TESTIMONY OF JASON LIVINGOOD
VICE PRESIDENT, INTERNET SYSTEMS ENGINEERING
COMCAST CORPORATION

on

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

before the

Committee on Energy and Commerce
Subcommittee on Communications and Technology

UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

MARCH 7, 2012

TESTIMONY OF JASON LIVINGOOD
VICE PRESIDENT, INTERNET SYSTEMS ENGINEERING
COMCAST CORPORATION

Good morning, Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee. My name is Jason Livingood and I am the Vice President of Internet Systems Engineering at Comcast Corporation. I would like to thank you for inviting me to testify here today. Your staff asked that we share our experience with our customer-facing Internet security efforts, particularly our Constant Guard cybersecurity measures, including botnet detection, notification, and remediation mechanisms, as well as our recent deployment of Domain Name System Security Extensions (DNSSEC).

At Comcast, we take cybersecurity issues very seriously, and know that our Xfinity Internet customers are concerned about security. We strive to provide our customers with the best, fastest, and most secure Internet service we can, and our engineering team devotes significant time, energy, and investment to update and refine constantly our cybersecurity efforts.

I think we can all agree that the benefits of an interconnected world far outweigh the risks and that it is probably unrealistic to expect complete and total security in any network, including the super-fast, interconnected networks operating today. Network operators and other entities in the Internet ecosystem, however, have the important job of managing these ever-changing risks. Our experience has taught us *that there is no "one size fits all" model for addressing cybersecurity risks*. The flexibility afforded to us to design and develop the best possible security solutions that are optimally adapted to our particular network architecture and customer environment is – and must remain – a core element of any successful cybersecurity policy framework. Attempting to impose uniform cybersecurity solutions could actually be counterproductive, by enabling an attacker that cracks a single solution to compromise multiple systems, and by slowing down or constraining our ability to rapidly develop innovative cybersecurity solutions.

Comcast is the nation's largest Internet Service Provider (ISP). With over 18 million residential and business broadband customers on one of the world's largest converged Internet Protocol-based voice, video, and data network, ensuring the safety and security of the network over which they receive our services is one of our top priorities. Deterring, detecting, and responding to cybersecurity threats is therefore a fundamental requirement for our continued business success.

Cybersecurity threats such as bot networks ("botnets") are particularly insidious because they turn ordinary users into unwitting participants in global criminal enterprises. Bots are a form of malicious software that infect a computer and allow it to be remotely controlled for nefarious and criminal purposes by a malevolent party. Some security companies estimate that as many as ten to fifteen percent of American households are likely infected. A bot can cause significant harm to the individual user, an entire network, and beyond. This threat is growing and is a major source of identity and credit card theft. Bots are also used to conduct massive Distributed Denial of Service attacks, steal user names and passwords, send spam, and facilitate other malicious and criminal activity.

Because botnets are typically surreptitiously installed on common consumer devices like personal computers, a consumer-focused approach to cybersecurity is essential to protect individual consumers, the broader infrastructure of our network, other networks, and the Internet in general. This threat becomes even more challenging when we consider the growth and proliferation of a variety of new mobile, smart phone, tablet, and other personal devices that have Internet access, which could also be vulnerable to infection. Internet users are increasingly aware of and concerned by the numerous and constantly evolving threats to their cybersecurity. As public awareness of these issues grows, so, too, does consumer demand for comprehensive security offerings that provide peace of mind as well as a more secure Internet experience.

Comcast understands that consumer-based security tools must work in conjunction with network-based measures in order to secure end users from cyber threats. We have been at the forefront of providing a consumer-oriented security product suite aimed at preventing – and, where necessary, remediating – disruptions and damage caused by malware, viruses, bots, and other cyber threats that affect the safety and security of both our network and the customer devices connected to our network. We have invested substantial resources to provide consumer education, established a dedicated customer security assistance team, and deployed state-of-the-art technologies and applications in our networks to combat bots and other Internet threats.

With that introduction, let me first describe Comcast's general approach to cybersecurity, and then describe our efforts to combat botnets and our DNSSEC deployment.

Comcast's Approach to Cybersecurity

"Security" encompasses a broad spectrum of techniques, tools, protocols, and practices. There is no one silver bullet or quick fix, especially because the risks and threats change so very frequently and dramatically as new technology is developed and as bad actors in cyberspace continue to innovate. They constantly adapt to the latest counter-measures and employ new techniques and tools. As a result, our security protections will never be complete; we must continuously learn, adapt, and work to improve and develop new capabilities to meet the ever-changing threats. Indeed, there is no realistic possibility that any network will ever be "completely" secure. But consumers' increasing desire for robust security protections and the need to protect our network provide Comcast with strong incentives to continuously invest in new and advanced security tools and offerings.

The threats that ISPs like Comcast observe appear to be primarily and overwhelmingly driven by economic motivations. There is a *sizable* underground economy that drives and profits from cybercrime, and this is the main threat facing individual Internet users today. Unfortunately, with respect to some threats, such as botnets, the pace of change and other complexities can render many of the available solutions from Internet security software developers outdated or inadequate for addressing the latest and most recent form of an infection. For example, software does not readily exist for consumer use which can reliably, 100 percent of the time, remove new forms of malware as soon as they are released, and do so quickly and easily. In such instances, the security risks and vulnerabilities faced by ISPs are not a function of insufficient resources or investment, but rather a reflection of the pace of adaptation and innovation demonstrated by cyber criminals and of the relative immaturity of malware remediation tools.

The available data on malware infections highlight the breadth and scope of the problem. For example:

- According to Symantec's Norton Cybercrime Report 2011, 54 percent of online adults across the globe have experienced viruses or malware on their computers. At least 10 percent of adults are estimated to have been victims of phishing scams.[1/]
- Microsoft's 2011 Security Intelligence Report estimated that approximately 10 million personal computers in the U.S. are infected with some type of malware every quarter.[2/]

[1/] Available at http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

- Over one million web site URLs are estimated to host malware, and the number of impressions of advertising containing malware is estimated at 3 million per day.[3/]
- One security solutions provider has estimated that "the probability that an average Internet user will hit an infected page after three months of Web browsing is 95 percent."[4/]
- It is also estimated that between 10 and 15 percent of American households have a device which has been infected with a bot.

Comcast's Consumer-Facing Cybersecurity Offerings

The prevalence of botnet and malware problems reflects the fact that it is relatively easy for a device to become infected. There is a misconception among the public at large that online users cannot become infected unless they download a program or application presented to them – but that is simply not the case. A user's personal computer can become infected through such common acts as opening an email that may contain a virus, clicking on a web site that shows up in a search result but serves as a host for a virus, or even by clicking on an ad or link that launches a hidden virus while navigating a legitimate web site. It is possible for the end user's device to become infected via a so-called "drive-by infection," where someone gets infected just by visiting a web site. For example, a site may itself be secure but the advertising network it uses may show an advertisement that has an embedded malware code, and the advertisement need only be displayed rather than clicked for an infection to occur.

[2/] Microsoft Security Intelligence Report, Vol. 11, June 2011, available at http://www.microsoft.com/security/sir/default.aspx

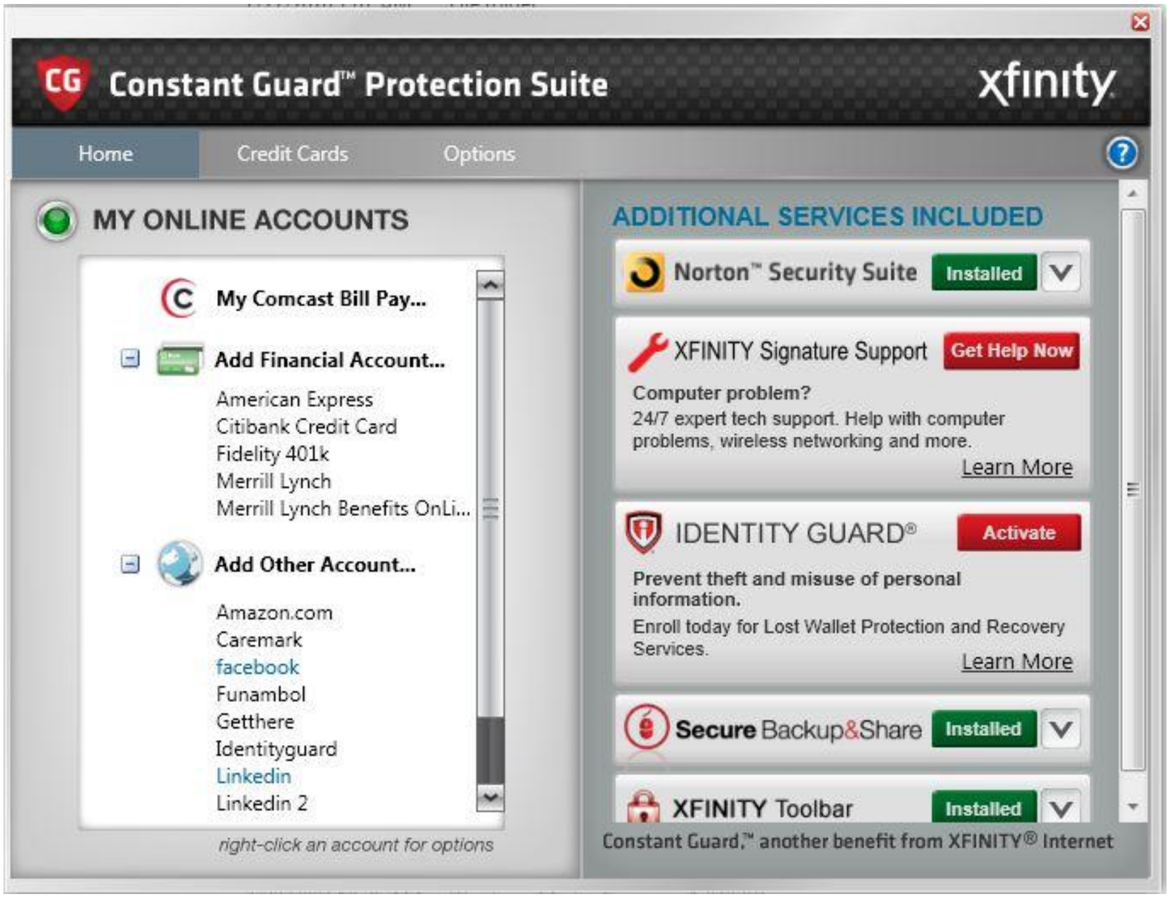
[3/] "Report: malware-laden sites double from a year ago," http://news.cnet.com/8301-27080_3-20040367-245.html?tag=mantle_skin;content, March 8, 2011.

[4/] *Id.*

At Comcast, we understand that securing cyberspace is a complex task that requires multiple approaches. Education, prevention, detection, remediation, and recovery are the core objectives of our anti-malware efforts, which include our comprehensive security suite, Constant Guard.

Constant Guard offers a multilayered, holistic approach to Internet security that provides protection, detection, notification, and remediation for our customers. Constant Guard combines extensive technological resources, including software such as the Norton Security Suite, anti-phishing and anti-spyware technology, secure data backup and sharing, identity protection, ant-botnet tools, DNS security, and privacy protection tools, with an extensive educational program, customer support, and strategic partnerships with related industry experts. It also provides brand-new protections designed to address the growing bot problem by integrating anti-keystroke logging technology with a secure login.

Unlike traditional anti-virus approaches that focus solely on protecting the computer or device, the Constant Guard Protection Suite (see screen shot below), one of the Constant Guard system's components, protects the user's personal information and privacy by concealing typed characters, safeguarding credit card information, protecting and remembering passwords, and providing one-click secure login to financial, commercial, and any other online accounts. The range of features and software offered in the Constant Guard system is offered to all of Comcast's Xfinity Internet customers at no additional cost.



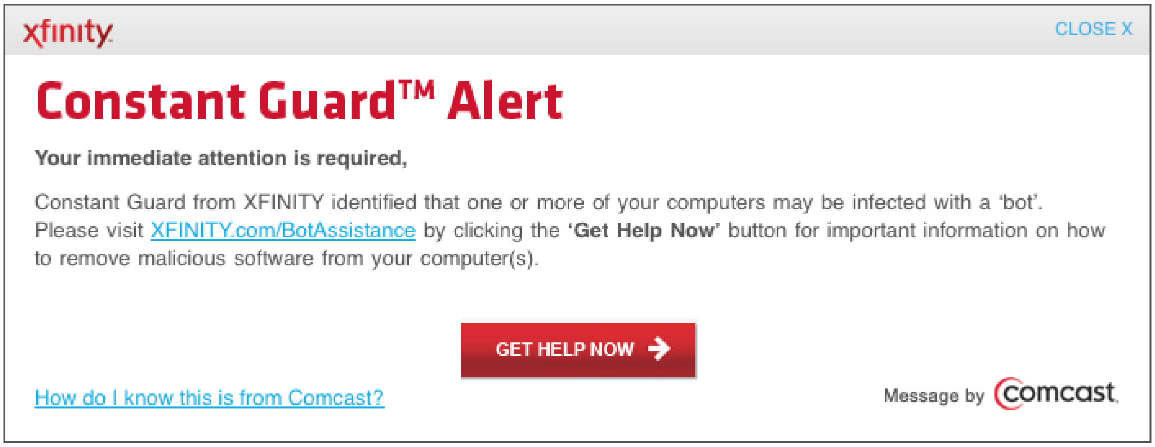
Computer problem?

24/7 expert tech support. Help with computer problems, wireless networking and more.

Prevent theft and misuse of personal information.

Enroll today for Lost Wallet Protection and Recovery Services.

Irrespective of whether a subscriber installs any software from Comcast, we also strive to identify computers infected with malware that are operating in bot networks. Once detection has occurred, Comcast employs a graduated notification process for alerting subscribers with devices that may be infected by a bot, alerting users first via email and then, if the problem persists, through browser notification, such as the example provided below:

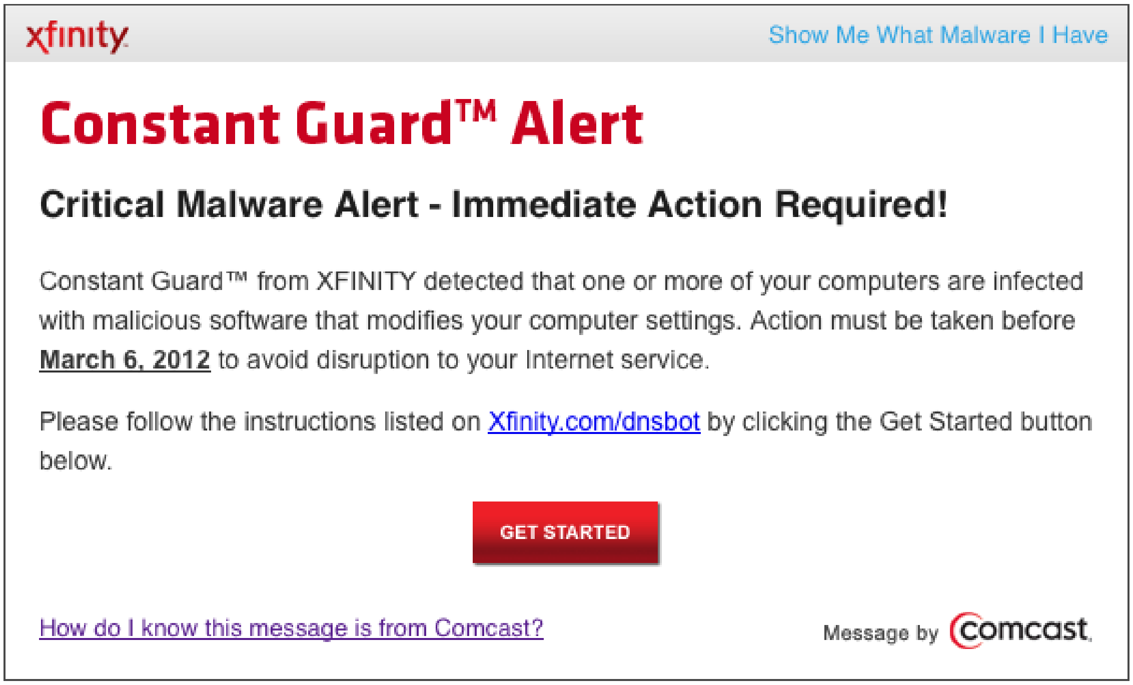


Constant Guard™ Alert

Your immediate attention is required,

Constant Guard from XFINITY identified that one or more of your computers may be infected with a 'bot'. Please visit XFINITY.com/BotAssistance by clicking the '**Get Help Now**' button for important information on how to remove malicious software from your computer(s).

These alerts have also been customized to specific types of malware, such as the DNS Changer malware that was the focus of the Federal Bureau of Investigations' recent Operation Ghost Click.



Constant Guard™ Alert

Critical Malware Alert - Immediate Action Required!

Constant Guard™ from XFINITY detected that one or more of your computers are infected with malicious software that modifies your computer settings. Action must be taken before **March 6, 2012** to avoid disruption to your Internet service.

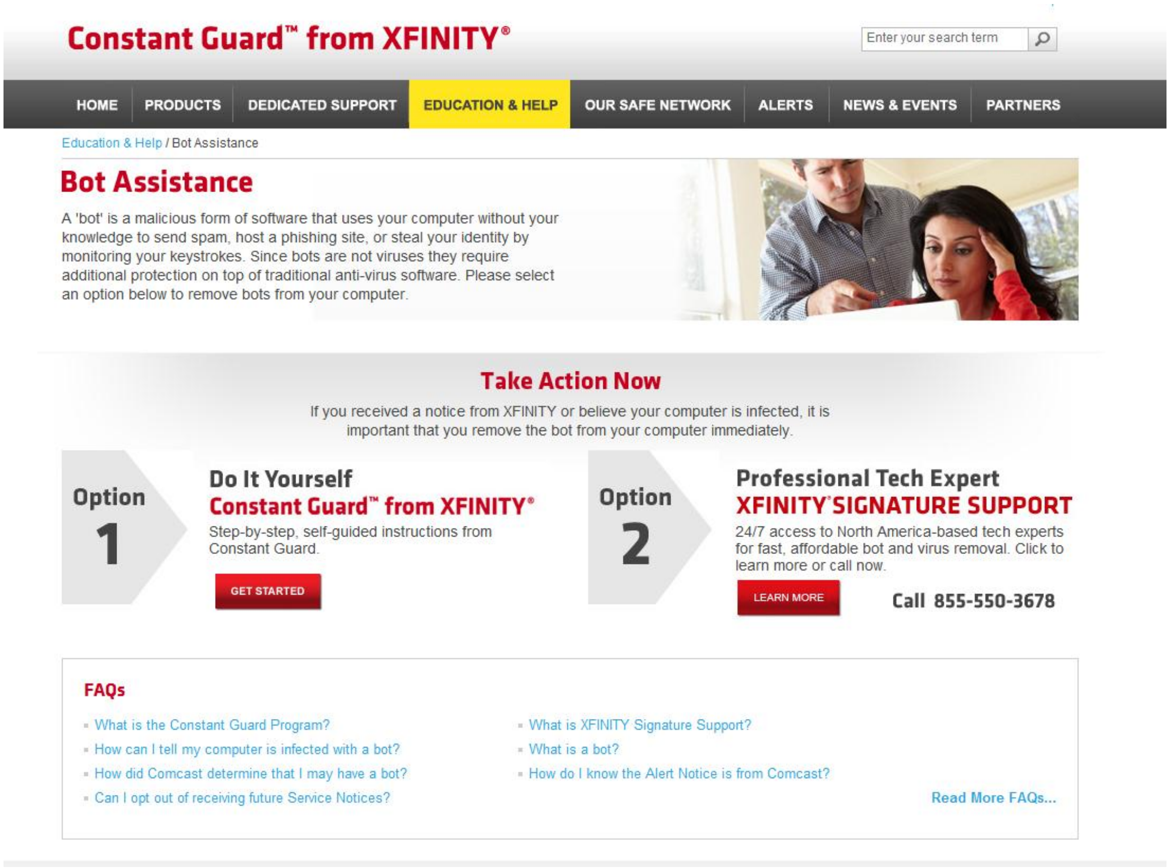
Please follow the instructions listed on Xfinity.com/dnsbot by clicking the Get Started button below.

Infected users are directed to the Constant Guard Center web site[5] where they can find the resources needed to safely remove the malicious bot. Once there, subscribers can avail

[5] http://xfinity.comcast.net/constantguard/botassistance/

themselves of either of two types of solutions: (1) a do-it-yourself option with step-by-step, self-guided instructions; or (2) access to round-the-clock U.S.-based technical experts on bot and virus removal.

This screen shot shows what the Constant Guard Center looks like, followed by what a user can discover about the malware they have:



Bot Assistance

A 'bot' is a malicious form of software that uses your computer without your knowledge to send spam, host a phishing site, or steal your identity by monitoring your keystrokes. Since bots are not viruses they require additional protection on top of traditional anti-virus software. Please select an option below to remove bots from your computer.

Take Action Now

If you received a notice from XFINITY or believe your computer is infected, it is important that you remove the bot from your computer immediately.

Option 1

Do It Yourself
Constant Guard™ from XFINITY®
Step-by-step, self-guided instructions from Constant Guard.

Option 2

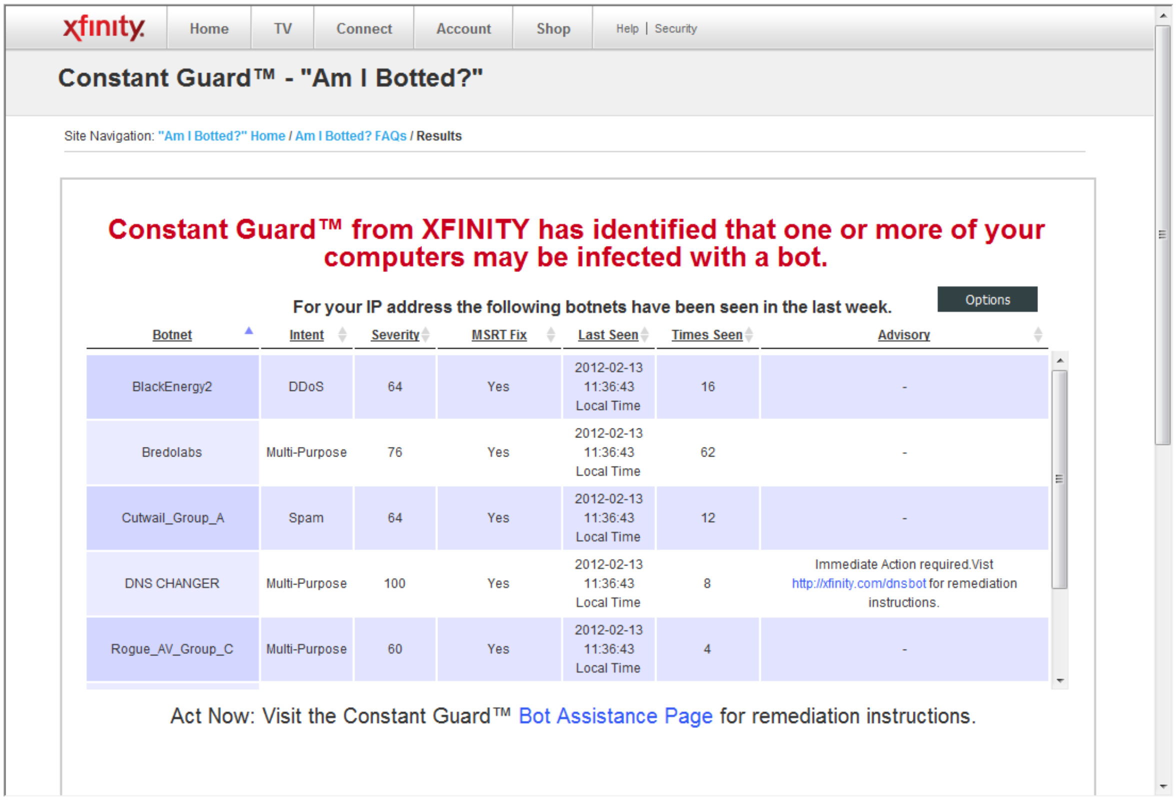
Professional Tech Expert
XFINITY® SIGNATURE SUPPORT
24/7 access to North America-based tech experts for fast, affordable bot and virus removal. Click to learn more or call now.

Call 855-550-3678

FAQs

- What is the Constant Guard Program?
- How can I tell my computer is infected with a bot?
- How did Comcast determine that I may have a bot?
- Can I opt out of receiving future Service Notices?
- What is XFINITY Signature Support?
- What is a bot?
- How do I know the Alert Notice is from Comcast?

Read More FAQs...



Constant Guard™ - "Am I Botted?"

Site Navigation: "Am I Botted?" Home / Am I Botted? FAQs / Results

Constant Guard™ from XFINITY has identified that one or more of your computers may be infected with a bot.

For your IP address the following botnets have been seen in the last week.

Botnet	Intent	Severity	MSRT Fix	Last Seen	Times Seen	Advisory
BlackEnergy2	DDoS	64	Yes	2012-02-13 11:36:43 Local Time	16	-
Bredolabs	Multi-Purpose	76	Yes	2012-02-13 11:36:43 Local Time	62	-
Cutwail_Group_A	Spam	64	Yes	2012-02-13 11:36:43 Local Time	12	-
DNS CHANGER	Multi-Purpose	100	Yes	2012-02-13 11:36:43 Local Time	8	Immediate Action required.Vist http://xfinity.com/dnsbot for remediation instructions.
Rogue_AV_Group_C	Multi-Purpose	60	Yes	2012-02-13 11:36:43 Local Time	4	-

Act Now: Visit the Constant Guard™ Bot Assistance Page for remediation instructions.

Comcast recognizes that consumer-based security tools need to work in conjunction with network-based measures to help secure networks and safeguard end users from cyber threats. Comcast has invested substantial resources to deploy state-of-the-art technologies and applications to secure its network.

Comcast's DNSSEC Deployment

The Domain Name System (DNS) is responsible for translating host names (like www.comcast.com) to Internet Protocol addresses (the addresses used by computers to route Internet traffic around the world) and it is critical to the normal operation of Internet-connected systems. Domain Name System Security Extensions (DNSSEC) is an enhanced level of Internet security that ensures the authenticity of the sites that consumers seek to access when they type domain names into their browsers for example, and prevents them from being unwittingly directed to fraudulent replicas of those sites.

Comcast this year became the first ISP in North America to fully implement DNSSEC. Comcast’s decision to deploy DNSSEC has its origins in the 2008 discovery of what has come to be known as the “Kaminsky Vulnerability.” In July 2008, Dan Kaminsky, a security expert, announced the discovery of a serious and fundamental security vulnerability in the DNS. The so-called “Kaminsky Vulnerability” is a flaw that affects the way DNS servers handle requests to translate words into numbers, allowing knowledgeable hackers to trick the servers into redirecting web surfers and other Internet users to malicious web sites, among other risks. What made Kaminsky’s discovery all the more troubling is that the flaw is not just a bug unique to a single platform; it is a fundamental design flaw in the DNS protocol itself, which allows attackers to easily perform “cache poisoning” attacks on most nameservers on a widespread basis.

DNSSEC essentially patches the security hole in the DNS that was exposed by Kaminsky. Without DNSSEC, the dangers to ISPs and their end users from this security vulnerability are numerous. Left unresolved, hackers could, for example, operate “phishing” scams or “man-in-the-middle” attacks, in which users are directed to fake web pages for supposedly legitimate banks or businesses where they are tricked into disclosing sensitive personal data, including credit card and banking information. Web traffic, email, and other important network traffic can be redirected to systems under an attacker’s control, where it can then be used for a wide variety of criminal activities. Users can be led to download unwittingly malware that threatens not only their personal information and devices, but also the integrity of an ISP’s whole network.

In response to Kaminsky’s discovery, Comcast not only patched its systems prior to the public announcement of the vulnerability, but also immediately started to investigate deploying DNSSEC. We launched a DNSSEC trial in October 2008 to understand and document the steps that ISPs and other implementers should undertake to implement DNSSEC-capable resolvers widely across large-scale networks. In February 2010, we expanded our trial to all production network DNS server locations across the country. Comcast performed this upgrade at the same time that it was upgrading its systems to handle IPv6, the next generation of IP addressing, which is something many other ISPs are doing now as well. Later that year, the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign, Inc. collaborated to deploy a signed DNS root zone, a seminal step in enabling DNSSEC globally. This in turn enabled Comcast and other ISPs to be in a position to begin to validate names using an official and public root rather than a temporary one for testing. After that, many top-level domains (TLDs) such as .COM, .NET, .ORG, and .GOV followed suit and signed their respective TLDs, enabling us to both sign domain names in DNSSEC-enabled TLDs, and to perform DNSSEC validation when our customers seek to access a web site or other domain name-based Internet resource.

ISPs play two critical roles in DNSSEC. The first is to validate DNSSEC as part of the DNS lookups performed for users. These lookups occur when a customer tries to access a site, such as www.comcast.com or www.paypal.com. When a Comcast customer tries to connect to that web site, a Comcast DNS server checks that domain name, and verifies the signature to ensure that it is valid and has not been tampered with by hackers. A customer will only be connected if this security verification has been passed, which occurs so quickly our customers do not even notice that it's being done.

The second role is to cryptographically sign the domain names that the ISP owns (such as www.comcast.com and www.xfinity.com), so that when customers or others using DNSSEC try to connect to services in those domains, they can validate the security of the associated DNS responses. ISPs typically own or manage thousands of domain names.

DNSSEC will help to enhance the security of our customers' Internet experience. But its real impact will be felt as it becomes comprehensively deployed across the entire Internet ecosystem. To that end, Comcast has been actively engaged in industry-wide efforts to encourage others to adopt DNSSEC. On behalf of Comcast, I have been actively involved in the Federal Communications Commission's Communications Security, Reliability and Interoperability Council ("CSRIC") Working Group 5 on DNSSEC Implementation Practices for ISPs. ICANN, the Internet Engineering Task Force (IETF), the Internet Society (ISOC) and many other groups are also working hard to make DNSSEC adoption a top priority across the Internet ecosystem.

Accelerating the rate of DNSSEC adoption by ISPs is not without challenges. There are operational procedures, network equipment, and software that may need to be adjusted or upgraded to support DNSSEC validation, and some companies may perceive the immediate costs of implementation to outweigh the rewards. There are other challenges to be faced as well. For example, in the past six months we have experienced several instances of .GOV domains with serious errors in their authoritative data, causing affected domain names to fail DNSSEC validation, which made these sites unreachable for our customers until those domains were fixed by their administrators. These were not always easy to resolve, as establishing the contact information and an escalation path for domains in the .GOV TLD, as with all other domains, can be fairly challenging (due in part to deficiencies in WHOIS-based data, an issue that is getting attention within ICANN). In addition, the .GOV domain infrastructure could be more closely monitored in order to identify and rapidly resolve DNSSEC validation in a coordinated fashion rather than having each ISP inefficiently trying to notify domains and track these issues to resolution on their own (there are some efforts in these areas, but they may need more resources). The problems associated with the .GOV TLD are not uncommon for early adopters of any new technology, especially considering that the rate of .GOV DNSSEC adoption is actually quite high compared to other TLDs. This will be an issue that will occur as more domains sign, so it is important for the Internet community to foster good, reliable, and repeatable domain signing practices, which will clearly enhance the security benefits associated with DNSSEC deployment.

Comcast has worked hard to be a leader with our DNSSEC deployment. As of today, over 18 million residential customers of our Xfinity Internet service are using DNSSEC-validating DNS servers. In addition, all of the operable domain names owned by Comcast, numbering over 5,000, have been cryptographically signed.

The expansive deployment of DNSSEC unquestionably will help to foster a more secure environment on the Internet, but we are only too aware that cyber threats are ever-changing. The growing sophistication, number, and scale of cyber threats underscores the importance of ensuring that ISPs and other key players continue to have considerable flexibility to address and respond to those threats, and to be able to do so as rapidly as possible. As important as DNSSEC is, it is just one of many resources available to improve security on the Internet.

Comcast's Participation in Public-Private Cybersecurity Initiatives

In addition to investing in network-based security tools and consumer-oriented offerings, Comcast has taken an active role in industry-wide and public-private initiatives aimed at addressing key cybersecurity issues on a systemic level. Comcast is an active participant in the

FCC's CSRIC, which serves as an important forum for developing best practices and voluntary mechanisms for ISPs to meet cybersecurity threats (and other issues). Comcast personnel are currently participating in several CSRIC working groups focusing on issues like Network Security Best Practices (CSRIC WG 4), DNSSEC Implementation and Practices for ISPs (CSRIC WG 5), Secure BGP Deployment (WG 6), and Botnet Remediation (WG 7, chaired by Comcast Fellow, Michael O'Reirdan).

Comcast is also a sponsor-level member of the Messaging, Malware, and Mobile Anti-Abuse Working Group ("MAAWG"), which is also chaired by Mr. O'Reirdan. MAAWG is the industry's largest global trade association that works against messaging spam, malware, viruses, denial-of-service attacks, and other online exploitation. MAAWG has been particularly active in developing voluntary practices that could serve as a framework for botnet remediation. It has published several reports and comments on the issue, drawing from technical experts, researchers, and policy specialists from a broad base of ISPs and Network Operators representing over one billion mailboxes, as well as from key technology providers, academia, and volume sender organizations. MAAWG is currently engaged in a comprehensive effort to develop a program that will gather true cross-ISP bot infection metrics. The MAAWG metrics will help scope the size of the problem, and measure the success of the industry's efforts to combat it.

In addition to its involvement in these groups, Comcast is participating in an ongoing anti-botnet initiative, spearheaded by the Administration, to initiate a multi-stakeholder process aimed at developing a set of common principles for addressing botnet issues. This effort is aimed particularly at highlighting the most effective practices and protocols related to botnet detection, mitigation, and remediation, as well as consumer education. There have also been discussions centering on strategies for targeting criminal behavior, including ways to reduce recidivism, increase the effectiveness of botnet takedowns, and decrease the number of botnet command and control servers, as well as the number of messages conveyed between the servers and infected machines.

Comcast is also involved in a range of other organizations where security practices are discussed or worked on in other ways, including the North American Network Operators' Group (NANOG), the joint FBI-industry group InfraGard, and the Domain Name System Operations Analysis and Research Center (DNSOARC), among others. And I personally serve on ICANN's Security and Stability Advisory Committee (SSAC), as well as on the Board of Trustees of ISOC, which has been instrumental in supporting key security initiatives like DNSSEC. Comcast also is a founding member of the Broadband Internet Technical Advisory Group (BITAG), which from time to time may touch on security-related work.

Conclusion

As you can see, Comcast has strong incentives – without the need for a government mandate – to explore and implement successfully a wide range of cybersecurity measures. We believe that, to be effective, it is vital that everyone who is part of the Internet ecosystem play a meaningful role in cybersecurity. That includes private and government networks, personal computers and other device makers, application providers, software developers, and others. ISPs and other affected entities must have the flexibility to respond to real-time botnet and other security threats in a manner that minimizes delay, and maximizes initiative and innovation. This is especially true since the threats evolve far more rapidly than any laws or regulatory framework. For example, a few years ago, spam seemed to be a primary focus, but that has now shifted to malware and bots, so organizations must have the freedom to remain nimble and handle whatever comes next. In addition, the Internet itself is an organic and ever-changing thing, and the pace of innovation within it is amazingly fast.

Thus, flexibility is absolutely necessary in light of the high-velocity changes in technology, business models, service, application vendors, and customer devices employed by each network operator and/or installed by Internet users in their homes or on their devices. Indeed, a government-mandated "one size fits all" approach could actually undermine cybersecurity by allowing criminals and hackers to launch an attack on multiple networks simultaneously if they are able to circumvent uniform or homogeneous detection and deterrence measures, or could constrain the pace of innovation in Internet-related technologies, services, and applications.

In contrast, clarification of the rules for inter-industry and industry-government information sharing on actual or potential cyberattacks would enhance cybersecurity preparedness and response. Information sharing is critical to effective cybersecurity efforts, but it potentially conflicts with statutory provisions, including the Electronic Communications Privacy Act ("ECPA"), the Freedom of Information Act, antitrust restrictions on intercompany sharing of proprietary information, and privacy provisions in the Communications Act. The uncertainty over the applicability of these laws to cybersecurity efforts can create procedural impediments to the timely sharing of relevant information. We support Congress' efforts to review these issues and provide clarification.

The government also should consider embarking upon a consumer education campaign that would utilize Public Service Announcements and other outreach tools to enhance public awareness and understanding of cybersecurity issues in general and bot/malware threats in particular. In addition, special research and development tax credits to encourage the development of bot/malware-related end user notification and remediation tools, and special tax credit for costs related to notifying and remediating customers affected by malware could also accelerate deployment and adoption of consumer-oriented tools that promote cybersecurity and make network environments safer for all consumers.

Thank you again for inviting me to testify. I would be happy to answer any questions you may have.