognition among global governments of the severity of this problem, and we can see significant progress from these years of relationship building, education, and

training among international law enforcement organizations. This progress has been slow in coming but we now see clearly demonstrated to criminals that engaging in cybercrime has become an activity with a rapidly increasing risk of incarceration, regardless of their country of residence" (McAfee, 2009).

- The COTI should promote increased transparency with regard to online financial fraud in the United States. "A lack of [financial fraud] statistics for the United States [...] makes it difficult to get a sense of the dimension of the problem" (Sullivan, 2009). In several western countries, including Australia, France, Spain, and the United Kingdom, useful information on payment fraud is collected and made publicly available.



When disclosed, these statistics can reveal more details, such as higher risks in certain transactions and in various locations. For example, because only 20 percent of individuals order goods over the Internet in Spain, compared to 57 percent in the United Kingdom, Card-Not-Present transaction fraud is much more prevalent in the UK than in Spain.

MAIN FINDING # FIVE: Large improvements are needed at an institutional level to enhance awareness, willingness to cooperate, dialog, and coordination.

Recommendation 3: The COTI should lead several initiatives to promote institutional improvement in the anti-malware community, on threat names, coordination, and standards, especially.

- The COTI should promote the creation of an international and independent authority which main task will be to name malware threats, or, at least, to recognize, label, and coordinate response to the big trends. The Conficker Working Group is a good example of a private industry effort in this area. Yet, a more institutionalized approach to this kind of initiative would be helpful. Rather than relying on ad hoc groups, this strategy would allow an industry-wide and coordinated surveillance, labeling, and response effort. While increasing cooperation and coordination between AV developers is demonstrated by joint efforts to name massively distributed malware unanimously, there is no official *and independent* body that decides on the names for cyberattacks. Introducing such an authority would both facilitate the comprehension of the world of malware by outsiders and underline the public nature of each threat. Indeed, a piece of malware should not be associated with the first AV company that detects it or names it, but rather should be given a universal name in order to make the dimension of collective responsibility on the malware debate clearer to all users.
- The COTI should promote increased coordination between key actors, even when such coordination seems hindered by each actor's individual interests. For instance, AV software companies do not systematically share data about known attacks with the rest of the anti-malware community, let alone with their competitors. While remaining entirely independent, the COTI should develop an enticing structure and strong partnerships to encourage private actors to share data about known attacks. Sharing this information with

the larger public (including competitors) is of course a more challenging question that deciphering proprietary data from information that should be made public. The most promising route to more coordination probably is self-regulation, a rather common *modus operandi* in the Internet industry. The COTI should push AV software companies and other members of the chain of trust to discuss a code in which all parties would agree to make attacks public as soon as they exceed a certain number of compromised computers or networks. In these negotiations, the role of consumer groups will be crucial. As an intermediary between the general public and the anti-malware community, they will both help convince private actors they should release as much data as possible and help create and diffuse a culture of online security in which AV software companies have a moral duty to share critical information about malware just like pharmaceutical company have a moral obligation to share any piece information that could fundamentally affect public health.

- The COTI should stimulate and promote the action of standard bodies like the Anti-Malware Testing Standards Organization (AMTSO) or the Institute of Electrical and Electronics Engineers' Industry Connections Security Group (IEEE ICSG). The chain of trust framework should be introduced to these bodies, and standards should be defined for each link of the chain.

MAIN FINDING # SIX: The reality of the world of web-based is still far from the ideal set by the web chain of trust.

Recommendation 4: The COTI should work to reinforce the chain of trust by eliminating weak links and increasing transparency.

- The COTI should push for a stronger chain of trust, enticing its members and partners to work towards a more robust end user/ISP relationship, through bot notification or an initiative similar to the AMCA's Australian Internet Security Initiative (AISI) and Australia's Internet Industry Association code in the United States and abroad.
- On top of the efforts needed to enhance coordination, as described in recommendation 3, a more general move towards increased transparency will be a key element to strengthen the chain of trust. Not only should actors who are engaged in the fight against web-based malware share data about know attacks, they should also strive to be as transparent as possible with regard to their specific actions, agenda, and resources. Moving towards a more open community will have at least three beneficial effects. First, it will increase awareness (as defined in *Drawing chains of trust*, page 24) and opportunities of collaboration. The more information available about each actor, the easier it is for other actors to adapt to their actions and be as efficient as possible. Besides, increased transparency will make the concept of chain of trust and its incarnation in the anti-malware community easier to grasp. Finally, it will facilitate the identification of potential "weak links" which are expected to be more reluctant to openness than stronger links.
- The COTI should work towards the elimination of weak links in the chain of trust in general. The notion of responsibility should surpass an actual legal responsibility to protect users from unwanted software. This battle will eventually come to pass.

Conclusion

Earlier this year, the ICANN draft report cited above expressed a seemingly plain- but in reality insightful- view on the malware dilemma: "In the end, all responsible parties have a role to play. Collaboration, data sharing, and education are effective and important tools for dealing with Internet security problems." (ICANN, 2010)

In order to better represent the world of web-based malware, its strengths and its weaknesses, and also opportunities for improvement, this report applied the chain of trust framework to all the actors involved in the field. The recommendations derived from my findings come to the same conclusion as the ICANN did: all parties have a role to play and bear their own share of responsibility, as demonstrated by the chain of trust paradigm. Hopefully, my findings and recommendations will help the COTI and its partners start stemming "the rising tide of malware" and make the Internet safer for all users.

References

Anderson, C. Wired Magazine, October 2004. *The Long Tail.* Retrieved from http://www.wired.com/wired/archive/12.10/tail.html

Australian Communications and Media Authority, December 2009. *Online risk and safety in the digital economy.* Retrieved from http://www.acma.gov.au/scripts/nc.dll?WEB /STANDARD/1001/pc=PC_311304

Business Week. (2006, May 29). *Meet the Hackers.* Retrieved on March 13, 2010 from http://www.businessweek.com/magazine/content/06_22/b3986093.htm?campaign_id=bier_tcm

Cisco. (2010). *Japanese ISP Applies Service Control Solutions for Secure Broadband Services*. Retrieved on 2010, April 25 from http://www.cisco.com/en/US/prod /collateral/ps7045/ps6129/ps6133/ps6150/prod_case_study0900aecd80419db4.html

Clinton, Hillary R. (2010, January 21). *Remarks on Internet Freedom.* Retrieved from the U.S. Department of State website: http://www.state.gov/secretary/rm/2010/01/135519.htm

Federal Bureau of Investigation (2010, March 12). *IC3 2009 Annual Report on Internet Crime Released*. Retrieved on 2010, March 20 from http://www.fbi.gov/pressrel/pressrel10 /ic3report_031210.htm

Greenstadt, R., Day, O., & Palmen, B. (2008). *Reinterpreting the Disclosure Debate for Web Infections*, Proceedings of the Seventh Annual Workshop on Economics and Information Security, Hanover, New Hampshire. Retrieved on 2010, March 13 from http://www.eecs.harvard.edu/~greenie/

Harris, L. Comcast Voices, March 2010. *The botnet challenge.* Retrieved on 2010, March 20 from http://blog.comcast.com/2010/03/the-botnet-challenge.html

Harris, M. Techradar, April 2005. *Spammers recovering from McColo shutdown.* Retrieved on 2010, March 19 from http://www.techradar.com/news/internet/spammers-recovering -from-mccolo-shutdown-591118

ICANN. (2010, February 12). Registration Abuse Policies Working Group Initial Report. Retrieved from http://gnso.icann.org/issues/rap-wg-initial-report-12feb10-en.pdf

International Telecommunications Union. (2008). *ITU Botnet Mitigation Toolkit.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html on 2010, April 19

Internet Industry Association. (September 2009). *INTERNET SERVICE PROVIDERS VOLUNTARY CODE OF PRACTICE FOR INDUSTRY SELF-REGULATION IN THE AREA OF e-SECURITY, Consultation Version 1.0*. Retrieved from http://www.iia.net.au/index.php/section -blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.htmlon 2010, April 19

Internet World Stats (2009). *The Internet big picture*. Retrieved from http://www .internetworldstats.com/stats.htm

Krebs, B. Security Fix (November 2008). *Host of Internet spam groups is cut off.* Retrieved on 2010, January 13 from http://www.washingtonpost.com/wp-dyn/content/article/2008 /11/12/AR2008111200658_pf.html

Levy, S. Wired Magazine, February 2010. *How Google's Algorithm Rules the Web.* Retrieved from http://www.wired.com/magazine/2010/02/ff_google_algorithm/all/1

Lohr, S. (2010, January 10). The New York Times. *Companies fight endless war with computer attacks.* Retrieved from http://www.nytimes.com/2010/01/18/technology /internet/18defend.html

McAfee (2009). *2010 Global Threat Predictions*. Retrieved on 2010, March 14 from http://newsroom.mcafee.com/article_display.cfm?article_id=3607

NSCA (2010). *The 2010 State of Cyberethics, Cybersafety, Cybersecurity Curriculum in the U.S. Survey*. Retrieved on 2010, March 14 from http://staysafeonline.mediaroom.com /index.php?s=67&item=50

Scansafe (2009). *Global Trends Report*. Retrieved on 2010, February 26 from http://www.scansafe.com/gtr

Schneier, B. (2008, January 18). *The Psychology of Security.* Retrieved on 2010, March 21 from http://www.schneier.com/essay-155.html#sdendnote1sym

SCMagazine (2008, April 2). *Americans feel safe online, says poll.* Retrieved from http://www.scmagazineus.com/americans-feel-safe-online-says-poll/article/108583/

SCMagazine (2009, May 19). *"Chain of Trust" initiative launched to fight malware*. Retrieved from http://www.scmagazineus.com/chain-of-trust-initiative-launched-to-fight-malware/article/137079/

Sophos (2010, February 3). *Top ten malware-hosting countries revealed*. Retrieved on 2010, March 18 from http://www.sophos.com/pressoffice/news/articles/2010/02/malware -hosting-countries.html

Sophos (2010, February 3). *The world's top 10 dirtiest web-hosting countries*. Retrieved on 2010, April 25 from http://www.sophos.com/blogs/gc/g/2010/02/03/worlds-top-10-dirtiest-webhosting-countries

StopBadware. *COTI launch.* Retrieved on 2010, March 11 from http://blog.StopBadware.org/2009/05/19/sbw-asc-ncsa-launch-chain-of-trust-initiative

StopBadware. *Guidelines.* Retrieved from http://StopBadware.org/home/guidelines on 2010, March 13

StopBadware. (May 2008) *May 2008 Badware websites report.* Retrieved from http://stopbadware.org/home/research on 2010, April 17

Sullivan, R. (2009). *The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States*. Retrieved 2010, March 22 from http://kansascityfed.org/home /subwebnav.cfm?level=3&theID=10970&SubWeb=10782

Symantec (2009). *Norton Online Report*. Retrieved March 13, 2010, from http://nortononlineliving.com/

The Official Google Blog (2010, January 12). *A new approach to China*. Retrieved from http://googleblog.blogspot.com/2010/01/new-approach-to-china.html on March 13, 2010

Wall Street Journal, The (2010, March 3). *Most People Do not Understand Cyber Threats, Says Former DHS Chief*. Retrieved March 21, 2010, from http://blogs.wsj.com/digits/2010 /03/03/most-people-don%E2%80%99t-understand-cyber-threats-says-former-dhs-chief/

Websense (2009). *Websense security labs-State of Internet Security, Q1 – Q2, 2009*. Retrieved on March 13, 2010 from http://securitylabs.websense.com/content/

Appendix

Appendix 1: An inventory of malware stakeholders

→ Actors Fighting Malware

◊ Government

- Executive
  - Howard Schmidt, the Executive Office of the President's Cyber-Security Coordinator
  - Law enforcement (federal, local)
  - Regulatory
    - FCC + FTC
    - Japan's Information-technology Promotion Agency + Computer Emergency Response Team Coordination Center
    - Germany's BSI
    - The EU's ENISA
  - Department Homeland Security
    - US-CERT
  - NSA
  - State Department
  - Department of Defense
- Legislative (ex: CDA 230)
- Judiciary (ex: Zango *vs* Kaspersky)
- Other
  - MS-ISAC

Schmidt said his goal is to develop a comprehensive strategy to secure networks and ensure an organized, uniform response to future cyber incidents. He said he would work to strengthen public-private partnerships in the United States and abroad, promote research and development of security technologies and lead a cyber security awareness and education campaign.

Requested that a U.S. District Court halt the sale of "stalker spyware"

◊ Organizations

- Security Community (non-cyber):
  - Think Tanks
  - Universities and Academics
- Large Security Companies
- Computing & Internet Industry
  - Internet Service Providers

James A Lewis (CSIS) often quoted on Google vs. China dispute

Comcast—end-user education
- The Security Channel
- Best Practices Guide for customers
- Bot warnings

Google Safe Browsing API

- Browser Makers
- Search Engines
- Software Vendors/Projects
  - End-user applications
  - Web server software
- Hardware Vendors
- Anti-Malware Companies
- PII Protection Companies
- Registrars & registries
- Hosting Companies
- Online/Offline Educational Resources
  - Computer security courses and books (ex: *Crimeware*)
  - Company trainings and similar educational opportunities
  - Online courses (ex: SANS)
- Release Trackers
- Ad Networks
- Takedown and Cleanup companies
- Social network operators
- Other Communication Giants

Microsoft's Security Center and Software Removal Tool

Symantec's entertaining educational YouTube videos; Dasient's web anti-malware service

The Koobface threat

- Internet Regulation/Independent Institutions (ex: ICANN)
- Trade Associations (ex: MAAWG, APWG, ICSG)
- Non-profits (ex: National Cyber Security Alliance, Center for Democracy and Technology)
  - Databases
    - StopBadware's Clearinghouse
    - The Wildlist Organization International
- Anti-Malware Communities
  - Institutionalized communities
  - Computer Security blogs and websites
  - Twitter communities/threads
  - Internet Forums
- Press

AVAAR: Association of Anti-Virus Asia Researchers

"New" StopBadware: increased focus on communities

    - Specialized and Semi-specialized
    - Mainstream media
    - Other information providers

- Hardware and Software Retailers
    - Responsibility dilemma → who is responsible

- Academics
    - University education
    - University research
    - K-12 education

- Victim Associations

- Banks and Financial industry
    - Large banks
    - Smaller banks
    - Organizations (ex: FS-ISAC)
    - Insurance companies

- Businesses & Business Organizations

- International Conferences
    - Computer Security Institute
    - RSA Conference

◊ Individuals

- End users
- Corporate/In-house Security Professionals
- Independent Security Professionals
- Independent computer consultants serving individuals and small businesses
- Teachers
- Parents—children
- Volunteers

→ Malware Distribution Channels

- Websites (malicious or compromised)
    - Social engineering (ex: download this codec to watch this video)

    - Drive-by downloads (exploit via browser, plug-in, or other app)
    - Redirects to social engineering or drive-by download sites
- Ad networks
- Internet Service Providers
- Portable media (flash drives, hard drives, CD/DVD, etc.)
- E-mail
    - Social engineering
    - Attachments
    - Worms (exploit e-mail app)
- Network (via open ports, stack exploits)
- Rogue applicationsw
- Downloaders (i.e., one piece of malware downloads others)
- Other social engineering

→ Malicious actors

◊ Government

- Rogue governments
- Lack of governmental and law enforcement structures

◊ Organizations

- Rogue/Bulletproof Hosting Companies
- Rogue Anti-Malware Companies
- Rogue Ad Networks
- Rogue Marketplaces
- Crime Syndicates/Organizations
- Businesses seeking to eliminate the competition/engage in espionage
- Politically-motivated groups

◊ Individuals

- "Mules"
- Malware developers
- Bot herders
- Crime bosses
- Spammers
- Corrupt government officials and law enforcement officers
- Corporate insiders
- Black market operators/traders