Botnet Remediation Overview & Practices

Released Oct 1, 2013

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.

TABLE OF CONTENTS

Introduction

This paper has been written for a broad audience of service providers, operators of popular web properties and other members of the Internet ecosystem that increasingly find themselves having to interact with users whose computing devices have been compromised by a botnet or malicious software.

Historically, typical industry responses to bot-infected end-user computers and devices have relied heavily on Internet Service Providers (ISPs), but recently remediation efforts have evolved to include other stakeholders and intermediaries. Today, the response to bot-infected end-user computers often includes direct interaction with members of broader Internet community, including:

- Security vendors (including anti-virus vendors)
- Operating system providers,
- Internet web site sites (including social, financial, gaming and other interactive sites)

Two issues motivate this broader level of engagement. First, stakeholders increasingly recognize the long-term impact of malware upon their customers and online services. Second, stakeholders now have better mechanisms to detect compromised devices, provide notification, and aid in the remediation process. Research and the general consensus of the working group recognizes that notifications from trusted third parties have the potential to enhance user awareness and motivate user action, reducing the burden that formerly fell almost exclusively on ISPs.

This paper focuses on traditional computing devices (PCs, Macs, etc.), leveraging and building on the OTA Botnet Notification Best Practices white paper published in December 2012.[1] Future documents and updates will focus on the mobile landscape, recognizing that tablets, smart phones and similar mobile devices are outpacing the growth of PCs and increasingly being targeted by cyber criminals.

For the purpose of this document, remediation is the action or set of actions required to remove malicious software from a compromised device and return it to a safe operating state. Remediation is a critical step to curb the impact of bots, though it is recognized that without tools and processes to harden the devices and prevent reinfection, bot infections will repeatedly reoccur.

Outside of the scope of this paper, but extremely important is recovery. The working group defines recovery as the steps and actions a user must take after the botnet and related malware have been removed. Recovery may include but is not limited to the process of recovering personal data, documents, account access and related information that have been compromised by the botnet. This may include router and home network reconfigurations to working with banks and commerce sites to recover lost funds and identity theft.

[1] https://otalliance.org/news/releases/botnetnotice.html

With this paper, we seek to arm stakeholders with remediation tools and highlight best practices in order to accelerate their deployment and usage. OTA shares this and other related best practices that can be leveraged and modified by other industry sectors. Finally, we hope to spur technology innovation and collaboration to enhance online trust and confidence, and help address unresolved challenges identified by the working group.

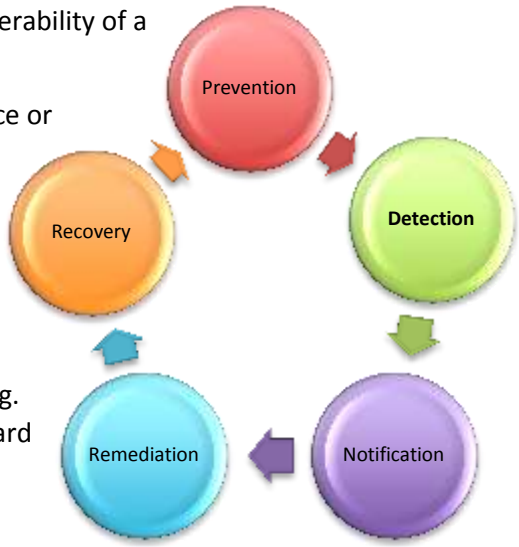
Background

Botnets and related malware is an ongoing problem impacting everyone who relies on the Internet. For users, botnets can compromise one's identity, lead to damaged credit scores or reputation, or even allow a cyber-criminal to clean out a person's bank account. For businesses and governments, botnets are used to commit cybercrime, complete fraudulent transactions, conduct espionage against corporations, slow down communications and disrupt business through Distributed Denial of Service (DDos) and other attacks. Considered collectively, botnets represent a significant threat to a nation's critical infrastructure and the overall vitality of the Internet and related services and commerce.

This paper builds on previous efforts by OTA and the industry in prevention of botnets (through education and awareness about safe computing practices), secure site and mobile application development, patch management and secure code development to detection and notification.

The anti-botnet lifecycle requires efforts across five major areas as listed below.

1. Prevention – Proactive activities that can reduce the vulnerability of a user's device.
2. Detection – Efforts aimed at identifying threats on a device or network.
3. Notification – Steps to inform a user or responsible entity of the issue.
4. Remediation – Actions to remove malicious software from a compromised device(s).
5. Recovery – Actions to resolve the impact of the attack (e.g. to a user's identity from theft, account takeover, credit card fraud or related damages caused by a botnet or other malicious code.)



A variety of remediation options exist today, including:

- Use of self-help malware removal tools
- Professional assistance via remote access technologies
- On-site / in home support (via a paid support or knowledgeable friend)
- Retail Support
- Reinstalling of operation system and applications

As computer prices have dropped dramatically, support professionals and retailers are increasingly recommending the most definitive answer: simply replace an infected system, particularly if the system is near end-of-life.

The costs, resources and obstacles to these strategies vary widely. This paper serves to outline such practices, while also sharing considerations, obstacles, tradeoffs and lessons learned.

Responding to the increased threats of botnets and their impact on critical infrastructure and user's devices, the OTA hosted a two-day workshop in Washington DC in June 2013 to help identify best practices focused on device remediation. Participants from the ISP, carrier, finance and security communities were represented, along with representatives from several trade and industry working groups.

There was a broad consensus that to adequately contain and counter the botnet threat, a multi-stakeholder effort is required. This requires a concerted endeavor including the public and private sector, intermediaries, and infrastructure providers as well as software developers, ISPs and the security community. Equally as important: users themselves need to take steps to protect their device and stay safe online. For example, users need to understand the importance of keeping their computer patched and up-to-date.[2] Similarly, users need to learn that they must not click on links received in unsolicited email, nor reveal their username and password in response to a phishing attack.

While mobile remediation is outside the scope of this document, it is important to understand that the mobile platform and other devices are becoming popular vectors.[3]

As the" Internet of Things" becomes a reality, cybercriminals increasingly target non-traditional networked devices. [4] [5]

The growing number of mobile users and malicious apps combined make mobile devices a fertile ground for abuse. The increased prevalence of look-a-like applications and "brand jacking" in mobile application stores highlights this problem. These malicious apps compromise user's devices and personal information as

WHY CARE

- Over 10 billion devices are connected to the internet, (Cisco 2013 report)
- IDG forecasts by 2017, 87% of connected devices are projected to be mobile "smart connected devices"
- Upwards of 100,000 devices infected per week.*

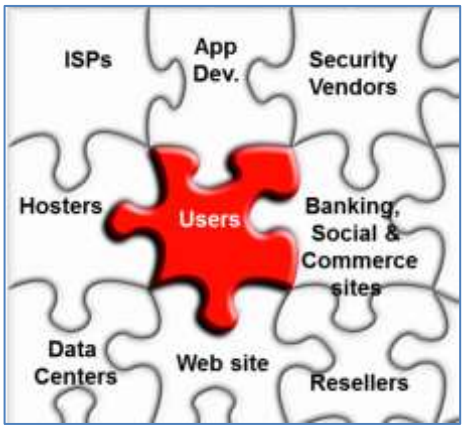
[2] Users should consider automatic application patch management services such as Secunia PSI www.secunia.com

[3] http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/?ss=future-tech

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

[5] http://www.ftc.gov/opa/2013/04/internetthings.shtm

well as the brands they hijack.[6] Note while any mobile devices have a one-touch restore capability and automatic cloud storage back up they are not without their respective tradeoffs and limitations.[7] The working group plans to address Mobile remediation practices and processes in subsequent best practices papers as wells as best practices for the data center and hosting ecosystem.



In parallel to this effort, the Industry Botnet Group (IBG)[8], the Federal Communication Commission, Communications Security, Reliability and Interoperability Council (CSRIC), and other groups including the Cloud Security Alliance (CSA) have initiated efforts to address the hosting and data center ecosystem.[9] In addition the Center for Strategic and International Studies (CSIS) has developed practical solutions and recommended controls to aid in the prevention of such attacks.[10]

Connecting User Notification with Remediation Tools

An end-user's first hint that one of their devices has been affected by malware may come from a notification or alert from their own security software, or from their ISP or another online service.

While the OTA notification botnet white paper released in late 2012 discuses notification in detail, it is importance to highlight the interdependency of notification and remediation processes.[11] Notifying a user of a malware problem alone is not sufficient to protect consumers from the impacts of botnets and malware, but it is a critical step.

Keys to Successful Notification

- Discoverable
- Timely
- Comprehendible
- Prescriptive
- Actionable

[6] OTA has been calling for all app platforms and mobile store fronts to adopt voluntary efforts to complete security and privacy screening and brand verification all apps.

Source: eSecurity Planet http://www.esecurityplanet.com/malware/fortinet-zeroaccess-botnet-was-leading-threat-in-q1-2013.html

[7] http://blogs.computerworld.com/android/22806/google-knows-nearly-every-wi-fi-password-world

[8] http://industrybotnetgroup.org/

[9] http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv

[10] http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

[11] https://otalliance.org/docs/OTA%20Botnet%20Notification%20Whitepaper2012.pdf

To maximize protection, users must:

- Receive, read and comprehend the notification provided. It is important that the notice includes adequate and easily understood details about the malware that's in play.
- Take action to address the issue(s) outlined in the notification.
- Apply protective measures to their device to help prevent the incident from recurring.

There are several practical concerns that can impede the remediation process. First, tools may not yet be available to tackle some of the threats that consumers face or existing tools may not remove the threat completely. This may be as a result of a zero-day threat to the complexity of some malware and the damage they may leave behind once removed.

In one example shared in our earlier workshop, an ISP noted a botnet that appeared to be coming from a residential user's IP, but that malware wasn't on one of the end user's computers. The malware had actually compromised the user's home networking device (router). Externally, the ISP was not able to identify the infected device accurately. In cases such as this, the customer continued to receive notifications from their service provider about an "infection," but they were never able to identify the device or remediate the issue. This frustrated the consumer, who complained to the service provider, taking significant resources to resolve. Subsequent efforts need to focus on addressing the remediation of non-traditional connected devices, including customer premises equipment (such as home broadband routers/wireless access points) and gaming/entertainment devices not to mention mobile devices connected over WiFi in the home).

Another issue raised was users' ability to obtain appropriate remediation tools - both during and after discovery of a malware incident. Users are not experts when it comes to running anti-virus or malware removal software on their devices. Most are unfamiliar with the terminology and require a high degree of assistance to guide them through the process – otherwise they give up and / or ignore the tools provided. Fake antivirus products represent another potential landmine for unwary consumers.

Regardless of the method or source of the notification, users need to know whether the notification is genuine. Care must also be taken when crafting the content of the message, as the user needs to understand the issue, know what malware is infecting the device, and understand the necessary steps to remove the malware. [12]

A social networking company shared their experience with enabling users to run remediation tools within their web site. This leveraged the trusted brand of the service by working with the infected users from within a familiar interface. Furthermore, these one-time "checkpoint" scans did not interfere with any existing antivirus solution that might already have been installed on the device. However, for this to work, the tools had to be able to completely remove the specific

[12] See OTA Botnet Notification Best Practices White Paper
https://otalliance.org/docs/OTA%20Botnet%20Notification%20Whitepaper2012.pdf

malware the user was infected with. Sometimes these one-shot tools were able to help, and other times they were not.

Key Issues

Addressing the botnet problem is a complex and multifaceted issue. Within the specific area of remediation, workshop participants identified the following key issues:

1. Discoverability of Remediation Resources - Where can users find trustworthy remediation resources?
2. Discovery & Notification - Are the resources intuitive and comprehensible for the novice user or are they designed to be used by the more advanced user?
3. Paths to Remediation Methods, Alternatives & Challenges - Can we identify the critical success factors associated with successful remediation?
4. Proactive Preventative Measures - How can a user avoid infection in the first place, and what steps should they take to be prepared when their device is compromised?
5. Collaboration - How can stakeholders share data with each other regarding common customers to help make remediation more timely and successful?
6. Obstacles - What obstacles do users face when attempting to eliminate malware?

Discoverability of Remediation Resources

Today there is no single source for users to discover appropriate remediation resources. Some users may have anti-malware products pre-installed on their device, while others must procure a security solution after they experience a problem. Some users may go directly to a trusted vendor or retailer for the solutions while others may be directed to a particular solution by the organization or service provider who notifies them of their incident. With the onslaught of malicious sites and search fraud, consumers are often left alone to determine if a tool is trustworthy. Furthermore, when a company offers multiple remediation resources, it is often unclear which is the best or most appropriate tool or resource in each scenario.

An anti-malware tool that works well to tackle one issue may fail when challenged with a different one, and unfortunately there is no single "best" antivirus product that works perfectly all the time on every threat that may be present on any system. Additionally, once a device is compromised, there may be other malware on the device and a single scan or tool may not be sufficient to remediate the threats. That is why it is crucial that the specific malware be identified so the appropriate tool can be deployed to remove the infection. However, this involves a level of complexity that may be too much for the average user.

Discovery & Notification

As outlined in the notification best practice white paper published by OTA, for any infected device, a malware infection may be discovered by the user directly, by their security solution, by their ISP or network provider, or even by a 3rd party such as a bank or ecommerce site. The means by which an end user might be notified of the infection can range from self-identification of symptoms (such as a slow or crashing device), receipt of an alert from the security software installed on the device, an email or text message from a service provider, or perhaps being placed in a restricted environment such as a "walled garden" that limits the resources that the users can access to until the infection is removed or neutralized.[13]

Paths to Remediation Methods, Alternatives & Challenges

After performing scan and removal steps, a device may appear clean. However, there are limited ways to ensure that the malware has been completely removed. Only some of the malware that was present may have been removed, or the malware that was noticed may still be present but hiding itself from the user and her malware removal tools. Additionally while the bot may be removed, the registry or other system components may be corrupted, creating additional vulnerabilities, slowing the machine, or causing subsequent crashes.[14] This is one of the key challenges in devising an effective remediation strategy and a major obstacle to remote support. Unfortunately, sometimes one may not be able to know unless they completely reformat and reinstalls the system, ("nuke and pave") which poses one of the largest remediation challenges.

Figure 1 below illustrates the multiple paths to successful remediation and the wide range of intermediaries that may detect and notify a user. It is acknowledged that this diagram is not all-inclusive, and there may be other edge cases and other actions that may also apply.

[13] http://en.wikipedia.org/wiki/Walled_garden_(technology)

[14] http://support.microsoft.com/kb/822705

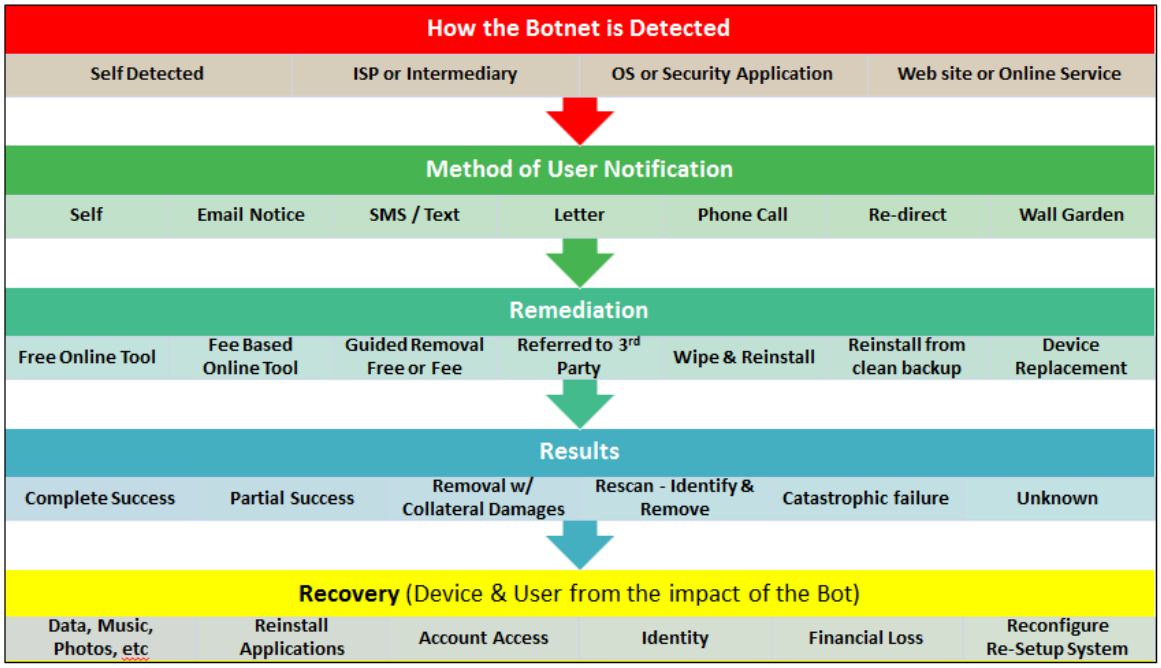


Figure 1- Path from Detection to Remediation

Proactive Preventative Measures

Workshop participants agree that, in light of the copious challenges outlined, preventative measures that can keep malware infections from happening in the first place will be most effective. Preventative measures can be considered in two major categories; education and technology.

Education initiatives and awareness campaigns are oft cited as a solution, but when done alone and coming from non-authoritative sources are not sufficient for solving the malware problem. A user can be very security aware, and try to do all the appropriate things that they should be doing, and still get infected through no fault of their own. (For example, they might end up infected via a drive by download from a legitimate web site as a result of cross-site scripting exploit or malvertising, attacks that occur with no interaction on the part of the user.

Preventative & Preparedness

- Non-Use of privileged account for routine work
- Automatic updates of OS & applications enabled
- Availability of recovery media (OS & applications)
- Backup of critical files
- Networking & Internet configuration documentation
- Documenting and securing passwords & logon credentials

It is critical to increase efforts to inform users about the risks they face and how to appropriately manage their exposure to those risks, just as is done in the physical world every day. For example, it is potentially dangerous to drive a car, but most of us do so, although we probably take steps such as buying insurance, making sure our tires are safe and using seat belts to manage the risks and dangers we face.

One of the challenges to remediation and ultimately recovery is the lack of preparedness of the user including the absence of original media for their operating system and applications, and failure to back up of important user files and documentation. Not unlike being prepared for a storm or major incident, users need to accept that over time one or more of their devices will very likely be compromised. Without taking steps in advance, the ability to effectively remediate the device may be significantly hampered.

Leading browsers, functioning as the tip of the spear between users and online threats, have expanded their security functions. This includes blocking and presenting warnings when phishing and malicious sites are encountered. When used in conjunction with an up-to-date security solution and automatic operating system and application updates, web security features help to protect the innocent user.

Collaboration

Collaboration among stakeholders to aid end user remediation of infected systems may take many forms. In figure 2, we have listed six possible scenarios, that illustrate a variety of stakeholders and the roles they may have in detection, notification & remediation. This model also illustrates the importance of collaboration and data sharing including feedback mechanisms to help to measure effectiveness. For the purposes of this model we have defined the stakeholders as follows:

- Security Vendors - May include AV, OS Vendor or other security related service provider.
- "Third Party" - May include banking, commerce, communication and / or social / gaming sites that may detect abnormal behavior, traffic and or account activity. Third parties may also include onsite or in-store support by a third party dispatched or referred to by another stakeholder.
- ISPs - May also include web and email hosters and data centers.

SCENARIO	DETECT	NOTIFY	REMEDIATE
1	Security Vendor	Security Vendor	Security Vendor
2	ISP	ISP	ISP
3	3rd Party	3rd Party	3rd Party
4	Security Vendor	3rd Party	ISP
5	3rd Party	ISP	Security Vendor
6	ISP	Security Vendor	3rd Party

Figure 2- Notional Model for Ecosystem Collaboration

In the scenarios 1-3, a single stakeholder may solely detect, notify and remediates the malware. In scenarios 4-6, the roles may changes and shift from one stakeholder to another. For example in scenario 6, the ISP may detect the infected device, the security solution may notify the impacted user and a third party such as a support professional to remediate and remove the bot.

Obstacles to Remediation

Remediation is perhaps the most complicated and costly function for any party to undertake. While awareness efforts and tips for prevention and notification are relatively simple and embraced by many trade organization and public affairs groups, those awareness efforts have not prevented infections from occurring.

Remediation has several obstacles which need to be considered and overcome. Depending on the remediator's infrastructure and line of businesses, their respective may differ greatly. The OTA working group, many of whom are active contributors to the Federal Communications Commission, Communications Security, Reliability and Interoperability Council (CSRIC), have leveraged and expanded upon the taxonomy as identified in drafting the obstacles to implementing the Anti-Botnet Code of Conduct for ISPs. [15] Please note this is a non-exhaustive list of potential obstacles.

Other Considerations

It is imperative that industry, users, business and stakeholders recognize the importance of being prepared for device compromise and a resulting data loss. Ranging from the out-of-box user experience when purchasing a new device, to the installation of new features and application, prevention and preparedness must be emphasized.

When an infection is discovered, users should be advised to curtail usage of the device and disconnect if from the Internet until the threat can be identified and remediated. In multiple device households or in the business environment, users should cease usage and utilize a secondary device to investigate remediation solutions and alternatives. Depending on the circumstance a user may need to isolate the infected machine to preserve evidence or isolate other machines on the network to limit spread of the infection.

Avoid Rogue (Fake) Anti-Virus (AV)

Rogue or fake AV scams further complicate the path to remediation and risk confusion to end users who are likely already in a dangerous situation. Scammers prey on users who are searching for free solutions. Unfortunately these fake anti-virus solutions generally attempt to install additional malware and/or deceptively charge consumers for unneeded "services."

Providers of remediation tools and services can enlist brand protection firms to scan for abuses of trademarks that can confuse users.[16] End users should use a safe search engine when looking for remediation tools to lessen the risk of ending up with a fake or malicious security product. Finally, all are advised to avoid sites or offers that create a false sense of urgency or make extreme statements like an FBI warning. As a best practice, rather than click on a link, users should go directly to a recognizable name brand security software vendors sites and consider their solutions (see Appendix A for a partial listing).

---

[15] http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv

[16] Such firms include but are not limited to BrandProtect http://www.brandprotect.com/, MarkMonitor https://www.markmonitor.com/ and IID (Internet Identity) http://www.internetidentity.com/.

Recovery

Recovering from a malware infection is not usually complete after remediation. Multiple additional steps are often needed to assess the extent of the damage and to restore data and integrity of accounts. When restoring data from a backup, users are advised to scan the backup files to ensure they do not reintroduce the malware. Passwords for all online sites should be changed to something that is unique for each account as malware often includes keystroke loggers that capture passwords.

Affected individuals should also check their bank account and credit card statements to look for any fraudulent charges. Ordering your free annual credit report can help you spot and new accounts that may have been opened. Note as with the rogue AV solutions offered, there are deceptive sites offering free credit reports. [17]

Multiple Device Households & Businesses

The remediation processes discussed in this document generally apply to consumers and businesses alike. In both environments, the presence of multiple machines increases the potential attack surface. If one machine is infected, there is a good chance other machines at the same location will also be infected and need to be addressed in the remediation process. Any preventive steps should also be applied to every applicable machine and device in the workgroup or home network. In addition, all external storage devices including USB and flash drives should be scanned and cleaned prior to usage.

Business Considerations

In the process of remediating a malware infection, businesses must consider any legal and contractual requirements to notify customers, partners and resellers. If a compromised device contains business or customer personally indefinable information (PII), the business may have to consider notification to regulatory authorities and may have an implicit (or statutory) obligation to report infection to impacted customers. An often cited example is when data from a large company is lost because of an incident at a small company they work with, such as their accounting firm. As there are currently 46 separate state breach notification laws as well as international notification requirements, businesses are advised to seek legal and compliance assistance. For detailed information, see the OTA Data Protection and Breach Notification Resource Guide athttps://otalliance.org/breach.html.

[17] http://www.consumer.ftc.gov/articles/0155-free-credit-reports for trustworthy credit report request channels.

Current Remediation Practices

Computer users faced with an infected device may have several options available to remediate the device. Unfortunately, not all the options are equally appropriate or effective for the given situation. In the workshop, participants enumerated the primary options in the table below and considered the efficiencies, cost, and difficulty of each.

Method	Effectiveness	Cost ($)	Time	Collateral Damage	Difficulty Level	Considerations
Tool Based (OS, ISP, Application and/or AV vendor)	Moderate	Free or low cost	Varies	Low	Moderate	• Tool may be provided and or integrated with the operating system, paid antivirus solution, or provided by service provider. • Persistent infections might require multiple tools or scans to complete removal. • It is recommended to start with a specific tool (known to fix the current issue) that is newly downloaded to the computer and then follow-up with a full scan and further preventative actions. • Scans can take several hours to overnight depending on size of hard drive, the scanning technology used, and the thoroughness of the scan. • Users may perceive security-related tools difficult to use. • Some malware may actively interfere with the use of tools.
Manual Removal	Depends on skill of technician and tenacity of malware	Varies	Can be high	Varies	High (experts only)	• Requires skilled technician or advanced user • Removal efforts might damage device, render it inoperable • Removal may be incomplete • May not be practical for the majority of users and support technicians

Method	Effectiveness	Cost ($)	Time	Collateral Damage	Difficulty Level	Considerations
Professional Help **Online vs. Onsite**	High	Moderate to High	Moderate	Minimal	N/A	• Users may be upset by perceived "upsell" if referred to paid service from another provider. (More of a problem if you refer your user to your OWN paid service. • Lack of knowledge of trusted servicers list. Fake AV sites often try to induce payment and others push unnecessary add-ons. • Servicer provider can help advise on best remediation solutions, including setting up and configuring a new device if this turns out to be the user's preferred option. • Bringing the device to the retail location will typically result in a quicker turn around and broader set of diagnostic tools.
Reinstall OS	Moderate	Low to Moderate	High	May need to migrate files	Moderate to High	• A new device might be a better option for older hardware. • Requires that "restore media" be available. • Sophisticated malware might remain in the master boot record even after a system reinstall and require more advanced steps. • Need to have data backup available. Reinstalling applications raises collateral damage. • Completing all related updates and obtaining drivers can be very time consuming and frustrating. • Upgrading an OS is not recommended without a complete system wipe as it may not remove the threats fully or repair a corrupted registry and related system damage. Additionally legacy hardware may not support newer operating systems memory and process requirements.

Method	Effectiveness	Cost ($)	Time	Collateral Damage	Difficulty Level	Considerations
Acquire a New Machine / Device	High	Medium	Moderate (migrate files)	Legacy apps may not be able compatible or original media may not be available.	Low	While making this recommendation may be the most economical in time and productivity, it may be difficult for a user to embrace. Considerations – • Are the legacy applications supported by the new device OS? • Are the legacy applications vulnerable? • What is the confidence this environment can adequately be hardened to help prevent a reoccurrence? • Based on replacement costs and the rapid pace of technology innovation, if a device is three or four years old or older a new device may be more cost effective. • Disposal of a computer along with removal and destroying all personal data on the machine. (PC buy back?

Conclusion

Effectively addressing the threat of bots and related malware requires a coordinated effort including prevention, detection, notification, remediation and recovery. While cybercriminal efforts evolve quickly, so have industry remediation solutions ranging from new technical solutions to "self-healing" software. One of the key challenges is that cybercriminals continue to "out innovate" device defenders. This underscores the need for collaboration and data sharing, and work focused on evaluating the problem holistically. The more that can be done to prevent the distribution of bots and the more that can be done to harden devices, applications and operating system, the safer the Internet will be and the more the entire Internet ecosystem will prosper.

Ideally, web sites will embrace notification as an opportunity to strengthen the consumer relationship and their brand value proposition, while reducing fraud related costs. Additionally ISPs, commerce and banking sites can realize several benefits including increased revenue and brand loyalty, market differentiation, reduced shopping cart abandonment and decreased incidence of account takeovers.

As outlined, self-help tools and resources are not perfect. This paper's authors believe there is an opportunity to build upon the services offered today by service providers, consumer electronics, and computer retailers and office supply stores. Examples cited include annual subscription support programs, free quick-look quarterly tune ups and related services. Additionally, other stakeholders may negotiate preferred rates for their customers and realize revenue streams from referral fees, affiliate programs and fee-based service offerings involving such service providers.

In addition, data sharing on effectiveness and metrics have been continually raised as an unmet need, including active support and possible funding from the public sector. OTA encourages a renewed effort to share aggregated data to better understand progress and identify areas requiring added research, potential governmental assistance and further innovative approaches.

Last but not least, to effectively aid in the remediation of devices, it is important to recognize that the end user has a shared responsibility to both help prevent infections, and to be prepared for the reality that one of their devices will likely become compromised. Users should have recovery media available, trustworthy backups of important data and personal files and photos, as well as any required documentation at their disposal.

See Appendix A for a listing of known Resource and Tools https://otalliance.org/botnets.html.
This listing will be updated based on submissions and vetting by the working committee. To submit tools for review, email admin@otalliance.org.

Acknowledgements

This document reflects strategic input and guidance from a broad cross section members of the ecosystem including representatives of the financial services industry, leading ISPs, security community and commerce sites. Special thanks to members of the OTA multi-stakeholder anti-botnet committee including: Pat Barnes - Nominum Inc., Don Blumenthal – PIR, Matt Carothers - Cox Communications, Paul Ferguson - Internet Identity (IID), Adam Moore - Verisign, Joe St Sauver - University of Oregon, Kevin Sullivan - Microsoft, Ameya Talwalkar - Symantec, Brendan Ziolo - Alcatel-Lucent.

Updates of this paper will be posted at https://otalliance.org/botnets.html. To submit suggestions and comments, please email admin@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. https://otalliance.org/