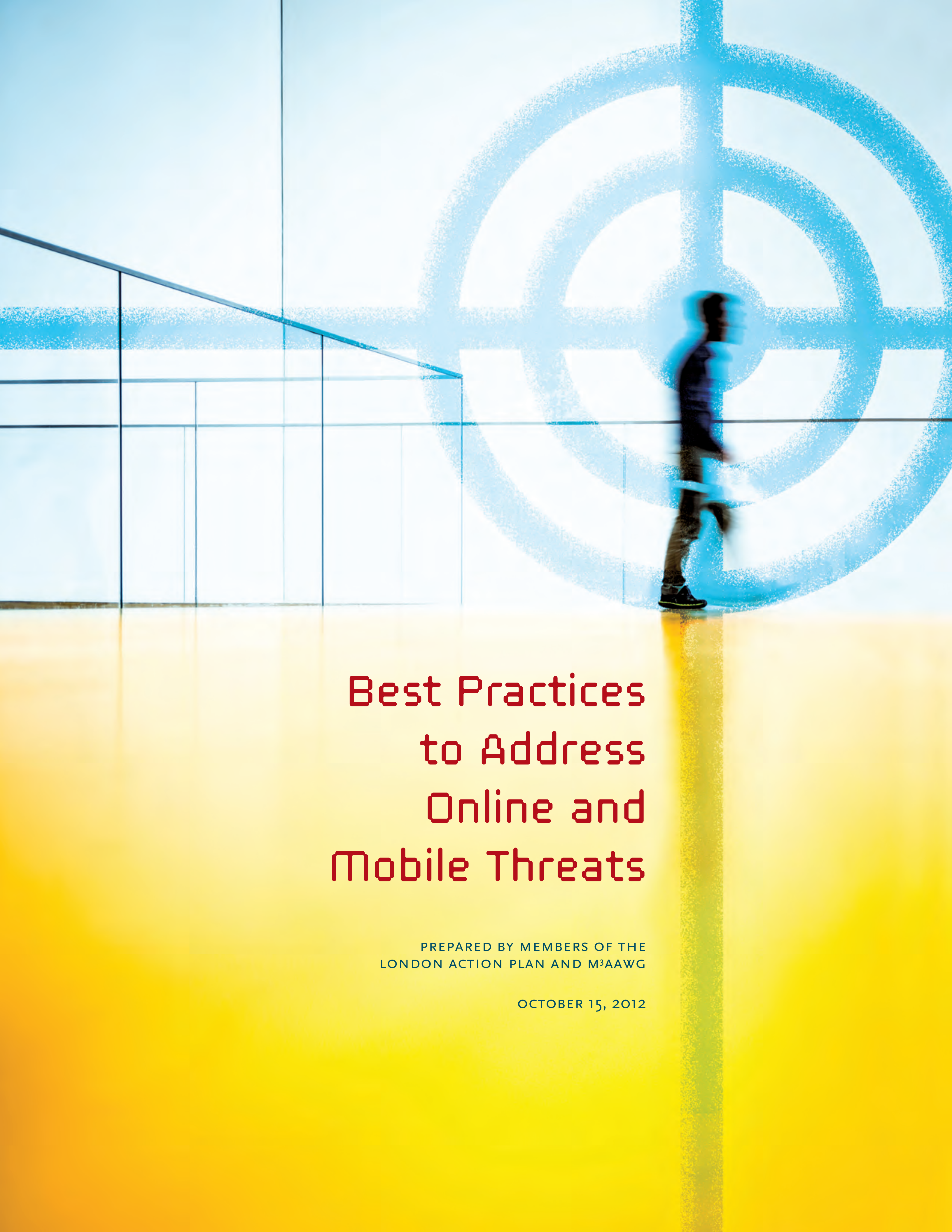


Best Practices to Address Online and Mobile Threats

PREPARED BY MEMBERS OF THE
LONDON ACTION PLAN AND M^{3}AAWG

OCTOBER 15, 2012

CAUCE

London Action Plan
International spam enforcement network

M3AAWG
MESSAGING MALWARE MOBILE

Industry Canada Industrie Canada

Canada

Table of Contents

Executive Summary

Internet and mobile technology affects almost every facet of our day-to-day lives and is part of almost every business model. As technology has become integrated into our lives, our dependence on computers and mobile devices has grown. We use the devices to connect to family and friends, shop and bank online, engage with civic agencies and elected officials, interact with business colleagues and partners, streamline supply chains and deliver just-in-time products from manufacturing facilities to retails outlets. With a growing dependency and rapid migration of commercial transactions to online and mobile platforms come threats from cybercriminals.

Cybercriminals profit from sending spam, phishing, injecting malware onto websites, spreading botnets, redirecting Internet traffic to malicious websites, and inserting spyware onto computers and handheld devices.

The economic impact of these endless attacks is not easily measured, be it by country or on a global scale as losses from cybercrime often go unreported or under reported by victims, financial institutions that cover the expense of the loss, or by businesses that incur everything from defence and remediation costs to service downtime due to Distributed Denial of Service (DDoS) attacks.

The primary focus of this report is not only to study the risks in the online and mobile environment that threaten consumers, businesses and governments every day, but also to suggest best practices to address these threats. The focus is on four major areas:

Malware and Botnets

Malware and Botnets are the major threats to the Internet economy. Malicious software or "malware" is created or used by criminals to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Botnets are groups of machines infected with malware that communicate (often through a complex network of infected computers) to coordinate their activity and collect the information the individual malware infections yield. Imagine the computing power and bandwidth capabilities that come with being able to control over one million computers.

Criminals are continuously changing their malware to avoid its detection and remediation. Consequently, most Anti-Virus (A/V) software has difficulty identifying emerging and recent threats. A growing proportion of malware can detect that it is being "monitored" while it is running, perhaps by an anti-virus researcher, and will alter its behaviour to make it more difficult for malware experts to analyze its functions. Some malware will even respond to attempts to monitor and analyze it by counter-attacking with a DDoS.

Because of this, it is becoming increasingly difficult for the online security community to keep pace with the malware threat environment.

Phishing and Social Engineering

Phishing refers to techniques that are used by malicious actors to trick a victim into revealing sensitive personal, corporate, or financial information.

Phishing has been steadily increasing in frequency, sophistication, and damage since it emerged as a threat in the mid 1990s, and it is showing no signs of abating. As well, the type of data sought through phishing has grown increasingly more valuable, evolving from simple access to email and consumer bank accounts that incur individual losses in the thousands of dollars, to current-day high-value targets. High-value targets, such as corporate executives with access to corporate accounts, special privileges, or corporate bank information, have been used to produce catastrophic single-event intellectual property and financial losses of several millions of dollars, with an untold number of events occurring annually.

Although phishing is not new, increases in the number, targeting, and sophistication of the attacks in recent years represent an ever increasing threat to companies, governments, and consumers as well as eroding overall confidence in the digital economy. Defences must be coordinated to leverage open, transparent, multi-stakeholder solutions to maximize effectiveness, minimize costs, and increase public trust.

Internet Protocol and Domain Name System Exploits

A variety of illegal activities use vulnerabilities associated with the Domain Name System (DNS) and Internet Protocol (IP) addresses. The most serious DNS exploits are resolver exploits, in which bad actors introduce forged data to redirect Web and other traffic to false versions of popular websites. These exploits cause an elevated risk because in many cases consumers are completely unaware that they have been redirected to a fake site rather than the one they actually wanted to visit.

Every computer on the Internet has an IP address, which is used to identify that computer much as telephones are identified by telephone numbers. Traditional IP addresses, known as IPv4 (Internet Protocol version 4) addresses, are 32-bit binary numbers, invariably written as four decimal numbers, such as 64.57.183.103. The first part of the address, in this case 64.57.183, often identifies the network, and the rest of the address, in this case 103, the particular computer (“host”) on the network, although these days, classless inter-domain routing (CIDR) has eroded that traditional division.

Since IP addresses are hard for humans to remember, and are tied to physical networks, the DNS is a distributed database of names that let people use names like www.google.com rather than the corresponding IP address 173.194.73.105.

Despite its enormous size, the DNS gets excellent performance by using delegation and caches. That is, different organizations are each responsible for their part of the domain name system, and end-sites remember recent DNS results they’ve received. Since it would be impractical to store all of the names in the DNS in a single database, it is divided into zones that are stored on different servers, but logically linked together into an immense interoperable distributed database.

Mobile Threats

With the advent of the smartphone and the application markets for Android, Apple and Blackberry devices, the e-commerce environment has grown to include these mobile devices. As consumers migrate their e-commerce activities to these devices and platforms, bad actors seeking to profit and defraud have been quick to follow. In addition the mobile environment creates additional unique opportunities for new types of attacks and threats targeting both consumers and businesses.

Mobile devices provide increased functionality and ease of use for consumers. They are often carried by individual users, are typically kept in an active state, and are often GPS enabled and location aware. Because of this, mobile devices are inherently more attractive for malicious attacks.

In the past few years, the mobile environment has seen increased development of malware, the first mobile botnets, an increase in premium rate text message (SMS) scams and sophisticated exploits that have been associated with the jailbreaking of mobile devices.

Cybercriminals have a strong preference for operating in a transnational environment, further complicating enforcement efforts. For example, an illegal online pill seller living in the U.S. might send spam advertising those drugs from a compromised computer in Brazil, pointing potential purchasers at a website with a Russian domain name (while physically hosting that website in France). Credit card payments for orders might be processed through a bank in Azerbaijan, with orders being drop shipped from a site in India, and proceeds funneled to a bank in Cyprus. Criminals know that by operating in this manner, many factors complicate any official investigation into their online crimes, and reduce their likelihood of being caught. These factors include a lack of cooperation, differences from one jurisdiction to another, and the cost of international investigations.

Conclusion

This report is submitted by an international group of experts from industry and government. It summarizes best practice recommendations to address these new and more sophisticated online and mobile threats. It is our hope that this report will facilitate effective ongoing collaboration between this group, LAP, M^{3}AAWG and the OECD to address these threats.

Introduction: The Evolution of Online Threats

Since 2006 the global Internet and mobile economy has seen the evolution of online threats and in certain instances new types of attacks. The tools used to defraud and steal information in the online and mobile environment today are increasingly sophisticated, providing bad actors and fraudsters with an expanded toolbox.

An example of a new online attack would be "fast flux service networks", where public Domain Name System (DNS) records are rapidly changed by botnets, in some cases every three to five minutes or less, in order to hide phishing and malware delivery websites, child exploitation sites, and other websites that cannot be readily hosted at a conventional provider. The basic idea behind fast flux is to have numerous compromised computers associated with a single fully qualified domain name, and changing the DNS records with extremely high frequency (every few minutes), effectively swapping which hosts are associated with that domain name.[1] This use of a constantly changing set of hosts makes it much more difficult to take down these illegal websites; as you find and report three or four "botted" hosts, another three or four are rotated into place, replacing the ones being tracked by the security community with a brand new batch.

While much of this illicit online activity is invisible to typical end users due to modern-day filtering and blocking techniques, spam remains an important vehicle, often conveying malicious payloads as well as unwanted spam. Spam is not just an email phenomenon.
It continues to expand into various forms of new media. For example, mobile messaging and Voice over Internet Protocol (VoIP) spam are now extremely common, as are spam comments on social media, blogs and other websites, and spam entries polluting and degrading the quality of search results in online search engines.

The domain sector (consisting primarily of the Internet Corporation for Assigned Names and Numbers (ICANN), Registrars and Registries) can play a critical role in the anti-abuse space, particularly as new Internet protocols (e.g., IPv6) become more prevalent and ICANN prepares to add a massive number of new Top Level Domains (TLDs). Today there are approximately 24 TLDs, such as .com, .org, .net, .gov, but in the near future there could be hundreds of new TLDs.

It is our suggestion that participants in the OECD strengthen their participation in the main coordinating entity in the domain space, the ICANN Government Advisory Council, working to encourage ICANN to redouble its efforts in the area of contractual compliance work and oversight of registries and registrars.

Much effort has gone into breaking down silos and facilitating cooperative ventures between business entities, NGOs, governments, regulators, and law enforcement agencies. The OECD, LAP, M^{3}AAWG and other international organizations have been effective in the development of existing public-private coordination and cross-organizational collaboration. For example, the DNS Changer Working Group[2], and the Conficker Working Group[3] are amalgams of subject matter experts, law enforcement, and industry representatives that have had notable success based upon a mutual-trust model, putting aside competitive concerns. This collaboration has been extremely successful, and remains vital to continued anti-abuse efforts.

However, there continues to be a need for stronger, more comprehensive, technology-neutral anti-spam and anti-abuse legislation and regulatory regimes facilitating cross-border cooperation. Part of the solution may lie in the diplomatic arena, particularly when it comes to enabling more effective cross-border law enforcement activity. Substantially improved end-user education and awareness are other important facets of effective anti-abuse measures.

Section 1 Malware and Botnets

Malicious software or "malware" is created or used by criminals to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in a variety of forms, from compiled programs to scripts, or bits of code inserted into otherwise legitimate software. 'Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software. Malware generally includes computer viruses, worms, Trojan horses, droppers, spyware, adware, rootkits, spamware and other malicious programs. Malware is generally designed to fulfill one or more functions, ranging from facilitating the introduction of other malware (*e.g.*, droppers/downloaders) to the collection of information (*e.g.*, spyware). Other malware may specialize in the malicious disruption of computers, users and networks.

Botnets are groups of machines infected with similar malware, that communicate (often through a complex intermediate networks of infected computers) to coordinate their activity and collect the information the individual malware infections yield. Botnets are most often named for the specific malware that implements and coordinates this communication, for example, Zeus and SpyEye. However, each machine in a botnet may contain a variety of malware components. For example, a Zeus botnet node may contain the Zeus malware itself (handling botnet communication, theft of information and downloading of additional malware), as well as other threats such as spamware (such as Cutwail) or "attack" components (such as Pushdo DDoS malware).

Botnets can be large. Botnets composed of more than 1,000,000 machines have been observed under the control of a single botmaster. However, a botnet does not have to be this large to be extremely damaging. Even a botnet composed of 1000 or 2000 nodes can wreak massive havoc.

In its beginning, malware was most often developed by "hobbyists", computer-knowledgeable people who were looking for a challenge or some "amusement". Since that time criminals (including organized crime) have realized that there is a lot of money to be made in malware. An example of this is the WinFixer case, where criminals have tried to scare victims into making software registration payments[4]. Today, virtually all malware is created and used for criminal purposes.

Malware, the principle major threat to the Internet economy, is being used to conduct the following activities:

- Capturing personal and business information by:
  - capturing keystrokes
  - collecting logins and passwords
  - copying address books
  - stealing sensitive corporate information, documentation, and/or trade secrets or even capturing sensitive government or military information
  - collecting banking and transactional information
- Facilitating devastating DDoS attacks for nation state purposes, political activism, or as a prelude to extortion, among many other purposes
- Sending spam via email, SMS and other methods

Criminals are continuously changing malware to avoid detection and remediation. Most Anti-Virus (A/V) software has a dismal track-record when it comes to identifying current and recent threats. A growing proportion of malware can detect that it is being "observed" (perhaps by an anti-virus researcher) and alter its behaviour to make it more difficult for researchers and analysts to determine how it works. Some malware will even attempt to discourage monitoring by counter-attacking researchers and analysts with a DDoS.

Because of this, it is becoming increasingly difficult for the online security community to keep up with the pace at which the malware threat environment is evolving.

The Malware and Botnet Threat Landscape – Present and Future Outlook

The present and future outlook for malware can be obtained from published reports of leading Internet security companies such as Symantec, McAfee and Sophos. Information for this report has also been drawn from a report by the Gendarmerie Nationale of France, and from the book entitled *Malware Forensics: Investigating and Analyzing Malicious Code*. These reports are referenced below; links to the complete reports/books can be found at the end of this section.

Based on the period of coverage of these reports, the "present" is considered to be 2011-2012, and "future" is beyond 2012.

The Present Malware Landscape

- 2011
  - Certain countries are identified by Symantec in their "Internet Security Threat Report: 2011 Trends" as the top sources for overall malicious activity, corresponding to their large number of Internet users.
  - Symantec identifies certain countries as sources of malicious activity (not necessarily state-sponsored), further identifying the type of malicious activity.
  - Symantec compares the overall average proportion of attacks originating from certain countries with the year 2010.
  - The year saw major data breaches and targeted attacks on high profile companies and agencies. Criminals added new platforms to their attacks as business increased its use of mobile devices. There were a number of politically motivated "hacktivist" groups (*e.g.*, Lulz Security and Anonymous) that received much media attention while the more common malware increased (Sophos "Security Threat Report 2012").
  - Even as organizations emphasized the importance of cyber security, the number of malware attacks and compromised websites grew steadily. In the second half of the year, Sophos observed an average of approximately 30,000 new malicious URLs each day, representing an increase of greater than 50% since Sophos' mid-year 2011 report.
- 1st Quarter 2012 (based on "McAfee Threats Report: First Quarter 2012")
  - Although the end of 2011 saw declines in many areas of malware and threats, PC malware in the first quarter of 2012 was at it's busiest in recent history, and mobile malware also increased at a large rate.
  - At the beginning of the quarter, spam volume grew but then resumed its downward trend. There was a moderate increase in malware targeting the Mac.
  - Diversity and growth in spam were seen in certain parts of the world, despite the fact that spam numbers remained relatively low worldwide.
  - New botnet infections leveled off though growth was seen in several countries.
  - The McAfee report cited above identified one country as once again hosting the greatest quantity of malicious Web content in the world.
  - Some significant arrests and actions were taken against cybercriminals and hacktivists, probably the most famous being the Waledac/Kelihos botnet takedown[5] and the very public arrests of members of Anonymous and LulzSec.
  - Microsoft led an operation to takedown the Rustock botnet that affected hundreds of thousands of computers and was responsible for a large portion of spam on the Internet.[6]
  - Threats continued to evolve and attackers continued to test our defences with new forms of attack.

Below is a more detailed examination of malware patterns:

- 2011 (based on Symantec's "Internet Security Threat Report: 2011 Trends")
    - **Website malware:** drive-by attacks continue to challenge consumers and businesses and are responsible for hundreds of millions of attempted infections every year. Symantec has determined that 61% of malicious sites are actually regular websites that have been infected with malware.
    - **Email-carried malware:** the number of such emails as a proportion of total email increased in 2011; large companies saw the greatest increase, with 1 in 205.1 emails identified as malicious for large enterprises with more than 2500 employees. This figure was 1 in 267.9 emails for small to medium size businesses.
    - **Border Gateway Protocol (BGP) hijacking:** Symantec found a number of cases where spammers were able to subvert the BGP protocol to send spam that appeared to come from a legitimate (but hijacked) source. Although the cases were low in number, this is a threat to watch out for in the future, and highlights the need to secure all infrastructure, not merely computers.
    - **Polymorphic Malware:** this is malware whose internal structure or content constantly changes, making it much harder for traditional pattern-matching anti-malware programs to detect. In 2011, Symantec frequently identified the polymorphic threat Trojan.Bredolab in large volumes, accounting for 7.5% of all email malware blocked, equivalent to approximately 35 million potential attacks in a year.
    - **Exploiting the Web:** attack toolkits: attack tool kits allow the creation of new malware and the assembly of an entire attack without having to write the software from scratch. Such toolkits account for nearly two-thirds (61%) of all threat activity on malicious websites and can be described as the products of "crime as a service".
    - **Exploiting the Web:** rootkits: a rootkit enables privileged access to a computer while hiding its presence from the administrator by subverting standard operating system functionality. Rootkit attacks are small in number but they are a growing problem. The current rootkit frontrunners are Tidserv, Mebratix, and Mebroot. They all modify the Windows master boot record (MBR) in order to gain control of the computer before the operating system is loaded. Variants of Downadup (aka Conficker), Zbot (aka Zeus), as well as Stuxnet all use rootkit techniques to varying degrees.
    - **Exploiting the Web:** social media threats: a social medium is almost perfect for the practice of social engineering since it is easier to fool someone when they think they are among friends. More than half of all attacks identified on social networking websites were related to malware hosted on compromised blogs/Web communication websites. A hyperlink for a compromised website would be shared by the social network.
- 1st Quarter 2012 (based on "McAfee Threats Report: First Quarter 2012")
    - Growth was seen in established rootkits and new families of rootkits emerged. There was a large increase in password-stealing Trojans.
    - Active malicious URLs continued to increase from the upward growth that was established in the 4th quarter of 2011.
    - Java and Flash exploits were popular tools for criminals.

The Future Malware Landscape

NEAR FUTURE (1–2 YEARS)

According to Symantec, BGP hijacking is a threat to watch out for in the near future. As well, polymorphic malware may be on the rise given that it is difficult for pattern-based anti-malware programs to detect it. Attack toolkits will likely remain part of the malware scene since they have the ability to regularly launch a flourish of new attacks following the introduction of each new version until the targeted vulnerabilities are patched.

Attacks on Macs will likely increase in number. The first known Mac-based botnet was discovered in 2009. The year 2011 saw the emergence of new malware against Mac OS X, including Trojans like Mac Defender, a fake anti-virus program. In May 2011, Symantec found a malware kit for Mac (the Weyland-Yutani BOT[7]) the first of its kind to attack the Mac OS X platform, using Web injections as a means of attack. While such kits are common on Windows, this new Mac kit is being marketed as the first of its kind. Many attack tools are cross-platform, exploiting Java vulnerabilities on both Macs and Windows PCs.

Rootkits will remain part of the malware scene. Symantec's Internet Security Threat Report states,

> "As malicious code becomes more sophisticated it is likely that they will increasingly turn to rootkit techniques to evade detection and hinder removal. As users become more aware of malicious code that steals confidential information and competition among attackers increases, it is likely that more threats will incorporate rootkit techniques to thwart security software."

Finally, social engineering attacks will likely continue to try to trick users to give access to their devices or divulge personal data. End users need to be vigilant for these attempts and software makers should take steps to prevent abuse of their products.

INTERMEDIATE FUTURE (1–10 YEARS)

The Gendarmerie Nationale (French National Police) report discusses emerging threats, expected targets and forms for the decade 2011 to 2020. These threats not only include online transactions and applications, but also industrial control systems, robotics, home automation, and onboard systems. In particular, SCADA (Supervisory Control and Data Acquisition) systems (remote monitoring, control, and management) and satellite systems may be targeted. It is expected that on-demand cloud computing will be leveraged in the furtherance of crimes.

Technologies that will likely be targeted are not necessarily state-of-the-art, but rather technologies that are deployed on a larger scale. Installation times for such technologies are shorter in order to reduce the financial impact. The trend here will be that the cash out portion of the attack moves closer to real-time. Currently, there may be weeks or months between the compromise of a user account, the sale of that user account (or bulk account information) to another and then the attempt at using those compromised accounts in a crime to monetize them. Automation on the criminal side will rise and we will see shorter lifecycles. Similarly, the time devoted to providing security will be shorter as well. As a result, attacks that were once not carried out due to lack of financial interest will become more lucrative due to the mass appeal. An example of this is telephone switchboard fraud (scammers exploiting security gaps in telephony switching and routing, and using them to make expensive overseas calls). Additional targets for attack will include critical infrastructure and strategic services such as financial, socio-economic, and other services.

In terms of expected forms of attack from 2011 to 2020, the Gendarmerie Nationale report states that all technical innovations will be open to attack since products come with bugs (or are not designed with security or serviceability in mind). Threats against individuals, businesses, public organizations, and governments will arise out of the increasing interest of users to communicate electronically as well as the increasing amount of personal information shared or stored online, which can either be collected, harvested or stolen. Although the level of threat complexity will not relate directly with technological complexity, it must be expected that threats will become more innovative and sophisticated. Malware delivery will become more effective at locating and exploiting vulnerabilities in wireless networks, Web applications, and other technologies for large scale data theft, despite existing protective measures. Social engineering will be more subtle, using more personalized approaches.

New Techniques for Malware Propagation

Symantec describes new techniques for malware propagation as seen in website malware, email-carried malware, Border Gateway Protocol (BGP) hijacking, threats against Macs, and social media.

In website malware, badly spelled, implausible email has been replaced by techniques like “clickjacking” or “likejacking” in which a user clicks a website link to watch a tempting video and the attacker uses that click to post a comment to all the user’s Facebook friends, enticing them to click on the same malicious link. Facebook has largely countered this attack by asking the user to confirm a “Like” before it posts if the user is “Liking” an untrustworthy domain.

In terms of email-carried malware, Symantec found that in 2011, 39.1% of such malware was delivered via hyperlinks rather than contained in an attachment, an increase over the 23.7% figure seen in 2010. This indicates that attackers are trying to circumvent security countermeasures by using the Web to deliver malware rather than attaching it to email.

Threats against Macs represent the propagation of malware onto platforms that have up to now been relatively free of malware. The means of attack are similar to those seen for Windows platforms.

As well, the fact that many attack tools have become cross-platform, making use of Java exploits, for example, is in itself a new method of malware propagation.

Attackers are taking advantage of the increased information on social media sites regarding a user’s likes, needs, and expectations, to improve their social engineering techniques, which are then used for malware propagation through spamming and phishing. Facebook is a prime example of a social network where attackers can find this information.

Risks for Consumers, Businesses, and Networks; Privacy Impacts

The risks for consumers, businesses, and networks of becoming infected with malware depend largely on how easily the malware can be delivered to them. Given the malware landscape described above, and the new methods for malware propagation, it is probably safe to conclude that the risks are very high. Indeed, we might as well put up the white flag and surrender if we do not defend ourselves with proposed best practices (described below) and continue to enhance our defences to mitigate the malware onslaught. Privacy impacts will grow in proportion to the number of malware infections, since malware such as Trojans tend to be associated with the theft of personal information. However, work to mitigate these risks is progressing as exemplified by the following new research.

New Notable Research on Addressing Malware

A search on the Internet using the key words "new malware research" yields the following research work:

NQ Mobile™ Scientists Reveal Ground-Breaking New Malware Detection Method – new RiskRanker™ system will proactively seek out and identify risky apps in the marketplace even before they are downloaded to mobile devices. More information is available at (as of August 13, 2012): http://thehackernews.com/2012/06/riskranker-new-malware-detection.html

New Research Shows Flame Malware Was Almost Certainly A U.S. or Israeli Creation. This is an example of research that aims to uncover the nature of malware. More details can be found at (as of August 13, 2012): http://www.forbes.com/sites/andygreenberg/2012/06/11/new-research-shows-flame-malware-was-almost-certainly-a-u-s-or-israeli-creation/

Study calls for more focus on internet policing than anti-malware software. New research is suggesting that governments should focus more funds on Internet policing rather than anti-virus software, according to a new cybercrime report conducted by computer scientists at the University of Cambridge, UK. More details are available at (as of August 13, 2012): http://www.domain-b.com/infotech/itnews/20120618_software.html

Best Practices for Addressing Malware

This section provides an overview of some current practices to address malware. While much of what is contained in this section is focused on individuals and ISPs it should be recognized that addressing malware is an ecosystem-wide problem that will require actions from a variety of parties, not limited to ISPs or end users. The interconnected nature of this problem was highlighted by an initiative started under the auspices of the U.S. Department of Commerce called the Industry Botnet Group (IBG) which created a graphic that illustrates that a wide variety of entities, including individuals, have a role to play in botnet and malware detection, notification, prevention and remediation[8].

For individuals, this section focuses on the prevention, detection, and remediation of malware. For the ISPs, this section focuses on providing advice regarding what an ISP can do to assist individuals in detecting malware. In addition, recommendations are given for malware education and awareness. The section concludes with a discussion of malware forensics in the legal and regulatory areas of society, as well as practices for addressing malware that are industry led.

BEST PRACTICES FOR INDIVIDUALS

A) Best Practices: Prevention

These recommendations focus on how individuals can avoid getting infected with malware.

1. **Choose a Secure and Current Operating System:** When choosing an operating system, look for one that has proven capabilities to reduce your exposure to malware. Regardless of what operating system you choose, be sure to run the most recent production version of it. Modern operating systems have built-in mitigations that help protect against exploits used by malware to compromise a system. Never continue to use an older version that's no longer being actively maintained by the vendor as it likely will not receive important security updates (if your hardware cannot run the most recent version of its operating system, you need to retire or replace that hardware).

2. **Stay Patched Up-To-Date:** Ensure that your operating system and all applications, including helper applications (such as Acrobat Reader, Flash Player, Java, and QuickTime) are fully patched and up-to-date. Most issues exploited by malware have had patches available for more than a year. On systems running Microsoft Windows, Secunia PSI is one tool that can help you keep third party applications up-to-date[9].

3. **Use Only What You Need:** In general, it's best to only download or use software that's needed to get the job done. Avoid downloading software or files that do not add useful or necessary features or functionality.

4. **Seek Expert Help:** Ask the experts what the best choice for your needs is. (The "experts" may answer in different ways, but if they're the ones you rely on for support, going with what they say will almost always be better in your circumstances.)

5. **Run an Antivirus Program:** While antivirus products aren't perfect, they still can help, so pick and use one, and keep its definitions up-to-date. Schedule a full scan of your system at least once a week. Be sure you select a real antivirus product, and avoid being tricked into installing a fake antivirus product that is, itself, malware! (And if your antivirus program doesn't also protect against spyware, also use an anti-spyware program). Many free anti-virus programs are available; a review of many popular free antivirus options can be seen in PCMag.com's article, "The Best Free Antivirus for 2012"[10]

6. **Use a Firewall:** Although firewalls aren't foolproof, a hardware or software firewall will at least potentially add another layer of protection against so called scan-and-sploit attacks.

7. **Use Strong Passwords:** Passwords should be sufficiently complex to resist guessing or cracking. Some people rely on passwords that are at least eight characters long, and include a mix of upper and lower case letters, numbers, and special symbols. Others prefer a set of three to five unrelated words that are easier to remember but difficult for computer programs to guess. Either way, do not always use the same password on multiple sites.

8. **Remember To Take Regular Backups:** If your system does become infected, having a clean backup can be tremendously helpful when it comes to getting cleaned up and back on the air.

9. **Clean Up Any Unneeded Temporary Files:** Some malware may hide copies of itself among temporary files, and even if there aren't any infected temporary files, removing those temporary files will speed up system scans and reduce the size of your backups. One widely used tool for cleaning up temporary files under Windows is CCleaner.

10. **Don't Routinely Run As An Administrator:** "Administrator," "root" and other accounts that have special powers should only be used when you're doing something that requires the special privileges associated with those high powered accounts (for example, intentional installation of new software). When you're doing normal user tasks, run as a normal user.

11. **Disable JavaScript (Or Use NoScript):** JavaScript (a scripting language that's not related to Java, name notwithstanding), enables many exciting interactive applications; however, it is also widely abused to drop malware on vulnerable systems. If you don't need JavaScript, don't enable it in your Web browser. If you must run with JavaScript enabled, consider using a browser plug-in to prevent JavaScript from running except when you must allow it (*e.g.*, NoScript).

12. **Block Online Advertising:** Another common approach used to drop malware is "malvertising," or delivering malware via malicious online advertising. While online advertising plays a critical role in underwriting many terrific free sites, in most cases you will be able to block that advertising (including potential malicious ads) and still successfully access the content on those sites. One popular ad blocking tool is AdBlock Plus.

13. **Block Known Malicious Domain Names in DNS:** Some malware relies on the ability to successfully translate symbolic domain names to numbers. If you block the translation of those names via your domain name server, that malware may then be unable to successfully run. OpenDNS is an example of a company that offers malware-filtered DNS of this sort.

14. **Filter/Defang Potentially Dangerous Email:** Your email administrator should scan email for potentially dangerous email attachments, potentially dangerous links, and other dangerous content that may be emailed to you. One example of such a program that can help with this is MIMEDefang.

15. **Files Downloaded Via P2P Applications Are Often Infected:** Be aware that many of the files shared on peer-to-peer (P2P) file sharing services may be intentionally or accidentally infected with malware.

16. **Assume Any USB Thumb Drive Has Been "Booby Trapped":** If you are given a USB thumb drive, or find a "lost" USB thumb drive, never put it into your computer. It may have been intentionally infected with malware, and then dropped where you might find it in an effort to get malware onto your system.

17. **Avoid Using Unfamiliar Wi-Fi Hotspots:** Some open Wi-Fi hotspots may intercept any unencrypted traffic, thereby potentially violating your privacy. Use of a Virtual Private Network (VPN) may offer some protection. Ensure that any wireless access point you operate is secured with WPA2 to limit access (and misuse) of it. Companies may wish to consider investigating 802.1X, a protocol that can help eliminate spoofed (so-called "evil twin") websites for corporate users.

B) Best Practices: Detection

These recommendations focus on how malware gets detected, when efforts to stay safe online fail.

1. Be aware when a local scan detects something: One of the most common ways that malware is detected is via an antivirus scan. Another similar option would be to perform a scan using a purpose-built one-time anti-malware tool such as one of the "cleanup only" tools mentioned in PC Mag[11].

2. Take notice when your system begins to behave strangely: Another prime indicator that something's amiss is when the system begins to behave "strangely." Strange behaviours may include running slowly or crashing; having unwanted windows pop up (*e.g.*, fake A/V notifications); asking for one Web page only to go to some other one; not being able to go to some sites at all (particularly if those sites are update sites or security-related sites), etc.

3. Take action if your ISP tells you that your system is doing bad things: For example, your ISP may notify you that your system has been observed sending spam, or has been seen attacking another system on the Internet.

4. Use software to check system integrity: This software can be used to identify unauthorized changes to critical files.

C) Best Practices: Remediation

These recommendations focus on how malware infected systems can be dealt with.

1. **Clean In Place:** This approach relies on the user (or someone acting on the user's behalf) running one or more antivirus products on the infected system in an effort to clean it up. (experts may also manually delete infected files in some cases). This process may be time consuming, and ultimately may or may not work. Even after devoting substantial effort toward cleaning up an infected system, the infection may remain, or the system may be unstable and/or ultimately unusable.

2. **Rollback:** If the user has a clean backup, another option is to roll back to that earlier clean backup. Selecting this option may result in the loss of work since that time, unless those files are separately preserved and can be restored (note that if this is done, it needs to be done very carefully to ensure that restoring those files doesn't result in the system getting re-infected). Generally speaking, a rollback strategy works best when backups are frequent, and multiple backup generations remain available for potential selection. ("Hmm. Yesterday's backup is infected. Maybe the backup we took last week will be clean?")

3. **Complete reinstallation:** In this option, the system is reformatted, and the operating system and applications are re-installed from scratch. This can be a time-consuming process, and will often be frustrated by a lack of original media (many vendors no longer ship a copy of the operating system on physical media when they sell new hardware).

4. **Replace the System:** Finally, at least some fraction of users may decide that they simply want to replace their infected system, rather than trying to clean it up. This option may be particularly popular if the infected system is old or was not very powerful in the first place, or if the user wants to potentially change operating systems or go from a desktop to a laptop, for instance.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT

A) Best Practices for Detection and Notification (ISP-to-User)

Many ISPs today notify customers if they are infected with malware. ISPs may use a variety of techniques to notify individuals of infection. This section provides a list of some activities different ISPs may be taking today to notify end users, however, it shouldn't be implied that any one technique has been identified as a best practice. There are different benefits and downsides associated with each form of notification. Examples include the following:

1. **Email:** When an infected system is noticed, the ISP may notify the user by email. Unfortunately, many times users never check the email the ISP provides for their use, and the user may never provide the ISP with the email address that they do routinely use. Users may also have become wary of trusting email notifications as a result of widespread phishing attacks.

2. **Telephone:** The ISP can also notify the user by telephone; however, users may also be suspicious of phone-based notifications as a result of voice-based phishing attacks. Phone notification is also tedious and time consuming if a large number of infected users need to be notified.

3. **Fax:** While it is unusual for consumers to use fax machines, they may still be used by some businesses, and as such, may be another way to reach some business users who may have become infected.

4. **Text Message:** In cases where the ISP knows the mobile phone number of the customer, another option would be to push text message notifications to the users.

5. **Regular (Paper) Mail:** An ISP may consider notifying users via traditional postal mail ("snail mail") perhaps via an insert to their monthly bill. However, if the ISP is not already mailing the customer, doing ad hoc snail mail notifications may be expensive and of limited effectiveness, particularly if the user is predisposed to discard snail mail communications unopened due to a perception that they are likely just marketing.

6. **Truck Roll:** In situations where the user has purchased an on-site support contract, another notification approach may be via an in-person "truck roll" to the customer's site. Obviously the ISP technician will need to be able to satisfy the customer of his or her credentials, and we must also note that this can be a very expensive notification option.

7. **In-Band (Web) Notification:** In this approach, an ISP notifies the user by interposing an interstitial message when the user attempts to visit a normal website. This approach can be somewhat disconcerting for users, but is less disruptive than some other approaches, such as the "walled-garden" approach (see below).

8. **Walled-Garden:** If an ISP needs to immediately limit the damage that an infected user can cause, one option is to put them into a so-called "walled garden." When this is done, the user is allowed to access selected sites for remediation and hardening purposes, and may perhaps be allowed to continue to have VoIP access for things like access to emergency services, but typically cannot access most

other Internet resources. It should be emphasized that this strategy is not meant to be punitive. It is a damage mitigation technique meant to protect other Internet users, the ISP, and the customer, while still allowing the customer to access network resources needed to fix their infected system.

For additional information see also Internet Engineering Task Force RFC6561 'Recommendations for the Remediation of Bots in ISP Networks"[12]

Notification to end users isn't limited to ISPs. Other parties in the Internet ecosystem who have a relationship with end users can, and have performed notifications. For example, it was widely publicized that both Google and Facebook attempted to alert end users of potential infections associated with the DNS Changer malware.

B) Best Practices for Education & Awareness

1. **One-On-One Teachable Moments:** In the unfortunate event that a customer's system does become infected, that may be a prime "teachable moment" when selected techniques for avoiding re-infection may be particularly salient.

2. **Customer Security Website:** The most basic example of offering customer education and awareness is probably the creation of a customer security website offering advice and access to tools. There are multiple security websites providing information to end users today. Some of those are listed by the Industry Botnet Group mentioned above[13]. These sites may be hosted by ISPs, non-profits, OS manufacturers, software providers, search engines, financial services companies or other ecosystem partners.

3. **Inserts in Bills:** If ISPs routinely send information to customers via regular mail, this may provide another opportunity to share recommendations for securing the customer's system, and is something that can be distributed to all customers, including those that have shown no sign of infection to-date.

4. **Public Service Announcements (PSAs):** Another opportunity to educate end users about malware would be through public service announcements through televisions and radio. For example, in the U.S. the National Cybersecurity Awareness Campaign, STOP THINK CONNECT, has developed numerous PSAs placed into circulation annually since 2010.

5. **Promotional Materials:** There area also a variety of promotional materials such as customized mouse pads, mugs, t-shirts, bottle openers, pens or pencils, or other give-aways that may help raise awareness of malware and botnet threats.

6. **Contests:** Another opportunity for sharing the cyber security message may be associated with contests, particularly things like essay contests targeting school age users.

7. **Formal Education:** Another vital part of education and awareness is to incorporate cybersecurity or digital citizenship curriculum into schools. Addressing cybersecurity generally and in particular malware and botnets, is a long term public safety issue, and like other public safety issues, it can be best addressed by establishing societal norms which in many cases may be best instilled as part of an individual's formal education.

Due to the rapidly shifting threat landscape and complexity of malware and botnet threats, education and awareness can only be partially effective at protecting end-users. Legal, regulatory, technical and industry efforts will remain at the forefront of dealing with the malware and botnet problem (see below). However, basic education and awareness about online threats remains a necessary ingredient to protecting end-users.

Industry, associations and governments should develop and promote communications programs that provide end-users with a basic understanding of threats and simple to understand techniques on how to protect themselves.

Many such initiatives already exist and can be used as models or simply as a source for educational material (see below). Several of these resources are broadly based rather than strictly focused on malware and botnet related issues. However, it is usually better to provide end users with a combined message about Internet safety rather than numerous uncoordinated suggestions. In other words, the information should be short and coherent whenever possible.

- National Cybersecurity Alliance - Keep A Clean Machine – http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine (part of the US National Cybersecurity Awareness Campaign STOP THINK CONNECT which is focused on botnets and malware)
- FBI: http://www.fbi.gov/scams-safety
- National Consumer's League: http://www.fraud.org/tips/internet/general.htm
- RCMP: http://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- U.S. National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/

C) Legal and Regulatory Best Practices

In the context of malware forensics, Malware Forensics: Investigating and Analyzing Malicious Code (reference at end of section) suggests some best practices for malware investigations. Several of those are reproduced here:

- Framing and re-framing investigative objectives and goals early and often remain the keys to any successful investigation.
- From the outset, understand the importance of identifying inculpatory, exculpatory, and missing evidence.
- Design a methodology ensuring that investigative steps will not alter, delete, or create evidence, or tip off a suspect or otherwise compromise the investigation.
- Create and maintain at all times meticulous step-by-step analytical and chain of custody documentation.
- Never lose control over the evidence.
- Define, re-define, and tailor these guiding principles throughout the course of an investigation in order to help clarify and likely make more attainable early identified investigative goals and objectives.
- Think through the following important issues early on:
  - » Does the jurisdiction of an investigation require any special certification or licensing to conduct digital forensic analysis?
  - » What authority exists to investigate, and what are the limits to that authority?
  - » What is the scope of the authorized investigation?
  - » How will intruding on the privacy rights of relevant data custodians be avoided?

D) Best Practices for Industry and Government-Led Collaboration

Secure software development practices represent a best practice for limiting the spread of malware. The Software Assurance Forum for Excellence in Code[14] (SAFECode) is a global, industry-led initiative to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

The FCC's CSRIC Working Group #7 released a voluntary Anti-Bot Code of Conduct for ISPs and network operators on March 22, 2012, as a cooperative industry-government initiative[15].

The Code focuses on residential Internet users and includes five areas of focus for ISPs: education, detection, notification, remediation, and collaboration. To participate in this Code, an ISP is required to engage in at least one activity (i.e., take meaningful action) in each of the following general areas:

- **Education** – help increase end-user education and awareness of botnet issues and how to help prevent bot infections;
- **Detection** – identify botnet activity in the ISP's network, obtain information on botnet activity in the ISP's network, or enable end-users to self-determine potential bot infections on their end-user devices;
- **Notification** – notify customers of suspected bot infections or enable customers to determine if they may be infected by a bot;
- **Remediation** – provide information to end-users about how they can remediate bot infections, or to assist end-users in remediating bot infections;
- **Collaboration** – share with other ISPs feedback and experience learned from the participating ISP's SAFECode activities.

M^{3}AAWG actively participates in this initiative and will be listing ISPs adhering to the code[16].

In addition, the industry has established the Industry Botnet Group (IBG) in response to a U.S. Department of Commerce request for information on how industry can take collective action to address botnets[17].

Properly configured (hardened) operating systems and applications can reduce the infection rate from malware. The United States National Security Agency provides guidance on hardening computers against all threats including malware[18].

Additional information is available for routers, wireless, switches, VoIP, database servers and applications at the same location. Additionally, operating system and application resources for hardening against malicious software can be found in NIST's Check Lists[19] (including Android devices).

The Korea Internet & Security Agency (KISA) provides a 'DDoS Shelter' service for free to small businesses which don't have proper tools to protect against a DDoS attack themselves. The DDoS Shelter filters malicious traffic of the DDoS attack and passes normal traffic. Also, the KISA detects suspected zombie IPs in a spamtrap and has domestic ISPs to take proper action against these IPs on their networks.

Country-specific efforts can be found at the following websites:

- **Australia:** www.icode.net.au
- **Germany ECO/Botfrei:** www.botfrei.de
- **Japan Cyber-Clean:** https://www.ccc.go.jp/en_ccc
- **Switzerland Melani:** http://www.melani.admin.ch
- **Finland Ficora:** http://www.ficora.fi/en

E) Best Practices for ISPs

The malware threat can be reduced by reducing or eliminating infection vectors. Email is still a very effective method by which malware propagates itself. To mitigate this vector, some ISPs, hotels and free access points block outgoing mail (port 25) from any computer on their network other than their own mail servers. This thwarts infected computers from propagating the malware via direct mailing.

In Europe, some ISPs have taken this a step further. Users on these networks by default only have Web access. Any traffic for all other ports is denied. To allow sophisticated users more flexibility, these ISPs provide tools to allow specific authorized users to use other ports/protocols and services.

In both instances, the monitoring of blocked traffic attempts can be used as early warning indicators of malware infected machines as well as hindering malware propagation and control and command communications.

F) Best Practices for Servers and Hosting Providers

Currently, one of the most prevalent reservoirs of malware is compromised Web servers. These servers become compromised either when current security patches are not applied for both the OS as well as support applications and Web frameworks, or due to insecure user passwords. These compromises are exacerbated in small and medium-sized business and at many hosting providers due to small abuse staff/teams. Automation is being used by some to ameliorate these issues and should become a world-wide best practice.

1. **Customer Terms of Service Requirements for Timely Security Updates:** All clients should agree to maintain current security patches or allow the hosting provider to update frameworks in their directories.

2. **Maintain Current Security Patches:** All security patches should be current. This process can be manual for very small systems or scripted for larger hosting providers.

3. **Use Audit Tools to Identify Hosts:** Tools to perform server wide auditing for insecure software versions should be run at least bi-weekly and identified software should be patched.

4. **Use IT Security Software:** Tools (such as Tripwire) should be used to monitor the integrity of each server.

5. **Run Antivirus:** Run antivirus software frequently (if possible two different packages) to monitor variable host files for contagion.

6. **Consider Using Cloud Servers:** Since cloud servers are professionally maintained and used by many clients, they will tend to be better secured; on the other hand, they may be more targeted for attacks (*e.g.*, DDoS) because they are used by many. In general, security will be enhanced only if it is built into the cloud design[20]. Nevertheless, cloud servers should be considered as a possible alternative for better security, bearing in mind the reputation of the cloud provider, the security measures put in place, and whether or not the servers have been attacked in the past. If nothing else, cloud customers are protected to some extent by the SLA (Service Level Agreement). The fact that the U.S. intelligence community is moving to the cloud, should attest to the security of cloud servers[21].

References

Symantec, "Internet Security Threat Report: 2011 Trends", Vol. 17, April 2012. Retrieved June 25, 2012 from: http://www.symantec.com/threatreport/

McAfee, "McAfee Threats Report: First Quarter 2012", Retrieved June 25, 2012 from: http://www.mcafee.com/apps/view-all/publications.aspx?region=us&tf=mcafee_labs

Sophos, "Security Threat Report 2012", Retrieved June 25, 2012 from: http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx

Gendarmerie Nationale, "Prospective Analysis on Trends in Cybercrime from 2011 to 2020", Retrieved June 25, 2012 from: http://www.mcafee.com/apps/view-all/publications.aspx?region=us&tf=mcafee_labs

J.M. Aquilina, E. Casey, C. H. Malin: Malware Forensics: Investigating and Analyzing Malicious Code, Syngress Publishing, 2008. Excerpts available July 5, 2012 from: http://books.google.ca/books?id=lRjO8opcPzIC&pg=PA254&lpg=PA254&dq=Legal+and+regulatory+best+practices+for+malware&source=bl&ots=aV_Hpgww l&sig=UptXrpohiXtzwvzMeMc83tQZKnQ&hl=en&sa=X&ei=gWP2T9j-KcfqogHUytn-Bg&ved=0CEcQ6AEwAA

Section 2
Phishing and Social Engineering

Phishing refers to techniques that are used by malicious actors to trick a victim into taking an action they would otherwise not take online, often revealing sensitive information such as personal or financial data. Fraudsters pose as known entities (friends, businesses), leveraging existing trust relationships to compromise their victims.

Phishing has been steadily increasing in frequency, sophistication, and damage since it emerged as a major threat in the mid 1990s, and it shows no signs of abating. As well, the type of data sought through phishing has grown increasingly more valuable, evolving from simple access to email and consumer bank accounts that incur individual losses in the thousands, to current-day targets: corporate accounts with special privileges ("super-user") and corporate bank information. Each single event can incur corporate intellectual property and financial losses up to millions of dollars, with untold number of events occurring annually.

Phishers now counterfeit messages and Web pages that are indiscernible from ones that are authentic, using armies of compromised legitimate machines (botnets) and infecting software (malware) to the same ends that previously required more overt end-user interaction. Phishers also have developed mobile malware that can render some protective measures ineffective.

IBM declared 2011 "the year of the data breach".[22] The Anti-Phishing Working Group[23] noted that the number of hijacked brands seeing fraudulent email usurping their brands reached an all-time high in March of 2012. RSA Security Solutions statistics showed an increase of 19% in the first half of 2012.[24]

The Phishing Landscape

Phishing is distinguished by the types of information sought, the types of targets attacked, and the channels through which attacks are conducted.

Goals of Phishing Attacks – What they're after

Information obtained by phishing is typically used for some type of financial theft, either directly on the victim, or on another target such as the victim's employer. Phishing, itself, is therefore typically only a first step and does not necessarily immediately result in any direct financial theft.

Common phishing attacks obtain:

- **Account Credentials** – The victim reveals specific information for accessing specific accounts, such as a username and password combination to their online bank, airline affinity points account, gaming account with controvertible points-for-cash, or other accounts with inherent value.
- **Personal Data** – The victim reveals other personal details that can be used to attack and compromise the victim's accounts, such as their date of birth and social security number.
- **Financial Data** – Payment mechanism details are revealed, such as routing numbers for a victim's checking accounts.
- **Malware Delivery** – Access to a victim's computer in order to install malware that enables further actions.

Techniques of Phishing Attacks – Methods they use

Predating the Internet, online and offline techniques that trick people into divulging information are often called "social engineering". When email phishing emerged, the attackers were not very discriminating. They broadly sent general-purpose emails to as many people as possible hoping some percentage would be tricked. As defences against these attacks strengthened, the attackers fine-tuned their strategies.

Typical types of phishing attack include the following:

- **Net-Phishing:** An indiscriminate, broad-based attack. One example is mail purporting to be from a well-known bank, expected to be used by at least some of the recipients.
- **Spear Phishing:** This targets specific individuals or organizations. It can be customized to trick victims who are traditionally more valuable (and suspicious) than average users. These might be employees of a targeted company that an attacker is looking to penetrate. Reverse phishing is a variant on spear phishing wherein criminals message from a collegial company or organization known to a victim with fraudulent "new" payment instructions.
- **Whaling:** A variant of spear phishing, this targets a specific high-value individual who can, in turn, provide broader access to other victims. Example victims are company executives and IT managers. This is a common vector for corporate espionage.
- **Clone (aka "Replay") Phishing:** A legitimate message is captured, and then resent with slight modifications making them easier to slip past past technical counter-measures or to trick victims into following a fraudulent Web link, even if the message is delivered to the "spam" folder.

Channels Used for Phishing – How they attack

Phishing attacks come through a variety of communication services. As a service becomes more widely available and automated, phishers exploit it.

- **Email** – This has been the most common channel of attack, due to its ubiquity, low cost per delivery, and ease with which it can be linked to fraudulent destination websites.
- **SMS** – Web links ("URLs") are broadly supported within telephony's Short Message Service (SMS). Due to the proliferation of link-shortener services used in SMS, the small form factor of mobile devices (small size and convenience), and users' inherent trust of telephone networks, attackers are able to evade defences more commonly found on traditional email clients. Also, SMS is often used as a separate channel for enhanced, integrated security mechanisms (in particular, two-factor authentication), which in turn makes it an increasingly attractive target for attackers. For more on this, see the Mobile Threats section of this report below.
- **VoIP** – Telephony and other voice activities are moving towards Internet-based mechanisms, collectively known as "Voice over IP" or VoIP. This integration of computers with phone systems makes it possible to trick victims into clicking fraudulent links that automatically place a telephone call, rather than go to a website. The call itself may directly generate revenue to the attacker, or it may direct the victim to a social engineer who convinces the victim to reveal information. Smartphones exacerbate the threat by simplifying this Internet/telephony integration for users.
- **Social Networks** – These create a group experience conducive to a sense of trust, which is, in turn, conducive to social engineering that exploits the victim's online relationships. Clone phishing can work extremely well when the attacker mimics a message from a trusted online friend.

Timeline of a Typical Phishing Campaign

A common account credential phishing campaign has four elements to it:

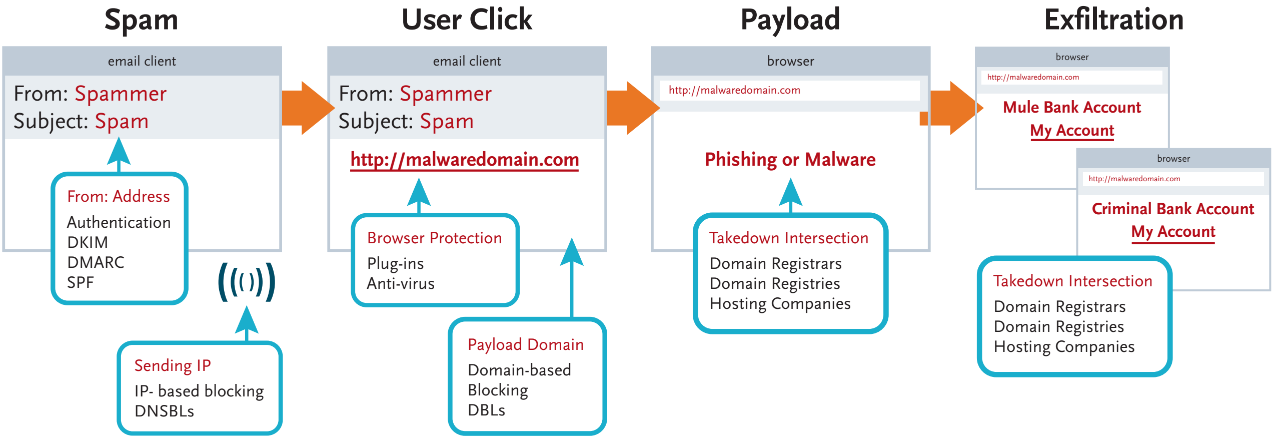
1. **Initial message** – A message is delivered and seen by an end-user. It appears genuine and therefore has a high degree credibility, typically containing counterfeit elements of a legitimate message, and ostensibly emanating from a legitimate source, such as one's bank.

2. **Call to action** – The end-user is exhorted to click on a link or reply to the message with confidential information. The most effective calls to action prey on fear and greed.

3. **Payload** – This content causes the victim to divulge the target information. It can be in the initial message or can be on a target website, called a "landing page". The website may be compromised, or can have a look-alike domain name to confound the end-user. The payload has either a form requiring the victim to enter confidential information, or a "drive-by download" mechanism wherein a user is convinced to click a link to a malicious site. When the user follows the link, malware is surreptitiously loaded onto the victim's computer, allowing the criminals to retrieve confidential data, after which the victim is redirected to a legitimate site.

4. **Exfiltration** – The data are transmitted to phishers through unwitting or collaborative third parties. For example, financial phishing uses intermediary bank transfers to obfuscate the identity of the thieves; people participating in the interim steps are known as "money mules".

There are a number of points where the workflow of a phishing campaign can be prevented or disrupted, as noted in Diagram 1:



Recent Social Engineering and Phishing Threats

The increased sophistication of phishing scams allows exploits to have greater potential leverage. For example, phishers now gain access to third-party Email Services Providers (ESPs), who send bulk mail on behalf of the world's largest brands. Criminals access an ESP's infrastructure, steal client lists, and send phishing spam or malware to unwitting recipients, who believe the message is from a legitimate list. A widely recognized breach was of the ESP, Epsilon, in April 2011, possibly obtaining data of over 150 companies, many on the Fortune 500.

Drive-by downloads are typically found on social networks. A call-to-action message is posted to the victim's friends through a hacked user-account, resulting in their computers becoming infected. Alternatively, the friends' accounts are hacked as they click-through. Google has seen millions of images on malware-infected sites form part of their search results.

Commercial phishing is directed at businesses rather than consumers and has become more common since November 2011, when the Cutwail[25] botnet sent out millions of emails purporting to be from services such as FEDEX and UPS. Two botnets, Zeus[26] and SpyEye, are completely dedicated to phishing activities. Torpig is a botnet that also engages in spreading easily customizable malware. Known variants look for ESP and financial institution login credentials. Torpig can be spread indiscriminately and stay dormant until the victim logs into a site for which the criminal wishes to have credentials. Attempts to take the botnet down have had only limited success.

The status quo is an arms race, with evolving attacks and defences. A recent example of this is at Pinterest, a new social media site that became compromised by spammers, malware and phishing schemes as its popularity grew over the course of 2011-12.

Ransomware is a common type of phishing scam that involves convincing an end-user that their computer has some form of malware. Ransom is extracted from the victim to "clean" the computer. Variations of this scam involve convincing the target that their computer is hosting child pornography, or that a "hitman" is intending to kill them. Another form of ransomware is malware that encrypts data on a victim's hard-drive; ransom is paid to be able to decrypt the data.[27]

The Damage for Consumers and Industry

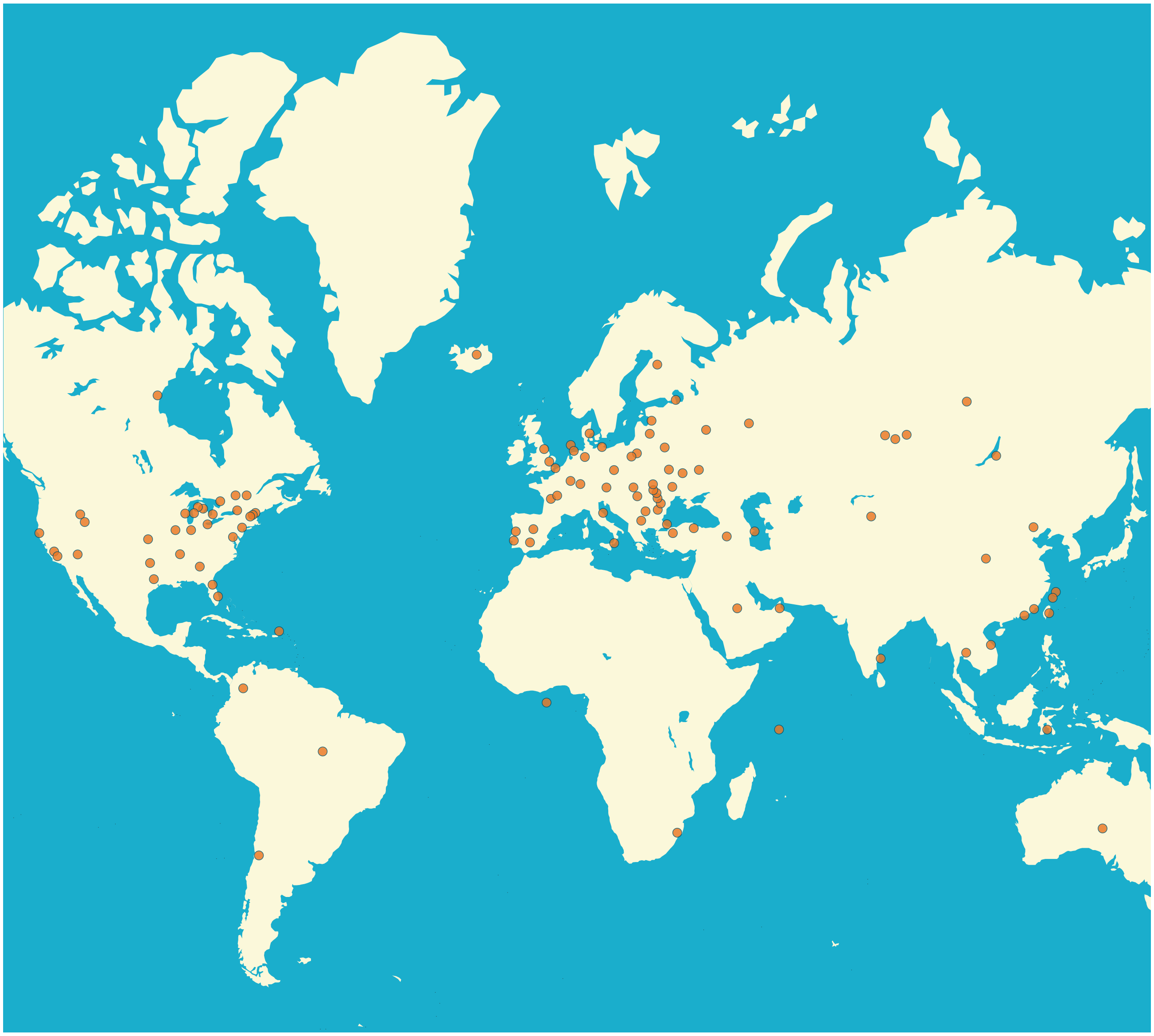
It is difficult to quantify phishing infection rates precisely. Work that is underway should help to remedy this.[28] Equally non-specific is the amount of money actually lost to financial phishing. That said, a stark example of the severity and frequency is provided by Automated Clearing House (ACH intra-bank transfers) losses to businesses in the United States. Security researcher Brian Krebs produced a map[29] of small and medium-sized businesses that incurred losses of hundreds of thousands of dollars due to these phishing schemes. Of the hundreds of incidents, a few are listed here, suggesting that total losses are staggering:

Western Beaver County School District	**US$704,610**
Bullitt County	**US$415,989**
Battle Ground Cinema	**US$81,000**
Shared Hope International	**US$179,000**
Patco Construction Company	**US$588,851**

Legions of Bots

Live statistical analyses of the millions of ongoing international attacks perpetrated by the Zeus and SpyEye botnets are available.[30] For context, the map below depicts command and control nodes for the Zeus botnet. Each dot indicates a control node, each of which controls tens of thousands of victim computers.

Ongoing research into data breaches and phishing is undertaken by dozen of organizations. The United States Secret Service, in collaboration with wireless carrier Verizon , produces a notable annual report.



Best Practices to Counter Phishing and Social Engineering

Although there is a wide range of anti-phishing best practices, this section is limited to techniques for outbound anti-phishing, available to organizations to protect their brand and their customers. Inbound anti-phishing protection has been well discussed in recent years. What is distinctive about the outbound approach is that it begins with mechanisms designed to develop trust among good actors, rather than beginning with a focus on malicious actors. This is done through collaboration among ESPs to allow services receiving messages to authenticate senders.

Many security solutions are expensive and difficult to use and consequently have not gained large-scale use. However, recent email-based authentication mechanisms facilitate inexpensive and easy protections against some forms of phishing and spoofing.

Authentication serves as a foundation, upon which reliable and accurate assessment capabilities can be built to make decisions regarding the handling of a message. It provides a validated identifier from which a reputation is built. Since the identifier is validated by a trusted party, there is little chance that an unauthorized or malicious actor can use it. The most common authentication mechanisms for email are SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) , which employ domain names as validated identifiers. The owner of a domain name is therefore the accountable party.

Classic spam filtering is based on heuristic algorithms making probabilistic assessments. No matter how good these algorithms are, they cannot be perfect; they sometimes produce false positives that declare that legitimate mail is spam, and false negatives, declaring that spam is legitimate. In contrast, authentication technologies perform rigorous validation of the identifier being used. They ensure that mail with the label is part of a stream of similar mail from the owner of the identifier; the use of that identifier cannot be spoofed. Hence all messages using it are taken as legitimately representing the owner. This permits a reliable assessment of the owner as a sender or author of mail. Misuse of the identifier without authentication is likely to be the work of a malicious actor. That is, these mechanisms make it possible to reliably validate legitimate mail and improve our ability to identify invalid mail.

In order to address the problems of phishing and domain spoofing successfully, brand owners and ISPs need to share information with each other about their email activity, such as policies for authentication and reports about problems. Historically, these arrangements were bilateral and private, between brand owners and individual ISPs. The results of an ad hoc industry consortium is a technical specification called DMARC (Domain-based Message Authentication, Reporting & Conformance) . DMARC, introduced in early 2012, leverages SPF and DKIM to provide brand owners with a means for easily communicating to ISPs how they would prefer any improperly authenticated messages to be handled. DMARC also provides ISPs with a mechanism for distributing back to brand owners aggregate feedback regarding the health of their email authentication deployment as well as forensic level intelligence.

EMAIL OPERATIONS AUTHENTICATION

Best practices dictate leveraging SPF and DKIM as a baseline for an email authentication strategy. This allows brand owners to verify the legitimacy of email that is distributed from their sending domains, confirming the sender's identity with the ISP community. If the identity of the sender cannot be authenticated, then ISPs may reject the message, or put it through additional filters to determine if it should be delivered. Without authentication, the chances of being filtered by major ISPs are greatly increased.

As with postal mail, underlying Internet mail services do not validate message authors or return addresses. Hence, the levels of assurance now required to counteract spam and phishing require additional mechanisms.

As with postal and telephony-based fraud, the underlying problem is social, not technical; technology can aid in its control, but it cannot eliminate it. Malicious actors are intelligent, motivated and adaptable.

Authentication is an integral tool in efforts to limit phishing and other fraud, and plays a key role in emerging reputation and accreditation systems.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO COUNTER PHISHING AND SOCIAL ENGINEERING

1. Implement authentication mechanisms.
2. Leverage authentication mechanisms in developing assessment capabilities regarding the handling of messages.
3. Brand owners and ISPs need to share information about their email activity.
4. Leverage SPF and DKIM as a baseline for an email authentication strategy.

Authentication Basics

Authentication begins with an identifier. For SPF, it is the domain name in the message's return address in the envelope (called the "Mail From" identity). Through special records in the DNS, SPF links the domain name to specific Internet addresses (IP addresses); these refer to the machines that are authorized to transmit mail that has the domain name in the return address. SPF information in the DNS also can declare whether mail with that return address is required to go through the listed IP addresses or whether it might come through other machines. SPF's assurance is based on the domain owner's control of entries in the DNS, under the listed domain name.

For DKIM, the identifier is a domain name that is distinct from any other identifier in the message and recorded in a special DKIM header field ("DKIM-Signature"). An entry in the DNS, under that name, provides cryptographic information. As with SPF, the premise to DKIM security is that only the owner of the domain can list information under that domain name in the DNS. Rather than registering IP addresses, DKIM uses a type of cryptographic "signature" that attaches the domain name to the message in a way that cannot be spoofed. An artifact of the signature technology is that some parts of the message are protected against undetected modification in transit.

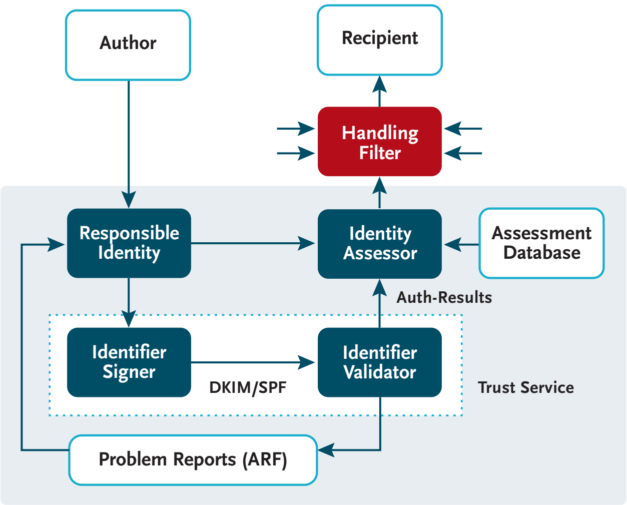
Neither SPF nor DKIM provide an assurance that a message is "safe" or "valid" or even that the actual author is the person who is listed in the author "from" field. Rather, they create accountability for the message: the owner of the domain name being used is agreeing to "some" responsibility for the message.

Adoption of SPF and DKIM has been quite good among major email providers like AOL, Hotmail, Yahoo! and Gmail. In addition, businesses are broadly adopting authentication across all their domains, not just those associated with a large volume of commercial email. This includes domains used for corporate email, customer support and other services. While most online fraud is associated with high-profile marketing domains, without authentication it is possible for any domain to be spoofed – and for critical business functions to be compromised.

For mail-sending operations, the recommended approach is:

- **Audit** – take an inventory of all machines and systems that send email on behalf of the organization, including external systems such as Email Service Providers (ESPs) or other authorized third parties.
- **Publish** – authentication and policy records in the DNS
- **Modify** – mail-sending software to use authentication and conform to policy
- **Establish** – reporting relationships for activity using the domain name
- **Monitor** – reports for patterns requiring attention
- **Maintain** – operations for on-going conformance

For mail-receiving operations, supporting these new mechanisms primarily entails adding modules to existing mail-filtering mechanisms:



References

Statistics

- Anti-Phishing Working Group Phishing Activity Trends Report / Domain Use Report
http://apwg.org/reports/apwg_trends_report_q1_2012.pdf
http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf
[N.B.: The APWG can provide spreadsheets of source data for its reports back to 2006, upon written request.
Contact: secretarygeneral@apwg.org]
- Anti-Phishing Working Group / U.S. Dept. of Homeland Security Crimeware Landscape Report,
http://www.apwg.org/reports/APWG_CrimewareReport.pdf
- The Anti-Phishing Working Group Web Vulnerabilities Survey
http://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdf

User-Facing Programmes

- The Anti-Bot Code of Conduct for Internet Service Providers
http://www.m3aawg.org/abcs-for-ISP-code
- iCode Australia - Internet Industry Association (Australia)
http://www.icode.net.au/home-why.php
[N.B.: this is also being adopted by South Africa]
- Cyber Clean Center - Japan CERT
https://www.ccc.go.jp/en_activity/index.html
- Anti-Botnet Advisory Center - ECO (Germany)
https://www.botfrei.de/en/
- STOP. THINK. CONNECT.
http://www.stopthinkconnect.org

Best Common Practices

- What To Do If Your Website Has Been Hacked
http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf
- Subdomain Registries Advisory
http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf
- Anti-Phishing Best Practices Recommendations for Registrars
http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
- Measures to Protect Domain Registration Services Against Exploitation or Misuse
http://www.icann.org/committees/security/sac040.pdf
- M^{3}AAWG Sender Best Communications Practices
http://www.m3aawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2a-updated.pdf
- Trust in Email Begins with Authentication (M^{3}AAWG Email Authentication White Paper
http://www.m3aawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf
- M^{3}AAWG /APWG Anti-Phishing Best Practices for ISPs and Mailbox Providers
http://www.m3aawg.org/sites/maawg/files/news/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf

Section 3
Domain Name System and Internet Protocol Exploits

A variety of illegal activities take advantage of vulnerabilities in the Domain Name System (DNS) and Internet Protocol (IP) addressing. Better management by network operators and improved practices by organizations that manage IP addresses can mitigate these threats.

Background

IP Addresses

Every computer on the Internet has an IP address, which is used to route traffic to and from that computer. Traditional IP addresses, known as IPv4 (Internet Protocol version 4), are 32-bit binary numbers, invariably written as four decimal numbers, such as 64.57.183.103. The first part of the address, in this case 64.57.183, identifies the network, and the rest of the address, in this case 103, the particular computer ("host") on the network.

The division between the network and host varies depending on the size of the network. A newer version called IPv6 uses much larger 128-bit numbers, written as blocks of digits separated by colons. Nearly all IPv4 addresses have been assigned, so in the coming decades there will be a gradual transition to IPv6.

For network traffic to flow from one computer to another, for example, from a user's PC to Google's Web servers or vice-versa, traffic from the sending computer flows through intermediate computers called routers to the destination.

There are about 400,000 networks connected to the Internet. The very largest routers, known as backbone routers, keep tables for all 400,000 networks. (They don't need complete routes, just enough to get to the next router on the way.) Other routers have information about networks to which they are connected, and send all other traffic toward a backbone router. To maintain the tables of 400,000 routes, backbone routers use a system called the Border Gateway Protocol (BGP) to exchange information about routes to various networks, so the routers can automatically adjust the tables when new networks come online or a link between networks fails or is repaired.

Like telephone numbers, every IP address must be unique. Internet providers and large businesses get blocks of addresses directly from Regional Internet Registries such as the American Registry for Internet Numbers (ARIN), which allocates IP space for North America, and the Réseaux IP Européens (RIPE) which allocates IP space for Europe, while smaller businesses and individuals use parts of blocks assigned to their Internet providers.

The Domain Name System

IP addresses are hard for humans to remember, and are tied to physical networks. The DNS is a distributed database that lets people use names like www.google.com rather than the corresponding IP address 173.194.73.105. Despite its enormous size, the DNS gets excellent performance by using delegation and caches. Since it would be impractical to store all of the names in the DNS in a single database, it is divided into zones that are stored on different servers, but logically linked together.

In principle, to find the address of Google's www.google.com, the DNS lookup software on a user's computer, known as a resolver, would first contact one of the "root" DNS servers, which would respond that for all names in .com, the resolver should ask one of a list of DNS servers that have authoritative information for .com (in this case, run by Verisign.) It then contacts one of the .com servers, which in turn replies that for all names in google.com, ask one of a list of DNS servers that have information for names in google.com (run, of course, by Google). It then contacts one of those DNS servers, which provides the IP addresses for www.google.com.

Internet users tend to look up the same names repeatedly. Every network and many individual computers have a cache that remembers recent DNS queries and answers, so if someone who uses the cache has recently asked for www.google.com, subsequent queries can be answered from the cache rather than going back to the master servers. Or if someone asks for mail.google.com or www.yahoo.com, the cache provides the servers for google.com (for mail.google.com) or the servers for .com (for www.yahoo.com), greatly reducing the number of queries to the master servers, and speeding responses to users.

There are a variety of ways that hostile parties can inject forged DNS data into caches and individual computers (some discussed below). A DNS extension called DNSSEC, for DNS Security, adds secure cryptographic signatures to data returned from DNS servers, so user computers can check the signatures for validity and ensure that the DNS data they use is valid, and actually came from the correct party. DNSSEC has been in development for a decade, but has only achieved significant use in the past year. The key management for DNSSEC is complex, and can present a challenge to managers of DNS servers.

DNS Exploits and Best Practices

The most serious DNS exploits are resolver exploits, in which bad actors introduce forged data to redirect Web and other traffic to false versions of popular websites.

A) Cache poisoning

One category of such exploits is cache poisoning, that is, using security holes to introduce forged data into DNS caches where it is then provided to victims' computers.

Few users will have any capability to detect false DNS information in use by their computers. By blending multiple exploits together, a perfect replica of any website, any trust seal, any logo, can be presented and show the correct domain name in the browser address bar. The result may be credential stealing, financial resource access, corporate or nation-state intelligence compromise, or just collecting re-directed advertising revenue.

Resolver exploits occur completely within the ISP and network operator's systems, needing no compromise of a user's computer. The most efficient mitigations are at the ISP or network operator's servers that provide DNS resolvers, where each preventive measure benefits all the users at once.

DNSSEC, when correctly deployed, will prevent cache poisoning and other DNS exploits. At this time, DNSSEC is not fully deployed, and is only effective in the parts of the DNS where the entire chain of DNS servers from the top level to the ones providing the addresses of Web servers implement it.

Even when DNSSEC is used everywhere, the software that carries out the DNSSEC validation steps must do so correctly to prevent falsified DNS server responses.

DNS server software requires diligent management to detect and correct bugs and exploitable vulnerabilities. Each time the software is updated, new unknown vulnerabilities might have been introduced by the update.

Even with 100% deployment of DNSSEC and bug-free DNS server software, operators of the DNS servers still need to promptly apply software updates to correct newly discovered software bugs, properly implement DNSSEC, and have good security hygiene for their own machines. If poor security hygiene allows an individual to hack into a DNS resolver or access it physically, that individual can again provide false answers to the users.

Interventions to detect the falsifying of DNS responses are possible if the monitoring system has a private, un-exploitable “other source” of DNS resolution data and periodically compares the responses the public is getting with the “known good” source.

Best Practices for Industry and Government to Address Cache Poisoning

1. Support the worldwide deployment of DNSSEC, to secure distribution of DNS data.
2. Support and test common DNS server software, to detect and report errors.
3. Support and test deployment of updated software at DNS resolver locations, to ensure that errors and bugs are fixed promptly.
4. Provide a Best Practice document for security hygiene for DNS resolvers, to educate network and system managers.
5. Conduct comparative spot monitoring to detect that DNS resolver exploits have taken place, to identify software vulnerabilities.

B) Malware That Targets the DNS

Another way to falsify DNS answers uses a technique employed by the recently publicized “DNS Changer” method. Malware modifies each user’s computer to change the DNS resolvers it uses, substituting hacker-controlled DNS resolvers rather than the user’s ISP resolvers. The individual who is controlling the DNS resolvers then selectively provides correct answers or falsified answers.

The DNS Changer malware worked not only on the users’ computers but also on the home or small business router. The advantage to altering the router settings is that the change is likely to be more long-lived and covers all computers, phones, iPads, TVs and other devices in the home or office – potentially home control devices, cameras, refrigerators, photo frames, wireless and wired networks, etc. The router may be within the broadband service provided modem or may be an extra device purchased and installed by the user.

The FBI recently worked with private industry to deprive the DNS Changer miscreants of their resources. The IP addresses used by the compromised resolvers were re-routed to accurate resolvers which ran for a few months while volunteer groups notified ISPs and users who were affected. Regardless of the FBI takeover of the DNS Changer IP addresses and recent shut off of those resources, users are still vulnerable to this exploit again in the future by new malware that uses different IP addresses.

Detection is possible at the ISP level by monitoring outgoing customer DNS traffic that goes to a resolver other than one that they provide. However, it is very common for technically advanced users – or those intentionally subscribing to a different DNS service – to send their traffic elsewhere. Careful design of the detection systems is necessary to avoid false positives.

In the future, users may be tricked into switching to a false DNS resolver by social engineering or some enticement. For example, if ISP resolvers are required to deny access to some DNS names, users may respond to offers that promise uncensored DNS access. There are many legitimate reasons to allow users to choose their DNS resolver service and the freedom for technically advanced users to make their own DNS queries without censorship or interference.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO ADDRESS DNS-TARGETED MALWARE

1. Educate for the public about the dangers of DNS resolver changes, to limit social engineering attacks.

2. Encourage network operators to share anonymized feeds of the top non-local DNS caches being queried from their networks, to identify possible rogue DNS resolvers.

3. Provide the feed to all vetted anti-abuse researchers to aid detection of services that have tricked users, or are falsifying DNS responses, and to distinguish them from legitimate DNS resolver services.

4. Develop metrics based on that aggregated data to help identify individuals for legal action, update a blacklist of fraudulent resolvers, and create coordinated mitigation operations such as occurred with DNS Changer.

5. Establish best practices for anonymization, sufficient to prevent connecting original users, their ISPs, and the DNS activity, to prevent retaliation against users who circumvent censorship, which would simply drive users to use harder to detect, but still possibly compromised DNS resolvers.

C) Non-technical DNS Attacks

Existing domain name registration processes often allow for the registration and use of new domains for a time without penalty and sometimes without cost.

The burden of detecting malicious use of domain names rests on the shoulders of anti-abuse researchers, often long after the malicious activity has begun, or sometimes ended. The burden of mitigating malicious domains is on every company that provides Internet access to users – either via requests to shut down malicious activities, or the often slow propagation of domain blocklists. Blocklists are necessary because requests to shut down or de-register domain names are often ignored.

The DNS registration system can be exploited by using stolen credit cards to register domains, by registering many domains at high speed using automation, and by using the domains maliciously within minutes after registration. Abuse researchers typically cannot observe newly registered DNS registration data for twenty-four hours. Blocklist operators take time to recognize malicious domains and then to propagate blocking information after the malicious act has been carried out.

Bad actors can create any subdomain based on domains they own, such as bankname.ssl-cgi.badactorexample.com. There is no limit on how many such names can be created at no cost. Fooling users doesn't require a brand name just anything that seems plausible. Names such as "secure-order.verification.badactorexample.com" are accepted by most users who assume it looks like other things they have seen.

Domain monetization services assist typosquatters in making money from domains that may include brand names or typos such as "SEARZ" or "PAYPA1" with a digit 1 instead of a letter L. While these domains may never be used in a phishing campaign, there are millions of such domains which make it difficult for abuse researchers to distinguish relatively harmless typosquats from the next malicious activity before it happens.

Phishers have used "look-alike" domains that have international characters which appear nearly exactly like a well-known website link, but can be registered without setting off any alarms because the brand name doesn't appear in the Latin character version of the domain name.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO ADDRESS NON-TECHNICAL DNS ATTACKS

1. Develop and intensify focus on detection of stolen credit cards used for registrations, to prevent malicious domains from being registered.

2. De-accreditation of registrars with excessive domains used for malicious purposes, and registrars who hide the true identities of owners.

3. Improve reputation algorithms to include domain age: domains more than a year old are less likely to be "throw away" domains. Some mail accreditors prevent clients from using domains less than a month old, and examining domains less than a day old is currently an effective way to preemptively find malicious activity.

4. Continue browser improvements and user education to recognize browser signals of extended validation certificates, and to prevent confusion by sites that use terms such as "secure" or "ssl".

5. Educate corporations to avoid sending user notifications that are similar to social engineering or phishing mail, or that are easily duplicated, to deter phishing and social engineering.

6. For sites and software that use domain blocklists, encourage a multi-layer approach with a variety of types of blocklists, including preemptive blocking methods as well as longer-lived but reactive block-lists, to improve blocking effectiveness

7. Support passive DNS projects such as ISC Security Information Exchange which provide early warnings to researchers about malicious subdomains actively in use.

D) Web and Other Server DNS Attacks

The reputation of legitimate domains can be exploited by breaking into legitimate Web servers and uploading malicious files. These files then become available with the legitimate domain in the URL. In order for domain blocklists to block this content, they would have to also block the legitimate content on the website.

Web redirections first present a domain with a good reputation – then redirect the user to the malicious destination site with an unknown reputation. Multiple levels of redirection are used, as are redirects to URLs with numeric IP addresses rather than domain names.

The success of such techniques depends on ineffective detection methods that stay at the superficial first level or fail to "act like a victim would" in following all the redirects. Unfortunately some marketers use multiple redirect levels to track customer response to marketing email. URL shortening services are often abused to redirect an individual from a well known domain such as bit.ly to a malicious website. It is difficult for a user to differentiate among millions of legitimate bit.ly URLs used to shorten a long Web address for Twitter posts, from ones that will lead to malware or an ad for illegal pill sales.

Differentiating non-malicious redirects from malicious ones puts an extra burden on abuse detection mechanisms.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO ADDRESS WEB AND OTHER SERVER DNS ATTACKS

1. Support a culture and mechanism that blocks compromised legitimate domains serving malicious content, along with rapid retest and delist; provide assistance to improve the security hygiene on all Web servers at the exploited site, to prevent the use legitimate sites.

2. Encourage URL shortener services to check and recheck all redirects in the chain for each redirection they supply, and to work with multiple abuse protection providers to identify new abusers, to prevent abuse of URL shorteners.

3. Develop educational tools and resources to identify and avoid URL shorteners without adequate anti-abuse measures.

4. Improve the effectiveness of URL reputation systems by training and testing, including testing redirects. Tests should appear to be a real user, should comply with policies regarding maximum redirect depth. These measures would limit abuse of URL shorteners and other URL services.

E) IP Attacks

IP attacks fall into two general categories: (i) computers lying about their IP addresses, and (ii) networks using ranges of IP addresses they are not authorized to use.

Each packet of data sent over the Internet includes the "source" IP addresses of the computer it was sent from, and the address of the computer it is destined for. It is possible for a hostile computer to put a false (spoofed) source address on outgoing traffic. For transactions in which the destination sends return packets back to the source address, notably the DNS, this can create unwanted traffic to the actual address that was spoofed. It is easy to send small DNS requests that provoke large DNS results, causing denial-of-service to the spoofed address

Each network can announce via BGP the ranges of IP addresses assigned to the network. Hostile networks can announce network ranges they are not authorized to use. This can steal traffic intended for the real network, or it can allow "stealth" traffic by announcing a range of addresses, performing an attack, and then withdrawing the announcement. Unless the victims are aware of the rogue announcement, they will blame the legitimate owner of the addresses.

In the early days of the Internet, address allocation was often done quite informally, with incomplete records. As a result, there is considerable legacy address space assigned to organizations that may have forgotten about it or gone out of business. Social engineering, (*e.g.*, forging documents or re-registering abandoned domains used in email) is used to gain control of address space.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO ADDRESS IP ATTACKS

1. ISPs and transit networks should filter traffic, keeping track of the range of addresses assigned to each customer network, and discarding traffic with source addresses outside the assigned range, to prevent their customers from sending traffic with spoofed addresses.

2. ISPs should implement BGPSEC (BGP security) to cryptographically protect route announcements and prevent publication of rogue data.

3. Regional Internet Registries should implement and follow procedures to verify the identities of purported owners of legacy space, to prevent bad actors from gaining control of address space.

References

- Wikipedia, Discussion of DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

- RFC 4034: Resource Records for the DNS Security Extensions. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005

- RFC 4035: Protocol Modifications for the DNS Security Extensions. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005.

- US CERT Vulnerability Note VU#800113, "Multiple DNS implementations vulnerable to cache poisoning", http://www.kb.cert.org/vuls/id/800113/

- DNS Changer Working Group, http://www.dcwg.org/

- Brian Krebs, "A Case of Network Identity Theft", http://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.html

Section 4 Mobile Threats

The Mobile Environment

With the advent of the smartphone and the applications markets for Android, Apple, Windows, and Blackberry devices, consumers are increasingly using their mobile devices to make purchases and carry out other financial transaction. iPhone, Android and iPad are the top three devices currently in use. Retail sales from mobile devices doubled to 11% of the overall e-commerce market from December 2010 to December 2011.

In the US, 79% of smartphone and tablet owners used their devices for shopping related activities in 2012, with 42% of tablet owners and 29% of smartphone owners having made a purchase with their device. In addition, 59% of U.S. consumers rated online shopping as their favourite way to shop, although 77% rated in-person shopping as the safest method.

Across the five leading EU markets (France, Germany, Italy, Spain, UK), mobile usage has nearly doubled since May 2011, with 20% of smartphone owners accessing retail sites and 15% making a purchase in May 2012.

Smartphone use is increasing fastest in emerging markets like India and China (a growth rate of 1050% and 172% over last year respectively). In the second quarter of 2011, revenue due to mobile commerce in China reached US$261 million. Additionally, a 2012 study of fifteen countries showed that 46% of online shoppers in China used a smartphone to make a purchase and that India and China spend approximately a third of disposable income online, the highest of all fifteen countries studied.

Globally, there are approximately six billion active mobile phones, equal to 87% of the world's population, up from 5.4 billion in 2010. In the first quarter of 2012 vendors shipped 398.4 million mobile units across the world (a slight decrease from 2011's 404.3 million).

There are 285 million mobile subscriptions in the U.S., with 54% of users owning smartphones. In Canada mobile subscriptions totalled 25.5 million by the end of 2011.

Apple expects that tablet sales will overtake those of PCs by the end of 2012, having sold a total of 55 million units by February 2012. Globally, 17.4 million tablets were shipped in 1Q12, of which Apple has a 68% market share.

App Markets

Unlike the PC software marketplace, where major applications are developed by a number of well known and trusted vendors, and users are less likely to install applications from less trusted sources, the mobile application ecosystem encourages end users to load large numbers of low-cost applications from smaller and often less trustworthy vendors, often including single-person enterprises. In many countries, most applications are obtained from app markets with inadequate security which feature apps peppered with malware. In other countries, users may be initially limited to loading applications only from phone OS vendor or carrier-approved app markets; however, users may override settings, allowing any app market to be shopped. Major phone OS vendors, including Apple, Google, and RIM operate high-volume application markets with tighter security. However, the scale of these markets makes it extremely difficult to prevent malware from occasionally being offered.

- Apple currently has 500,000 apps for sale, with paid apps generating US$4.9 billion since 2008.
- Android Market has 450,000 apps available, compared to 150k last year; averaging 1 billion downloads per month.
- RIM has 105,000 apps currently for sale and has averaged 150 million downloads per month since its inception in 2009.

As e-commerce has migrated to the mobile environment, bad actors and fraudsters have been quick to follow.

Particular Threats and Best Practices

A) Baseband Threats

There are several classes of baseband threats, including attacks in which an attacker creates an illicit GSM network and entices devices to connect to it, and attacks in which specially crafted messages attempt to exploit security holes in mobile devices. Both of these threats have grown as low-cost research and criminal GSM installations have proliferated.

Traditionally, operating a GSM (Global System for Mobile communications) network required a significant investment, which made research impractical outside of large institutions, limiting the discovery and exploitation of network-based attacks. For example, to spoof a GSM network, an attacker would need to operate a Base Transceiver Station (BTS). When GSM technology was implemented, network-based attacks against end devices were not much of a concern, so phones were not required to authenticate the networks to which they attached. Recently, free open-source software such as OpenBTS has allowed anyone to create their own GSM network at a fraction of the cost of carrier-grade equipment, bringing GSM security studies within reach of both security researchers and criminals.

There are well-founded concerns with over the vulnerability of mobile devices to exploits using specially-crafted data messages. For example, a device with insufficient verification of input parameters transmitted over the air interface which could lead to remotely exploitable memory corruptions in the baseband stack. The current low-cost cellular networks facilitate, as never before, research into and exploitation of such vulnerabilities.

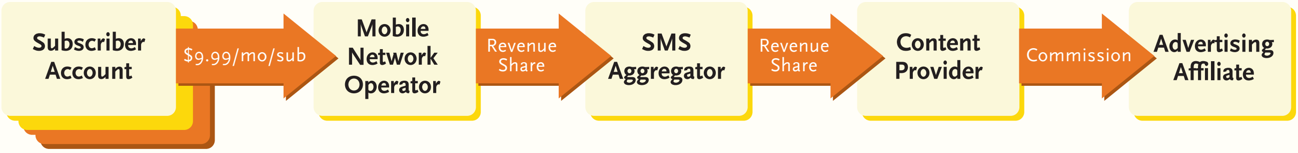
Attack scenario:

The attacker will operate a rogue Base Transceiver Station (BTS) in the vicinity of the targeted Mobile Station (MS). The rogue BTS sends out system information messages announcing the availability of a network that the targeted mobile station is willing to connect to. As the primary criterion for network reception is signal strength, the attacker can force the MS to connect to its rogue base station by simply transmitting with a stronger signal than the legitimate base station. This will not happen instantaneously, but the process can be sped up by using a GSM jammer to selectively jam the frequency of the legitimate BTS. This scenario is very similar to the one used by International Mobile Subscriber Identity (IMSI) catchers. Since GSM will not always provide mutual authentication, there is no protection against fake BTSs.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO PROTECT AGAINST BASEBAND THREATS

As carriers adopt new technologies (*e.g.*, 3G and LTE), handsets should be required to authenticate the carrier infrastructure to which they attach.

1. Service providers can work with handset manufacturers to also notify users when the handset opens a session that does not use mutual authentication, thereby alerting the user of this possible threat vector.



B) Fraud – Premium Rate Scams

Normally offered as services for voice and text applications billed to a subscriber's prepaid or postpaid telephone account, premium rate services include pay-per-call horoscopes, disaster-relief charitable donations, advice and chat services, monthly SMS love advice, and a wide range of other schemes.

Premium Rate Business Model

The desire to create a widespread, developer-friendly application ecosystem has led to complex and lengthy billing environments, such as the typical US$9.99/month SMS premium service subscription payment path, that are criminally-exploitable (depicted in the graph below).

In this example, a mobile network operator allows independent "SMS Aggregators" to obtain routing of a block of "short codes" (typically 4–7 digit phone numbers routable within some part of the global phone network). The SMS Aggregator then sells two-way SMS mobile connectivity to a horoscope application owner known as a content provider. The content provider pays a per-subscription commission to an advertising affiliate. Adjacent parties may be only loosely related.

The parties and relationships become progressively more problematic towards the right side of this diagram. In a number of cases, content providers permit poorly-authenticated Internet-only relationships with advertising affiliates to facilitate plausible deniability of their own or affiliates' spamming and/or fraud. Nearly anonymous payment mechanisms such as transfers to foreign banks, unregulated Internet virtual cash or online payment mechanisms lower barriers and enable spam to facilitate fraud.

Fraudulent exploits of Premium Rate Services have been occurring for many years, but the increased penetration of mobile services, the evolution of mobile data, and the establishment of a global cybercrime ecosystem have led to increases in the number and variety of attacks. Fraud may occur at nearly any step of the service or payment processes, from tricking the user into inadvertently using or subscribing to a service, an Affiliate falsely claiming subscriptions, to mobile malware that surreptitiously sends messages to Premium Rate Services without the knowledge of the subscriber.

A common exploit involves a fraudster who sets up a Premium Rate Service number, and places a "1-ring" voice call or sends a text message to a victim, hoping to lure them to respond.

Unauthorized subscription, "cramming" to Premium Rate "love advice" or other text message services by Affiliates and/or Content providers has been commonplace. This has caused many SMS Aggregators to implement secondary verification, typically involving a confirmation message or PIN exchange between the SMS subscriber and SMS Aggregator. But even these have been exploited; for example, the GGTracker Android malware sent US$9.99/month for an SMS subscription and confirmation messages without the subscribers' knowledge.

Spoofing the subscriber's identity, via unauthorized access to signaling networks or cryptographic exploits, is yet another method for committing Premium Rate fraud.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO PROTECT AGAINST PREMIUM RATE SCAMS

Premium Rate fraud is similar to many other kinds of cybercrime, and is therefore appropriately addressed by a number of common techniques including self-protection, consumer education, consumer protection and anti-malware measures.

The global mobile carriers association called "GSMA" has established a reporting service to allow subscribers to report SMS spam by forwarding messages to short code 7726 (which spells "spam"). Many carriers have adopted this code to receive reports from subscribers, however governments and enforcement agencies responsible for SMS spam in some countries have established their own numbers for reporting such as 33700 in France and 0429 999 888 in Australia.

Specific measures to protect against Premium Rate Scams include early defence, partner actions, and additional confirmation.

1. **Complaints to TSPs or Regulators:** These early defence mechanisms can provide early detection, before any money has been transferred. By including and enforcing anti-abuse clauses in their terms and conditions, TSPs and premium rate service platforms can stop payments to criminals before they occur. The TSP is warned at an early stage through complaints and enforces its terms and conditions, undermining the criminal's business case.

2. **Partner Actions Regarding Relationships and Payments:** Fraud depends on extracting monies to a hidden and/or unrecoverable location before the fraud is discovered. Parties may protect themselves by requiring full identification, qualification and/or authentication of other parties, by using reputable payment mechanisms and/or by delaying payment for a sufficient period.

3. **Additional Confirmations:** As many of the exploits involve cramming or falsified communication between adjacent parties in the payment chain, notifications and confirmations between more reputable parties can prevent or quickly identify fraud. Examples of this include an SMS Aggregator or Mobile Network operator confirm subscription with the subscriber rather than relying solely on assertions from the downstream side of the payment flow.

C) Mobile Spam

The following scenario is an actual account of recent international spamming activity along with the implications for international collaboration, particularly inter-carrier collaboration, as vital to anti-abuse defence of networks and subscribers.

Carrier A and Carrier B are in different countries; both countries have many speakers of the same language. Spam originating in Carrier A's network accounts for the majority of spam entering Carrier B's network in August 2012. Carrier A tracks spam in his network through shortcode-based spam reporting and analysis of messaging server logs. Carrier B has shortcode-based spam reporting, but does not collect the originating numbers of messages that are reported as spam. Carrier B does, however, perform automated anti-spam scanning on messaging traffic. As a result, Carrier B gathers information about sources and content of spam in his network.

Carrier A and Carrier B learned separately of the spam originating in Carrier A's network and being received by Carrier B. Carrier A shuts down spammers that he identifies on his network, but only if he has received a certain volume of spam reports against a given originating number. Thus, as long as a spammer in Carrier A's network sends only to numbers outside of Carrier A's network, he can send limitless spam to Carrier B's subscribers, since:

a. Carrier A will never receive spam reports from his own subscribers, his requirement for triggering a shutdown; and

b. No international common practices exist to thwart international spammers.

Without any data sharing among operators, spammers may operate quite freely *within a given country* if they take care to send their spam only to subscribers of operators *other than the network on which the spammer has his accounts*. Such targeting is common in the email world but so far has seemed less common in mobile spam, at least in part due to telephone number portability among carriers.

Data from the case described above show that Carrier A received zero spam complaints for more than 85% of the numbers sending spam from his network to Carrier B. Carrier A's own subscribers only sent spam complaints against approximately 5% of the numbers sending spam from Carrier A to Carrier B.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO PROTECT AGAINST MOBILE SPAM

1. **Dialogue and data-sharing:** Spammers exploit asymmetries among service providers in anti-abuse policies, defences and knowledge. One of the central lessons learned from the proliferation of Internet email spam from its infancy in 1993 to the present, when spam accounts for approximately 90% of all Internet email traffic, is that when ecosystem participants share information, it changes the game for spammers. Inter-carrier dialogue and data-sharing involving third-party enablers such as technology developers and industry bodies is vital to protecting the mobile ecosystem from spam and spammers migrating tools and techniques honed on the Internet over a decade or more to the open, increasingly IP-based and already globally interconnected mobile world.

While the following data points are not critical for collaboration among service providers, they are helpful to thwart spammers, and can all be obtained through spam reporting:

Data Elements	Notes
Mobile number of Spam originator	MSISDN (the unique number associated with a subscriber's handset) or IMSI (the unique number of a SIM card)
Number of Spam reports received	Requires collection and correlation of reports
Number of unique Spam reporters	Useful but not critical
Network of Spam originator	Derived by lookup

Note that none of the data elements identified above give personally identifiable information on the spam reporter. Information is only collected on the number being reported as originating spam.

As in the example of Carrier A and Carrier B above, data sharing of the elements above helps combat spam within a given country just as much as it does across country borders.

There are benefits and risks to the international, inter-carrier sharing of select data from spam reporting. Benefits include enabling remediation of voluntary subscriber complaints. Data-sharing and anti-spam dialogue among operators also facilitates their efforts to monitor, refine, and enforce their own Acceptable Use Policies. Finally, data-sharing can provide corroborating evidence for operator shutdown decisions, as well as for law enforcement, and regulatory actors. International, inter-carrier collaboration toward these goals will make it more difficult for mobile spammers to hide.

On the other hand, legal, privacy, and security concerns need to be studied when implementing any international collaboration in this space. Currently, these concerns act as an impediment to collaboration across borders. Note that, spam reports are voluntarily submitted by subscribers, it is not necessary to include any personally identifiable information (PII) when sharing complaint data, and it is not critical to include message content in the sharing of complaint data as sharing message content may increase the risk of accidental sharing of PII of reporters or persons other than the spammer. However, the content of messages reported as spam can also be helpful in identifying and blocking spam.

In summary, inter-carrier, international sharing of certain data elements changes the game for spammers as it leaves them fewer places to hide. Data sharing will require dialogue and consensus on the data to be shared as well as formats for data exchange among ecosystem participants.

D) App Store Security

Smart phones can be compromised by the installation of new software, usually obtained from a store controlled by the phone operating system (OS) manufacturer.

The Apple App Store has "apps" (short for applications, aka software) for iOS mobile devices. Google Play has apps for Android mobile devices. Android and iOS operating systems cover about 90% of the market share worldwide for smart phones as of August 2012. Of the remaining major smart phone operating systems, Blackberry phones are served by the Blackberry App World and Windows phones are served by the Windows Phone Marketplace.

When a smart phone is purchased by a consumer the phone is typically locked into a small set of "official" app stores (*e.g.*, the OS manufacturer's and the mobile carrier's). However, the user can reconfigure their phone to connect to unofficial or alternative app stores. This requires a varying degree of effort and skill depending on the phone type.

Mobile devices that use the Android operating system have a setting called "Unknown Sources" with a checkbox to "allow installation of non-Market apps". To access legitimate alternative app stores such as the Amazon Appstore, this checkbox must be on. Unfortunately the phone is then wide open to installing any unknown sources. Users can be more easily tricked into installing malware when it takes just one click. The malware writer gets a free pass without supervision by any official mobile app store once the Unknown Sources box is checked.

Official app stores have the ability to remove malicious apps from the users phone if that app was originally obtained from the same app store. Some malicious apps will be rejected prior to getting into the store if they violate the security policies set by that store.

However there are new ways to get past the app store restrictions even if the phone is configured to only use the official app store. Mobile device web browsers can be used to install HTML5 mobile apps which place an icon on the home screen of the device which looks the same as an app installed from an app store. Attackers can then exploit vulnerabilities in the stock browser than comes with the mobile device, or alternative browsers that the user may choose to install. Linkages from the browser to native functions of the device such as camera, microphone, phone diallers and geo location can be used by a criminal to obtain personal data and current activities of the mobile device user.

The username/password login that each mobile device uses to access the app store and authorize purchases is a significant point of vulnerability. Once in possession of these credentials, criminals can run up financial losses and install spying software. Both Apple and Google mobile operating systems presently require the same username and password as the keys to the app store and all other services including laptops, cloud file storage, contacts, calendar and email. Whereas a username and password would formerly have only allowed an attacker to access a subscriber's email account, the same credentials now provide access to the app store. In multiple cases, users have had laptops and phones wiped of data after criminals obtained this key information.

Various third parties offer anti-virus protection for some phones and make attempts to test all new applications in app stores for malicious activity or malicious intent.

Apple has placed more stringent restrictions on the review of apps before allowing them into their app store. The Google Play store has a less restrictive policy to get into the store but has removed apps which were already in the store and found to have malicious capabilities.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT FOR APP STORES

1. **"Application Neutrality":** Allow users to explicitly specify their "trusted" app stores, and perhaps the level of trust associated with each. This allows consumers to choose other reputable app stores without exposing them to risky app downloads from unknown sources.

2. Identify apps with malicious potential with rigorous security scans before allowing them into app stores instead of relying on complaints afterward.

3. Provide warnings, controls and education to users to reduce the incidents of users being tricked into following malicious instructions to get past security measures.

4. Improve security policies for app store password reset mechanisms to prevent criminals from obtaining app store credentials that do not belong to them.

5. Possible vetting of trusted app stores that adhere to certain security policies rather than limiting consumer choice to only one brand of app store.

6. Handsets may be locked to official app stores as an anti-competitive measure. While consumers may be well protected by this model, it invites consumers to employ workarounds that introduce security holes (*e.g.*, jailbreaking, rooting or unlocking devices). Policies that permit or assist in app-store locking should be weighed against the impact of the security holes created by the unlocking.

7. Encourage app stores to become members of botnet/online threats analysis centers, so that they can benefit from analyses, alerts, and reports coming from these centers. Malicious apps can then be detected, flagged and deleted in the swiftest way possible.

E) Mobile Malware

Malicious apps known as mobile malware exist for Android, iOS, and Blackberry devices. The vast majority of these apps are Trojan horse programs. Currently a majority of mobile malware target the Android platform. The Android platform is unique relative to iOS and Blackberry in that apps can be developed anonymously, whereas apps for iOS and Blackberry devices require application and/or developer verification before being certified and allowed to run on end user devices.

Most malware is or appears to be a useful application, and is distributed on websites or via unregulated app stores. Often these apps are legitimate ones that have been modified to include malicious code. Thus, users generally knowingly install these modified apps, unaware they contain malicious code.

Typically malicious code performs actions that generate revenue for the attackers. Direct monetization schemes cause direct financial loss to the victim and include malicious applications that can perform a wide variety of functions, including: sending premium SMS messages to a short-code registered by the attackers; downloading pay-per-download content; click pay-per-click links; make outbound phone calls to toll phone numbers; and intercept online banking credentials. Attackers can also generate revenue indirectly by collecting phone numbers for SMS spam, collecting device and user data for marketing, displaying advertisements, and selling commercial spyware applications. Commercial spyware applications allow a party to monitor a person of interest and collect device and user data such as SMS messages, emails, location, call logs.

Users are commonly tricked into knowingly installing and granting privileges to the malicious apps; attackers do not need to exploit a “security hole” to defeat security. While such exploits exist and have been used in malware, overall their existence in mobile malware is currently minimal.

Below are examples of malware for Android, Blackberry, and iOS.

Ikee (November, 2009): Ikee is a malicious iOS app that spread over-the-air (for example, across cellular and Wi-Fi networks) to jailbroken iOS devices. Jailbroken iOS devices are devices modified to remove default security restrictions. Other than spreading itself, Ikee changed the device’s background wallpaper to display a picture of 80’s popstar Rick Astley, in the tradition of the classic Internet prank known as “Rickrolling”. The worm was only capable of attacking devices that met three criteria: first, the device had to have been previously jailbroken by its owner; second, the owner must have previously installed an SSH (secure shell) application on the device, and; third, the owner did not change the default password.

ZitMo (September, 2010): ZitMo is a malicious Blackberry application. ZitMo is part of a two stage attack with the goal of compromising online banking accounts that use two factor authentication. Some banks require a special PIN code in order to login or perform wire transfers. The PIN code is sent to the user’s pre-registered phone number at the time of the transaction. During the first stage of the attack, the user’s Windows PC is infected with a malicious Windows application named Zeus. When a user visits their online banking website, Zeus tricks them into downloading and installing ZitMo on their Blackberry in order to access their bank website. When the PIN is sent to the user by SMS, ZitMo is able to intercept the SMS and send the PIN code to the attacker. The attacker then has the user’s online banking credentials captured via Zeus on the Windows PC, and the PIN code via ZitMo and can then carry out their attack.

Geinimi (February, 2010): Geinimi is designed to steal information from Android devices and add the compromised device into a botnet. Geinimi enables the attacker to launch attacks on third-party websites, steal additional device data, deliver advertising to the user, and cause the user’s phone to send premium SMS messages. To distribute these threats, the attackers obtained legitimate programs from Android marketplaces, added malicious code, and redistributed these modified versions on third-party Android marketplace websites. Users downloaded what they thought were popular, legitimate applications without knowledge of the extra malicious payload included in the packages.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT TO PROTECT AGAINST MOBILE MALWARE

1. Only obtain applications from reputable vendor application marketplaces that perform verification on applications or developers or directly from well-known application vendors themselves.
2. Review and understand permission screens, end user license agreements, privacy policies, and terms of agreement when installing new applications.
3. Maintain the default security restrictions on the device and do not jailbreak the device.
4. Evaluate the use of mobile security solutions such as mobile antivirus, secure browsers, mobile device management (MDM) solutions, enterprise mobile sandboxes, and data loss prevention applications to minimize the risk of infection and resultant impact.

F) Modifying Mobile Devices

Many Original Equipment Manufacturers (OEMs) and Mobile Network Operators (MNOs) establish secure mobile computing environments to maintain device stability, security, and uphold a positive user experience. In many cases, modifying these environments creates security vulnerabilities that may expose user information, enable theft of service in the form of unauthorized phone calls or text messages, enable remote control of device resources such as microphones or cameras to listen in or view without user knowledge, or enable an adversary to perform a long list of other unauthorized activities.

There are numerous techniques to modify the hardware and software of a device, but three of the more well-known modifications include “jailbreaking”, “rooting”, and “unlocking”.

Jailbreaking a Device

Jailbreaking is a term that describes the process to supersede the controls that an OEM implements on a device. OEM controls may be used to enforce application permissions, protect critical areas of the file system on a device, force applications to authenticate to the device, enforce password complexity, among many other management and administration functions.

Why do people jail break devices? One reason is that even though there are hundreds of thousands of mobile apps available, some people want to explore and load custom or modified versions of mobile apps. In some cases, a modified app may cost less than the official app, but may infringe on copyright; however, the less expensive app may contain malicious content.

Rooting a Device

Rooting a device is a process used to gain the highest user privilege of an operating system. Jailbreaking a device can be performed to supersede controls and elevate user access to gain root privilege to a device, which ultimately grants the user all privileges of the operating system.

Why do people root a device? In addition to loading custom or unauthorized apps and bypassing controls, root access enables a user to alter components and functionality of, or entirely replace the operating system on a device. Some mobile device operating systems are based on a form of UNIX with reduced command sets, freeing storage by eliminating functions not needed for most users of mobile devices. Rooting a device may enable a user to load additional commands as desired.

Unlocking a Device

MNOs may subsidize cell phone sales under a contract which requires the use of the MNO’s network for a period of time. In these cases it is common to use technical means known as “locking” to restrict the use of the phone to their own network. A device can typically be unlocked by entering a unique “unlock code.” Consumers can either find or purchase an unlock code online, or utilize a third party vendor who offers a unlocking codes and services for a fee.

BEST PRACTICES FOR INDIVIDUALS REGARDING MODIFICATION OF MOBILE DEVICES

1. Jailbreaking, rooting and unlocking devices in not recommended to anyone who seeks a standard, stable device with long-term OEM support as it may introduce vulnerabilities unknown to the user.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT REGARDING MODIFICATION OF MOBILE DEVICES

1. Develop and promote consumer education on and awareness of the risks of modifying mobile devices

Cross-particular Issues and Best Practices

A) Growth of Cross-border Exploits

As nations address internal attacks and threats, attackers quickly identify and exploit international vulnerabilities. For example, the North American "free iPad/iPhone" spam campaign originally targeted the United States. Canadian and U.S. carriers implemented technical defences blocking spam sent to their own subscribers. The attackers quickly identified this and began sending SMS spam to Canadian subscribers from U.S.-based phones, thereby evading defences. Similar cases exist in fraud, phishing, malware and spyware. And in most cases (*e.g.*, spam and malware defence), it has been found that stopping abuse at the source is necessary, as receiving nations may face a 'needle in the haystack' problem in identifying abuse hidden inside high-volume communications streams. Like the Internet, mobile communications networks are global, and require an international defence approach and international collaboration.

B) Blended threats

Mobile devices are now being used in the multi-factor authentication process for high value account logins. An example of the two factor authentication blended threat is a user visiting a financial website on their desktop computer and logging in with a user name and password as was done in the past. But now, the bank requires another step for the user to gain access to their account: receiving a call or text message on their cell phone with a code which the user then types into the desktop computer web browser. This extra step was added because so many users' desktop computers are infected with malware which has given away their banking password to criminals. Criminals have proven to be persistent in attacking each new method of protection. Now they need to compromise both the users' financial passwords and then their cell phone, and be able to relate the two together.

This makes phones an even more valuable target for criminals to compromise and gain control of. This control may be physical in the case of stealing the phone from the owner, or accomplished remotely with mobile device spying software. Either way, blended threats require more effort from criminals and are likely to target higher value accounts or higher value systems.

Mobile device apps are also used as token generators such as the six digit codes we used to see only on individually issued physical key fob two factor authentication devices. Google Authenticator and Amazon AWS Virtual MFA are two examples.

Depending on the vantage point a criminal operation has, they may be able to observe the content of traffic going to and from some mobile devices and pick up on authentication codes. This is the case with codes sent by email, which some banks offer as an option. SMS (text message) traffic is not encrypted.

The lack of a framework to share information regarding blended threats may itself be viewed as a threat; it allows a large number of exploits that could otherwise be suppressed. What is needed is to devise and implement defence strategies and frameworks that involve technical, policy, law enforcement, and legal entities in multiple countries.

Example: Zeus Mitmo (Man in the middle/mobile)

Zeus is a Trojan Horse application that targets Windows machines and attempts to steal banking information though browser keystroke logging coupled with form grabbing. The typical mechanisms for Zeus proliferation was through drive-by download activities and phishing attempts duping the user into navigating to a malicious site. It was first identified roughly in 2007 and has received many updates which have increased its sophistication, most recently being leveraged to attack within the mobile space. This update serves to benefit the Zeus malware since many companies including financial institutions are now using SMS as a second authentication vector, so having both the online username and password is not enough in the identity theft process. The evolution of this threat vector establishes an alternative planned by a Zeus gang: infect the mobile device and sniff all the SMS messages that are being delivered. The scenario is outlined as follows.

- The attacker steals both the online username and password using a malware (ZeuS 2.x).
- The attacker infects the user's mobile device by forcing him to install a malicious application either via SMS or via malware impersonating a legitimate banking or productivity application.
- The attacker logs in with the stolen credentials using the user's computer as a socks/proxy and performs a specific operation that needs SMS authentication.
- An SMS is sent to the user's mobile device with the authentication code. The malicious software running in the device forwards the SMS to another terminal controlled by the attacker.
- The attacker fills in the authentication code and completes the operation.
- The hackers then use this information to take over the victims' bank accounts and make unauthorized transfers to other accounts, typically routing then to accounts controlled by money mule networks.

D) International Considerations

Cybercriminals have a strong preference for operating in a transnational environment. For example, an illegal online pill seller living in the U.S. might send spam advertising those drugs from a compromised computer in Brazil, pointing potential purchasers at a website with a Russian domain name (while physically hosting that website in France). Credit card payments for orders might be processed through a bank in Azerbaijan, with orders being drop shipped from a site in India, and proceeds funneled to a bank in Cyprus. Criminals know that by operating in this manner, many factors complicate any official investigation into their online crimes, and reduce their likelihood of being caught. These factors include a lack of cooperation, differences from one jurisdiction to another, and the cost of international investigations.

Jurisdiction and International Cooperation

Law enforcement officers do not have unlimited powers. In particular, a law enforcement officer from one city or country will normally not have jurisdiction to investigate crimes or arrest a criminal in some other city or country. Cross-border investigations require international cooperation between the domestic and international police agencies, a process that may involve dauntingly complex formal processes, not to mention the time and resources required. The complications associated with these processes may delay investigations, or render some investigations impossible.

Statutory Coverage and Common Law Precedent

A given activity that's illegal in one jurisdiction, such as the U.S., may not be illegal elsewhere. For example, some countries may never have considered and/or passed a law outlawing email spam, nor have they criminalized the production of malware. In other jurisdictions, the legal system may not be able to keep up with a steady stream of new, chemically different but pharmacologically equivalent, drugs. In other cases, a law may be on the books, but the country may have no history of successfully prosecuting those who've violated that statute. If a criminal is working from such a jurisdiction, it may complicate the process of investigating, arresting, and prosecuting that offense.

Cost of International Investigations

Everything about operating internationally costs law enforcement more than working strictly local cases. If an investigator needs to travel to a foreign country, airfare and other travel costs may be substantial. Cash-strapped agencies may thus simply not be able to afford to work cases with international aspects.

Ironically, at the same time that it is expensive for a law enforcement officer to work a crime that has international aspects, cyber criminals are often able to purchase illegal goods or services abroad via the Internet at bargain prices. For example, a talented malware author from an economically depressed nation might be willing to write malware that will cause millions of dollars in damages for just a few hundred dollars.

All these and many other handicaps give cyber criminals a substantial incentive to work cross-border, and many in fact do.

BEST PRACTICES FOR INDUSTRY AND GOVERNMENT REGARDING CROSS-PARTICULAR ISSUES

1. **Collaboration:** The heart of effective international defence is collaboration. First, government and non-government parties in the affected nations must become aware of the issue. Next, collaboration is needed to devise and implement defence strategies and frameworks that involve technical, policy, law enforcement and legal entities in multiple countries. Major challenges in achieving the needed collaboration include identifying the right set of forums and obtaining appropriate attendance.

2. **Threat/Abuse Data Exchange:** One needed aspect of collaboration is the exchange of threat and abuse information. While human-to-human communications are needed, the breadth and scale of abuse (*e.g.*, the billions of daily spam and phishing messages) dictate the need for mechanized approaches. Here again, for a mechanized international framework to be successfully implemented, it must consider the obstacles to widespread implementation and adoption, including fragmentation among many disparate systems; differing functional needs of different nations (including legal impediments and technical/technological issues); and differing needs of different carriers. A general framework for abuse information exchange should also support peer-to-peer and centralized server models and identify both format and transfer protocols.

Conclusion

Since 2006, the online and mobile threat environment has changed dramatically, targeting a broader range of individuals, businesses, and networks. The emergence of new technologies allows for more sophisticated attacks to be developed by leveraging vulnerabilities across a broader range of services, channels and platforms.

Traditional methods to address online threats, with anti-virus software, firewalls, and education campaigns continue to be an important part of the defence. However, in the past few years, malware and botnets have emerged that transform themselves to avoid detection and remediation. To address these new and emerging threats, the international community needs to step further into the Internet ecosystem and collaboratively develop multi-faceted and multi-lateral approaches to combat them.

This report provides best practice recommendations for consumers, industry and governments to address online and mobile threats. These include recommendations for consumers to be more proactive in securing their own devices; for service providers to implement recommended security technologies and practices without delay; for governments to ensure modern regulatory and legislative environments are in place and enforced, and to work with international organizations to champion collaborative efforts.

These recommendations are a set of tools to manage online and mobile threats. However, the threats described in this report are a snapshot of the threat environment today. As online activities change, the use of mobile computing grows, and internet users and businesses change their responses and defences to existing threats, these threats will shift and change to exploit new vulnerabilities and pursue new targets.

Putting these recommendations into practice will take a concerted multi-lateral approach. To that end, the authors of this report strongly encourage the OECD to join with M^{3}AAWG and LAP to engage with the organizations that govern and administer Internet infrastructures. In addition, in order to stay in front of the changing threat environment, all organizations concerned should begin to more proactively collaborate in monitoring threats and implementing new measures as needed to address them.

Glossary

- **Border Gateway Protocol (BGP)** The protocol which makes core routing decisions on the Internet. It maintains a table of IP networks or ‘prefixes’ which designate network reach-ability among autonomous systems.[1]

- **Caches** Stores recently-used information in a place where it can be accessed extremely fast. For example, a Web browser uses a cache to store information regarding recently visited websites on your hard drive. Because accessing your computer’s hard disk is much faster than accessing the Internet, caching websites can speed up Web browsing significantly.[2]

- **Distributed Denial of Service (DDoS)** A type of cyber attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system. For example, sending either one or a large number of unwanted messages to keep a server or network from working properly.

- **Drive by Downloads** The unintended download of computer software from the Internet. A user may authorize a download without understanding the consequences, like a counterfeit executable program or the download can occur entirely without a user’s knowledge.[3]

- **Email Service Providers (ESPs)** A company that provides email services to other businesses. These services can include collecting and keeping lists of email addresses, sending bulk email to the addresses on the lists, removing addresses that bounce, and dealing with complaints and abuse reports caused by mass emailings.

- **Firewall** A hardware and/or software device on a computer that controls the access between a private network and a public network like the Internet. A firewall is designed to provide protection by stopping unauthorized access to the computer or network.

- **Global System for Mobile Communication (GSM)** A standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.[4]

- **Ingress filtering** A technique used to make sure that incoming packets are actually from the networks that they claim to be from, by blocking packets from fake IP addresses.[5]

- **International Association for Assigned Names and Numbers (ICANN)** Coordinates unique identifies including the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions.[6]

- **Money Mule** A person who transfers stolen money or merchandise from one country to another, either in person, through a courier service, or electronically. Online money mules typically exist as a result of phishing or malware scams.[7]

- **Node** In data communication, a physical network node may either be a data circuit-terminating equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

- **JavaScript** A scripting language which allows authors to design interactive web pages.

- **Phishing** An attempt to obtain personal information for identity theft or other sensitive information such as credit card numbers or bank account details for fraud. For example, an email message may appear to be from the receiver’s bank asking them to visit a website to confirm account details, but instead directs them to a false website where the personal information is collected.

- **Spoofing** Pretending to be another person or organization to make it appear that an email message originated from somewhere other than its actual source.

- **Typosquatters** Relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to an alternative website owned by a cyber-squatter. Once in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site; through the use of copied or similar logos, website layouts or content.[8]

- **VoIP** Routing of voice conversations over the Internet. This is distinct from a telephone call, which is made from your home or office phone which goes through the Public Switched Telephone Network.

- **Web injections** A type of security exploit in which the attacker adds code to a Web form input box to gain access to resources or make changes to data. Input boxes are typically for user authentication, however most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.[9]

References

1. http://en.wikipedia.org/wiki/Border_Gateway_Protocol
2. http://www.techterms.com/definition/cache
3. http://en.wikipedia.org/wiki/Drive-by_download
4. http://en.wikipedia.org/wiki/GSM
5. http://www.expertglossary.com/security/definition/ingress-filtering
6. http://www.icann.org/en/about/welcome
7. http://en.wikipedia.org/wiki/Money_mule
8. http://en.wikipedia.org/wiki/Typosquatters
9. http://searchsoftwarequality.techtarget.com/definition/SQL-injection

Footnotes

[1] http://Spamhaus.org and the Honeypot Project http://www.honeynet.org/

[2] http://www.dcwg.org/

[3] http://www.confickerworkinggroup.org/

[4] http://en.wikipedia.org/wiki/WinFixer

[5] http://blogs.technet.com/b/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx

[6] http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx

[7] http://krebsonsecurity.com/2011/05/weyland-yutani-crime-kit-targets-macs-for-bots/

[8] http://www.industrybotnetgroup.org/ecosystem

[9] http://www.microsoft.com/en-us/download/details.aspx?id=27605

[10] http://www.pcmag.com/article2/0,2817,2388652,00.asp

[11] http://www.pcmag.com/article2/0,2817,2388652,00.asp

[12] http://tools.ietf.org/html/rfc6561

[13] http://www.industrybotnetgroup.org/information

[14] http://www.safecode.org

[15] http://www.circleid.com/posts/20120223_fcc_releases_new_us_anti_bot_code

[16] http://www.m3aawg.org/abcs-for-ISP-code

[17] http://www.industrybotnetgroup.org. See also footnote 8.

[18] http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

[19] http://web.nvd.nist.gov/view/ncp/repository

[20] http://www.insaonline.org/assets/files/White%20Papers/INSA_Cloud_Computing_2012_FINAL.pdf (as of Sept. 17, 2012)

[21] http://www.forbes.com/sites/kevinjackson/2011/10/17/its-official-us-intelligence-community-is-moving-to-the-cloud/ (as of Sept. 17, 2012)

[22] https://www.fbiic.gov/public/2012/mar/2011IBMReport-March2012.pdf

[23] http://Apwg.org

[24] http://blogs.rsa.com/rsafarl/phishing-in-season-a-look-at-online-fraud-in-2012/

[25] http://en.wikipedia.org/wiki/Cutwail

[26] http://en.wikipedia.org/wiki/Zeus_botnet

[27] http://www.fbi.gov/portland/press-releases/2012/scam-warning-citadel-malware-delivers-reveton-ransomware-in-attempts-to-extort-money

[28] The American Federal Communications Commission Communications, Security, Reliability and Interoperability Council III exercise, particularly the botnet & malware working group http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii

[29] http://goo.gl/maps/dmQO7 reproduced courtesy of http://krebsonline.com

[30] https://zeustracker.abuse.ch and https://spyeyetracker.abuse.ch

[31] http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf

[32] http://www.antiphishing.org/reports/bestpracticesforisps.pdf

[33] http://www.openspf.org/

34 http://dkim.org/

35 http://www.icann.org/

36 http://dmarc.org

37 RFC 5321 http://tools.ietf.org/html/rfc5321

38 https://sie.isc.org/

39 http://therealtimereport.com/2012/05/03/mobile-commerce-online-retail-sales-from-mobile-devices-double-in-last-year/

40 Ibid.

41 http://blog.nielsen.com/nielsenwire/consumer/shopper-sentiment-how-consumers-feel-about-shopping-in-store-online-and-via-mobile/

42 http://www.fiercewireless.com/europe/press-releases/1-8-european-smartphone-owners-conducted-retail-transaction-their-device

43 http://www.mobify.com/blog/global-mobile-commerce-growth

44 http://www.chinadaily.com.cn/bizchina/2011-08/29/content_13208453.htm

45 http://utalkmarketing.com/pages/Article.aspx?ArticleID=23195&Title=Emerging_markets_spend_more_online

46 http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers

47 http://www.idc.com/getdoc.jsp?containerId=prUS23455612

48 http://arstechnica.com/tech-policy/2010/03/wireless-survey-91-of-americans-have-cell-phones/

49 http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use

50 http://www.computerworld.com/s/article/9225437/Are_Tablets_Inevitable_as_PC_Replacements_

51 http://www.idc.com/getdoc.jsp?containerId=prUS23466712

52 http://macworld.com/article/1164973/apple_reports_record_revenue_profit_for_fiscal_first_quarter.html

53 http://www.guardian.co.uk/technology/appsblog/2011/nov/22/android-paid-apps-revenues

54 http://googlemobile.blogspot.ca/2012/02/androidmobile-world-congress-its-all.html

55 http://business.financialpost.com/2012/09/25/blackberry-jam-2012-live-coverage/

Contributors

J. Trent Adams, Senior Security Standards Advisor, PayPal

Alex Bobotek, Lead, Mobile Messaging Anti-Abuse Strategy and Architecture, AT&T Labs; Co-Chairman, M^{3}AAWG

John Levine, President, Coalition Against Unsolicited Commercial Email (CAUCE) North America; Senior Technical Adviser, M^{3}AAWG; Chair, Anti-spam Research Group of the Internet Research Task Force

Chris Lewis, Chief Scientist, Spamhaus Technologies

April Lorenzen, CTO, Dissect Cyber Inc.; M^{3}AAWG Senior Technical Adviser

Neil Schwartzman, Executive Director – CAUCE – the Coalition Against Unsolicited Commercial Email

George Yee, IT Research Analyst, Office of the Privacy Commissioner of Canada

Frank Ackerman, Director Self-Regulation, ECO; M^{3}AAWG Public Policy Committee Co-chair

Chris Boyer, Assistant Vice President, Global Public Policy, AT&T; M^{3}AAWG Public Policy Committee Co-chair

Rudy Brioche, Senior Director and Policy Counsel at Comcast Corp

Betsy Broder, Counsel for International Consumer Protection at Federal Trade Commission, Office of International Affairs

Peter Cassidy, Secretary General, Anti-phishing Working Group

Will Clurman, VP Sales, Cloudmark

Eric Chien, Technical Director, Symantec

Dave Crocker, Principal, Brandenburg InternetWorking

Wout De Natris, Owner, De Natris Consult

Toni Demetriou, Senior Investigator at New Zealand Department of Internal Affairs

Richard Gane, Government of New Zealand, Department of Internal Affairs

Sid Harshavat, Senior Principal Architect, Symantec

Michael Kaiser, Executive Director at National Cyber Security Alliance

Alain Kapper, International Liaison, U.K. Office of Fair Trading

Masatoshi Kubota, Ministry of Internal Affairs and Communications, Japan

Steve Mays, Founder, Message Bus Inc.

Jesse McCabe, Director, Product Marketing, Return Path, Inc.

Tice Morgan, Principal Architect, Mobile Security, T-Mobile

Steve O'Brien, Manager, Censorship Compliance for Secretary for New Zealand Department of Internal Affairs

Michael O'Reirdan, Engineering Fellow at Comcast Cable; Co-chair, M^{3}AAWG

Eunju Pak, Senior Research Associate, Korea Internet & Security Agency

Jean-Jacques Sahel, Director, EU Institutional Affairs and International Organisations, Microsoft

Joe St Sauver, Ph.D., Nationwide Security Programs Manager, Internet2 and the University of Oregon

Tomas R. Shaw, Chief Information Officer, OITC

Kevin Sullivan, Technology and Policy Strategist, Microsoft

Ken Takahashi, General Manager, Anti-Phishing Solutions, Return Path, Inc.

Andy Tillman, U.K. Office of Fair Trading

Jean-Christophe Le Toquin, Director, Digital Crimes Unit, Microsoft EMEA (Europe, Middle-East, Africa)

Jerry Upton, Executive Director, M^{3}AAWG

Brooke Watts, Director of Marketing, Message Bus Inc.

Jeff Williams, Principal Group Program Manager, Microsoft

Tom, SURBL (surbl.org)

André Leduc, Manager, National Anti-Spam Coordinating Body, Industry Canada

Andy Kaplan-Myrth, Policy Advisor, Industry Canada

Lisa Foley, Policy Analyst, Industry Canada

Kate McIlroy, Policy Analyst, Industry Canada