Combatting Botnets Through End-User Notification

A View of Emerging Practices Across the Ecosystem

Released December 10, 2012

The Online Trust Alliance (OTA) is a non-profit organization formed with a mission of enhancing online trust, while promoting innovation and the vitality of the internet. OTA's goal is to educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

Contributors

OTA wishes to thank and acknowledge the following individuals and companies for their collaboration, input and guidance. While the paper represents the working consensus of OTA member companies and the workshop participants listed below, it is not likely that all recommendation are supported by every company.

Pat Peterson	**Agari***	Andrew Pynes	**Comodo**
Matt Carothers	**Cox Communications**	Thea Singer	**Critical Change***
Joel Lang	**CSID**	Ben Wilson	**DigiCert***
Mark Hammell	**Facebook**	Barry Greene	**GETIT**
Eric Davis	**Google**	Damian Menscher	**Google**
Tim Rohrbaugh	**Intersections Inc***	Rod Rasmussen	**IID (Internet Identity)***
Paul Ferguson	**IID (Internet Identity)***	Joe St Sauver	**University of Oregon***
Brendan Ziolo	**Kindsight***	Brennen Reynolds	**McAfee**
John Scarrow	**Microsoft***	Kevin Sullivan	**Microsoft***
Pat Barnes	**Nominum Inc.**	Ken Baylor	**NSS Labs***
Craig Spiezle	**Online Trust Alliance***	Bill Smith	**PayPal***
Andy Steingruebl	**PayPal***	Don Blumenthal	**Public Interest Registry***
Wolfgang Kandek	**Qualys**	Tom Bartel	**Return Path***
Maria Eriksen-Jensen	**Secunia***	Maxim Weinstein	**StopBadware***
Mark Goldstein	**Safe-Secure-Privacy***	Patrick Gardner	**Symantec***
John Harrison	**Symantec***	Geoff Noakes	**Symantec***
Manish Goel	**TrustSphere***	Tom Byrnes	**ThreatSTOP**
Bob Lord	**Twitter***	Peter Fonash	**US Dept of Homeland Security**
Danny McPherson	**VeriSign Inc***	Francis Bergen	**Xerocole, Inc.**
Rob Fleischman	**Xerocole, Inc.**		

** Member of Online Trust Alliance*

Table of Contents

Executive Summary

Botnets represent a complex problem impacting users, businesses and governments worldwide. Their impact ranges from mere annoyance to significant productivity losses. They are responsible for the distribution of billions of unwanted emails daily spreading malware and spyware that compromise personal information and the security of critical infrastructures that support our modern world.

Responding to the threats that botnets present requires a renewed commitment to multi-stakeholder efforts, through collaboration and data sharing. No single organization can possibly take on this challenge alone. Thus, an ecosystem wide approach to fighting botnets and malware yields significant benefits. An Antivirus Vendor (ASV) can detect many threats, but only on the systems running their software. An Internet Service Provider (ISP) can detect threats on a network, but that detection is only as good as the ISP's threat intelligence and monitoring capabilities. A social networking site can detect malware by looking at user behavior, but only malware that targets its own site. A bank can detect fraudulent transactions from zero-day malware that no one else has seen, but only if the malware targets the bank's organization. By using complementary detection, notification techniques, and sharing data, the ecosystem can address problems more quickly and limit damage to the extent possible.

When combined, these tactics create an integrated model, the OTA Botnet Multi-Stakeholder Ecosystem, including a shared responsibility involving both the public and private sectors. The five primary elements include:

- Prevention – Proactive activities which can reduce the vulnerability of a user's device
- Detection – Efforts aimed at identifying threats on a device or network
- Notification – Steps to inform a user or responsible entity of the issue
- Remediation – Actions to remove malicious software from a compromised device(s)
- Recovery – Actions to resolve impact to a user's identity from theft, account takeover, credit card fraud and related damages resulting from a botnet.

To develop the OTA Botnet Multi-stakeholder ecosystem, OTA solicited input from over 100 companies and organizations. Together we investigated collaborative initiatives and opportunities to address the challenges Botnets present to the ecosystem. The results of this outreach (through survey and facilitated telephone interviews), led to an OTA sponsored, full-day workshop in October 2012, focusing on End-User Notification best practices. These combined efforts and learnings are represented in the paper.

Preliminary List of Best Practices

1. Subscribe to trusted data sources to obtain information on potentially infected users.
2. Instrument existing systems to observe potentially compromised users.
3. Perform usability testing procedures to determine the most effective methods of user notification.
4. Design user notifications that are easily recognized by users as legitimate and distinguishable from fraudulent notifications.
5. Ensure that notifications lead to successful remediation by considering the entire user experience.
6. Construct notifications in the tone, reading level and language appropriate to the target audience. Consider multi-lingual phone support, notifications, tutorials and visuals.
7. Maintain trusted relationships between providers and users - do not simply direct them to third parties with whom they may not have a relationship.

Background

Botnets impact all users and infrastructure placing all devices at risk. This is monumentally important to individuals, companies and the government. The current trend for users moving to mobile devices unfortunately provides an environment ripe for botnets to flourish. This further increases the reach of botnets and the economic impact on businesses, banks and consumers.

Common distribution vectors for botnets include forged email carrying or leading to malicious payload. Additionally, compromised websites can distribute malicious advertising which can impact hundreds of thousands of unsuspecting site visitors within the course of a few hours.[1] [2] Sophisticated criminals create and iterate the functionality of botnets - evolving the techniques by which they deceive users. Botnets are increasingly targeting business users, government employees and consumers on a growing list of devices ranging from traditional computers, mobile phones and network equipment independent of their device, manufacturer or operating system.

Significant efforts have been initiated to mitigate botnets. Law enforcement including the FBI and Secret Service, academia and industry; along with leading ISPs, the AV community and other stakeholders have made significant efforts. Combined they have made progress in taking

[1] https://otalliance.org/resources/authentication/index.html

[2] Malvertising https://otalliance.org/resources/malvertising.html

down a large number of botnets and have voluntarily published best practices to assist others' efforts in this arena. [3,4, 5]

While individual organization's efforts are promising, we lack a holistic and integrated approach. For example, timely notifications to users of infected devices are critical. But such notifications cannot, in themselves eradicate the problem. The lack of more effective prevention practices means many devices will likely be re-infected within 90 days.

Recognizing the criticality to the economy and national security, the U.S Department of Commerce and U.S. Department of Homeland Security issued a request for information (RFI) on bots in September 2011.[6] OTA responded recommending for the formation of a multi-stakeholder effort to document and share best practices[7]. To spur information sharing, yet maintain confidentiality, it was suggested this be a closed forum.

OTA has since formed a multi-stakeholder working group to establish best practices. Unlike those being driven by trade organizations with limited participation, this group is building upon existing work including representatives of the ISPs, AV, security community, financial services sector and technology communities. [8]

To develop the OTA Botnet Multi-stakeholder model, OTA solicited input from over 100 organizations regarding collaborative initiatives. A full-day workshop in early October 2012 focused on user notification best practices. Future workshops are planned to focus on other best practices. Attendees represented a balanced composition of stakeholders with technical, operational and business skillsets. To encourage collaboration a workshop facilitator was retained and attendees agreed to "Chatham House Rule".[9] The goals of the workshop were to:

- Focus on what processes work (emerging best practices).
- Define how they can be refined, shared and more broadly adopted across the ecosystem.
- Understand and address future challenges in the space in order to effectively protect users.

---

[3] FBI Botnet Operation http://www.fbi.gov/news/stories/2011/april/botnet_041411/

[4] Microsoft Hands Case to FBI http://news.cnet.com/8301-10805_3-20109864-75/microsoft-hands-rustock-botnet-case-over-to-fbi/#!

[5] FCC Anti-Botnet Code of Conduct for ISPs. Note the adoption of the code is voluntary and based on limited reporting and disclosure, adoption by ISPs remains inconclusive and limited at this early stage. https://otalliance.org/resources/botnets/20120322%20WG7%20Final%20Report%20for%20CSRIC%20III.pdf

[6] https://www.federalregister.gov/articles/2011/09/21/2011-24180/models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of

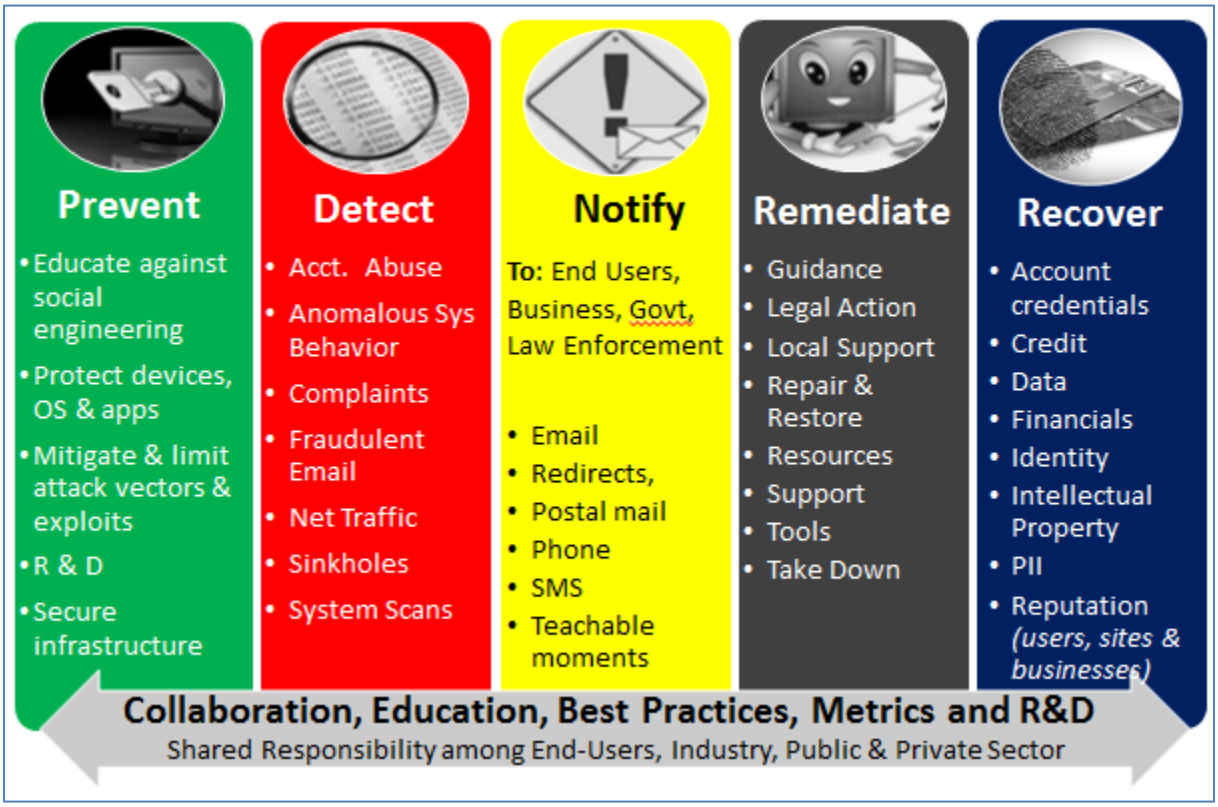
[7] OTA response to Commerce Department RFI Nov 14, 2011 https://otalliance.org/docs/OTA_DOC_BOTSFinal.pdf

[8] In March 2011 OTA Executive Director Craig Spiezle was appointed to the Federal Communication Commission's Communications Security, Reliability and Interoperability Council (CSRIC) http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii

[9] http://www.chathamhouse.org/about-us/chathamhouserule

The Anti-Botnet Ecosystem

In late 2011, the Online Trust Alliance developed a Botnet Taxonomy and Ecosystem model. Five primary functions were identified to address the threat and impact of botnets. A key premise of this model is the interdependency of functions and roles. Other important factors include; timely data sharing, collaboration, and education for users, businesses and industry.



The five pillars of the Anti-Botnet Ecosystem model are:

- **Prevention** – Proactive activities which can reduce the vulnerability of a user's device.
- **Detection** – Efforts aimed at identifying threats on a device or network
- **Notification** – Steps to inform a user or responsible entity of the issue
- **Remediation** – Actions to remove the malicious software from a compromised device(s)
- **Recovery** – Actions to resolve impact to a user's identity from theft, account takeover, credit card fraud and related damages resulting from a botnet.

A Shared Responsibility

A key component for this model's success will be a shared ownership from stakeholders across public and private sectors. The burden of fighting botnets should not rest solely on a single industry sector. We all have responsibility in employing voluntary best practices for the good of the ecosystem. Users have the responsibility to keep their system/device patched and maintained, and to exercise safe computing practices. Without user involvement and education, we will continually play "whac-A-mole", with devices that continually become re-infected.[10] Past efforts have focused on specific segments such as ISPs or software vendors. It is now necessary to look at the intersection of these efforts to develop the most creative, resilient and effective solutions.

Benefits of the Multi-Stakeholder Ecosystem Approach

A collaborative approach affords blended capabilities with complementary solutions. As previously mentioned, it is unlikely for any single organization to address each of the five pillars on their own or have the ability to see the threats targeting others. For example;

- An AV vendor can detect many threats, but only on the systems running that AV software and may not have visibility to what others are seeing.
- An ISP can detect threats on its network, but that detection is only as good as the ISPs threat intelligence and monitoring capabilities.
- A social networking site can detect malware by looking at user behavior, but only malware that targets their site.
- A bank can detect fraudulent transactions from previously unseen malware, but only if that malware targets the bank.

The ecosystem approach enables feedback loops for sharing threat intelligence. Take a simple example: a bank detects a fraudulent transaction and shares the originating IP address with the ISP. The ISP then examines network traffic from that IP address to determine the control channel. That can be shared with AV vendors and network-based detection vendors. Security vendors then update signatures so other infected devices can be identified and remediated. Then other users can be notified and their devices are protected from infection or cleaned before they can compromise the bank or site. This cross-stakeholder cooperation benefits each entity as well as their customers.

Cooperative ecosystem approaches can improve timeliness of response, and limit potential damage of botnets. Using complementary detection techniques, problems can be addressed in the shortest possible time and minimize the botnets impact and spread. In the ideal scenario a new botnet can be identified and steps taken to remediate infected devices before serious harm or data loss takes place. By sharing detection information, we can minimize the real world impact of an infection. Under this scenario, an ISP detects an infected IP address through network traffic analysis and passes that IP address to financial institutions. Financial institutions can then refuse transactions or prompt for further authentication for any sessions from that IP, preventing fraud before it starts.

[10] http://en.wikipedia.org/wiki/Whac-A-Mole

A collaborative, multi-stakeholder approach can have similar positive benefits with regards to botnet user notification. There is broad consensus from the working group that multiple points of user notification and education will drive user action. Imagine if an infected user got an email or other notification from their ISP, a banner from Google, a warning and secret question prompt from PayPal, and a walled garden from Facebook all in the same day. If a user repeatedly sees similar messages from multiple sources who they have a relationship with, it is more likely they will take action to remediate the threat or vulnerability. [11]

Overview of the Problem

Malware and botnets are global problems that affect all users, from residential users and small businesses to Fortune 500 companies and government agencies. With few exceptions they are individually ill-equipped to defend their systems and data against these attacks. These attacks (including social engineering, data and policy corruption, code manipulation and malware, worms, viruses, flooding, black-door implants, etc.) have created fear and doubt, confusion, and significant dollar and reputation losses. Additionally, they introduce inaccuracies, malfunctions, and denial of service, induced failures, data exfiltration, malfunctions, performance loss, and other problems, to systems across the internet.

In the recent example of DNS Changer,[12] over one million users had their DNS server silently changed to one controlled by an attacker. This attack prevented AV updates and redirected users who unknowingly visited malicious sites with drive-by downloads.[13] Complicating efforts to respond to this attack, this exploit to successfully modified routers which had default passwords, hampering effort to remove the infection.

The rapidly emerging trend of using personal devices in the workplace for accessing business networks is further complicating the landscape. Bring Your Own Device (BYOD) blurs the lines between traditional work and personal lives, and complicates matters greatly for IT and security managers. Users' devices are not under careful watch and control of security or IT resources – they may be more likely to have unpatched vulnerabilities or be compromised. This presents another dimension to corporate security altogether. Additionally, malware is increasingly targeting mobile devices. Prohibiting such devices in the work environment is not necessarily the best answer, but allowing and not managing such devices can damage the corporate security posture. This convergence is rapidly pushing the intersection of corporate and consumer security concerns.

Fighting botnets and malware is an arms race. Botnet operators and malware authors continue to evolve their craft despite the rising defense put forth by corporations and the security industry. They frequently update their techniques to evade security solutions. Past approaches of matching signature profiles, fingerprints and heuristics may now have limited effectiveness.

---

[11] Companies referenced in this example are for illustrative purposes and may not represent current or planned service offerings.

[12] http://www.fbi.gov/news/stories/2011/november/malware_110911

[13] Drive by downloads occur when a user visits a site and without their knowledge or direct interaction such as clicking on a link or accepting a download. The computer virus, spyware, malware, is executed and installed on their device targeting an existing application or device vulnerability.

Botnet authors create multitudes of variants within the same generation of malware producing greater than 100,000 variations and completely new botnet platforms by iterating their code. It's crucial to take a layered approach to security. For instance, by detecting malicious communications in the network. It is safe to assume that as long as the economic incentives remain, cybercriminals will continue to find new ways to compromise machines and evade detection.

Emerging Practices

Our focus on best practices is not aimed at prescribing a one-size-fits-all approach, but rather to build upon others' success, refine the ideas, and foster greater adoption of practices that help protect users. This is especially true in cases where best practices from one industry can be adapted to serve another, or what works for an international service provider can apply to a regional community-based service. Reasonable and appropriate regulatory solutions may limit use of ideas in certain sectors. There have been continuous efforts over the last several years to create solutions across the anti-botnet ecosystem, from prevention and detection, to notification of users when problems are detected, and assisting affected users in remediation and recovery. Each of the five areas of the ecosystem has contributed ideas through managing its own challenges, and has also reaped benefits from a cross-organizational and cross-industry approach to collaboration.

Kicking off the workshop, subject matter experts and organizations deeply involved with anti-botnet efforts, provided mini-case studies and overviews of their respective efforts to-date. Concise summaries of botnet problems and research on solutions were shared by nine experts representing seven well-known and respected companies, one governmental agency and a non-profit organization.

Following is a summary of key points and discussions from these presentations. To maintain confidentiality, the names of the presenters and organizations have been omitted.

Actionable Information Sharing

A representative of a major software company began the presentations with an overview of the major botnet disruptions that the company has addressed since 2010. In addition to shutting down or reducing the effectiveness of the botnets, a key outcome of these efforts has been the intelligence gained concerning the extent of the infections on computers around the world. Specifically, they gained insight regarding IP addresses of computers that were formerly part of the botnet. This data is critical to the notification process - allowing ISPs and other service providers to identify specific users impacted by malware.

Many organizations take this approach to collect then distribute data about compromised computers. Domain names or IP addresses formerly used by malware are pointed to systems known commonly as "sinkholes". These sinkholes capture traffic from infected PCs that was intended for the botnet controllers. The sinkhole systems are benign, but allow observation of the IP addresses that attempt to connect to them. Commonly this data is distributed to network owners and Community Emergency Response Teams (CERTs) around the world who can use this information to notify infected users.

Evaluating Detection Systems that Enable Notification

Not all data on infected systems is collected and reported by third-party organizations. Increasingly, due to their position in the network, service providers are deploying systems to detect and notify infected users. Several commercial products provide this functionality. When evaluating detection systems, there are several key requirements that need to be met:

1. Accurately detect that a user is infected: If you are going to notify a user that they have a botnet infection and lead them through a remediation process, you have to be very confident that they are actually infected.[14]
2. Positively identify the malware involved: It is also important to identify the type of botnet that they are infected with. This lends considerable credibility to the notification and assists in customizing the remediation process.
3. Provide coverage for a wide variety of malware: As noted above, malware is constantly changing in order to stay ahead of existing detection technologies. That's why technologies that look at more types of traffic provide better coverage.

With these requirements met, detection technology can then be confidently combined with a variety of notification techniques and remediation processes. Collectively they provide a valuable service to an ISP's subscribers to help keep their experience safe from botnets.

Notification Delivery and Design

Many participants shared their organizations' experiences regarding the creation and delivery of notices to users who have been impacted by malware. The notices can range from logon redirects to notification landing pages, from simple email notifications, to in-browser service notifications, and they may even include outbound phone calls to users. This has been one of the most public facing efforts to respond to malware. While progress is being made, we are in the early phases of evaluating effectiveness and understanding what elements of a notification are most likely to be effective.

There are many challenges to effective and efficient notification. As with other security notices, many users have become de-sensitized to fraudulent notices. As criminals often use such pop ups and redirects, some users have been "trained" to ignore warnings. In other cases, the cybercriminals spoof and forge email address and caller IDs. As a result it is increasingly becoming difficult to prove it they are legitimate. Even when the notification is recognized as legitimate, it often raises a flood of concerns with the customer including;

- How the botnet gained access to their device and whether anything they personally did, might have contributed to it gaining access.
- Which of their devices on their network or in their home was actually infected?
- Whether any confidential data might have been stolen or compromised.
- Will continued use of their computer/device put them in further peril?
- How can they remove the botnet malware from their device?

[14] A major challenges is a user (based on their IP address), may be detected to have a bot, but the impacted device can be any device within in the household including a mobile device which may have previously connected through their network. Such a scenario could be a guest or visitor connecting to the home network and no longer present when the user receives the notification and attempts to identify the infected device.

- Whether their privacy might have been or will be further compromised in sharing information between legitimate service providers who detected this problem.
- Whether this problem could interfere with their ability to access the internet.
- What the impact is to their data - photos and music files, etc… including the possible loss of data from both the botnet and the remediation being offered.
- Where users can go for more information, technical support and assistance.

When consumers receive a notification, they often experience a flurry of questions and concerns. The lack of answers and understandable information creates a situation when they desire immediate assistance. To determine how to best assist consumers following notification, many tests have been conducted. We are currently unaware of compilation of such attempts and will update this document as such information is made available.

Tips to Improve the Effectiveness of End-User Notifications

1. Use multiple communication channels to deliver and confirm notifications, including browser notice, email, SMS/Text, phone call, bill-insert, page re-directs within site, walled gardens, etc.
2. Use clear, language with layman terms, in local dialects and the primary language of users.
3. When possible, use consistent terminology and jargon among service providers involved in an incident and notification process.
4. Attempt to identify the specific device that is infected. This can be accomplished by providing operating system version information (e.g. Mac OS, Windows), browser information, attached devices, etc.
5. Provide the user the ability to verify the authenticity of the notification. For example, by including a shared secret known only to the provider and consumer such as the amount of the last bill.

Metrics for Notification Effectiveness

One of the presentations reported after the DNS Changer takedown, only half of the affected users were successfully mitigated. A search engine provider involved in the project, shared that after they began providing notification to affected users on their search results pages, approximately 10% of compromised devices were cleaned within a week. A social network site that sent notices to users, also saw 10% reduction in affected users over a three week period. Interestingly, another service provider noted that periodically changing the color of notifications successfully grabbed users' attention and resulted in an additional 10% cleanup.

A clear observation by the group was that there does not exist a comprehensive method to test the effectiveness of notification design and delivery, especially across different service providers. Designing and delivering notifications to consumers represent significant investments and service providers need to demonstrate both effectiveness of the process and the impact on their business to substantiate their efforts. In addition to reducing the number of affected users, business impacts such as increased customer retention and satisfaction ensure that providers can continue to invest in protecting and notifying users.

Connecting Notices with Remediation Tools

Notification alone is not sufficient to protect customers from the impacts of botnets and malware. To be fully protected users must receive and understand the notification, acquire and use remediation tools and then apply protective measures to their device to help prevent the incident from recurring.

Workshop participants expressed two current concerns about remediation. First, tools are not always available for the threats that consumers are facing and possibly being notified about. In one example, malware had infected a user's home networking device (router) but no tools were available to fix it. In cases such as this, the customer would continue to receive notifications from their service provider about an infection, but have no way to remediate the issue. This would frustrate that consumer, who would likely complain to the service provider, ultimately reducing the likelihood of the service provider continuing to invest in the notification program.

Another issue raised was users' ability to discover access and use remediation tools - both during and after discovery of a malware incident. Users are not experts when it comes to running anti-virus or virus removal software on their devices. Most require a high degree of assistance to guide them through the process – otherwise they give up and or ignore using the tools provided for their protection. A social networking company shared their experience, detailing how they enable users to run remediation tools within the web experience of their site. This leverages the trusted brand of the service by working with the users in a familiar interface. Furthermore, these "checkpoint" scans did not interfere with any existing antivirus solution on the device.

One case study presenter offered the following remarks about remediation efforts for the ZeroAccess Trojan:

> "We had to have a good robust detection technique for the threat as it evolved. We needed to build agile fast moving remediation tools to keep up with rapid threat changes. Communication was key to getting users cleaned. Not just sharing information, but also listening to customers. Usability studies were critical to finding what worked in guiding users from detection to remediation."

Several participants noted that in many cases antivirus and remediation technologies exist, but users may not have access to them. This gap may continue in the near future with the move to mobile devices and other non-traditional form factors. Botnet infection notification has the potential to significantly raise consumer awareness of their infected devices; however we must ensure that consumers have a clear path to successful resolution or we risk further confusing and frustrating them.

What has Proven to be Effective

There have been a large number of notable successes in this battle against botnets and the perpetrators behind them. First, the significant risks of botnets have been effectively conveyed to users at large - both professionals and consumers. Significant numbers in both groups are taking this problem seriously.

Many companies and stakeholders in the ecosystem are aware of the risks and are taking steps to combat the problem. Companies are experimenting with different methods of prevention,

detection, notification, remediation and recovery. And they are amassing a body of information about what is and isn't effective for their particular circumstances at this point in time. They are cautiously starting to share that body of information with their users and with other companies in ways that will raise awareness and result in positive actions, without unduly raising fears. In addition, there are increasing numbers of formal and informal cross-industry collaborative efforts to prevent and stop botnets.

Preliminary List of Best Practices

1. Subscribe to trusted data sources to obtain information on potentially infected users.
2. Instrument existing systems to observe potentially compromised users.
3. Perform usability testing procedures to determine the most effective methods of user notification.
4. Design user notifications that are easily recognized by users as legitimate and distinguishable from fraudulent notifications.
5. Ensure that notifications lead to successful remediation by considering the entire user experience.
6. Construct notifications in the tone, reading level and language appropriate to the target audience. Consider multi-lingual phone support, notifications, tutorials and visuals.
7. Maintain trusted relationships among providers and users - do not simply direct them to third parties with whom they may not have a relationship.

Note: These guidelines are intended to complement other security best practices recommended by OTA including but not limited to:

- *Use of Secure Socket Layers to encrypt HTTP connections and counter the collection of passwords and user IDs from cyber snooping and compromised wireless hotspots.*
- *Use of Email Authentication & DMARC to help counter spoofed and forged email messages and help validate email from legitimate senders.*
- *Extended Validation SSL Certificates (EVSSL), to enhance brand protection.*
- *Apply Anti-Malvertising Best Practices to block malicious code and drivebys.*

See other recommendations at https://otalliance.org/resources/index.html

Future Challenges

Documenting and reporting on current efforts is intended to demonstrate that many of the best minds are working to resolve problems caused by botnets and working towards preventing botnets all together. The information presented here is meant to honestly and realistically portray the current situation; and to acknowledge that much remains to be researched and discovered before we are anywhere near a world safe from botnets.

One goal of this workshop was to identify key challenges and potential solutions within the area of User Notifications, and to select a few key aspects to brainstorm further actions. The participants identified the following:

1. The lack of available quantitative metrics and use of such data to construct a business case for further actions. Lack of data prohibits the ability to measure risk and impact of botnets, to quantify effectiveness of various anti-botnet efforts, and to perform cost-benefit analysis.
2. There is a need to increase focus on prevention including a better understanding of root causes of botnet and malware infections.
3. Need to identify methods to reduce incentives for operators of botnets; to reduce their monetary incentives, access to accounts and infrastructure they need to establish their operations, etc.
4. Eliminate barriers to information sharing between those fighting against botnets. Share information on technique effectiveness, the impact of legal proceedings, and how to communicate with whom – for greatest effect.
5. The need to develop a “product plan” for botnet take-downs to ensure relevant parties are informed at the appropriate time and can take action to best protect their users.
6. Identify ways to make remediation of malware simpler and more effective for users.
7. Determine how to deal with changing tactics by criminals such as the move from botnets run out of consumer devices to commercial hosting facilities.

Clearly, the threat of botnets and related malware continue to impact users and infrastructures around the world, putting many devices at risk. The anti-botnet community, comprised of stakeholders from across the computing ecosystem, believes it has developed an effective multi-stakeholder strategy to limit the impact of botnets in the future. The outputs of this workshop illustrate there is much innovative thinking available to inform a strategy and battle botnets. There is much opportunity specifically around the core activity of proving notification to users. These notifications have been proven effective at reaching impacted consumers and connecting them with the resources they need to recover their devices and data following malware infection. The OTA intends for the practices demonstrated in this paper to be further developed and adopted throughout the global ecosystem. Furthermore, the future challenges identified during the workshop illuminate a path of ongoing work to ensure the safety and security of internet users around the world.

Resources

Online Trust Alliance https://otalliance.org/resources/botnets/index.html

FCC ABCs for ISPs
https://otalliance.org/resources/botnets/20120322%20WG7%20Final%20Report%20for%20CSRIC%20III.pdf

Industry Botnet Working Group http://industrybotnetgroup.org/information/

Kindsight: www.kindsight.net/securitylabs

Microsoft Corporation http://www.microsoft.com/security/resources/botnet-whatis.aspx

Symantec http://us.norton.com/botnet/promo

Acknowledgements

This paper reflects strategic input and guidance from a broad cross section of the ecosystem. Updates of this paper will be posted at https://otalliance.org. To submit suggestions and comments, please email staff@otalliance.org.

About The Online Trust Alliance (OTA)

OTA is an independent, non-profit with a mission to develop and advocate best practices and public policies which mitigate emerging privacy, identity and security threats to online services, organizations and consumers, thereby enhancing online trust and confidence. By facilitating an open dialog with industry, business and governmental agencies to work collaboratively, OTA is making progress to address various forms of online abuse, threats and practices that threaten to undermine online trust and increase the demand for regulation.

PO Box 803
Bellevue, WA 98009-0803
+1 425-455-7400
https://otalliance.org/