Routinized Desktop Intervention and Remediation

Corresponding Author Contact Data:
April Lorenzen, Dissect Cyber, data@dissectcyber.com

Colophon: Initial edition published November 14, 2013

Abstract

Desktop computers around the world are being cleaned up by their owners with help from local organizations. Education and resources for computer virus prevention and clean-up are provided locally by a variety of programs sponsored by government, industry associations, NGOs or commercial interests. In this paper we take an in-depth look at the methods used by and results from four different approaches. A list of resources is included for those who would like to create a similar program for their community.

Background

Cyber criminals are infecting innocent victim computers with malicious software at an alarming rate and enormous cost to the global economy. Personal and financial information is sucked out of victim computers by key loggers and advanced browser spying systems, defeating even multi-factor and certificate-based login security systems. The computing power and Internet connection of the infected computer is further abused to carry out malicious attacks on others. Criminal "bot masters" join large groups of these infected desktop computers together in networks often called botnets that are powerful enough to knock out major enterprises and affect government networks.

Technology-only solutions have not worked to rid the Internet of the danger of infected desktop computers and deny computing resources to criminal enterprises. Education, empowering with knowledge and the human component each have vital roles. Un-informed users can always be "social-engineered" to follow malicious instructions to get around any barrier that has been installed to protect. Technology can help identify homes and businesses with infected computers inside but often those with the data are not equipped to communicate with consumers.

The four organizations profiled herein are examples of those that stepped forward to fill this gap and, in that advance, provided working models that can be readily emulated by enterprises interested in providing structured interventions for neutralizing botnets at the root. Each has sought to empower users with solutions for cleaning up their machines while providing education about how to prevent re-infection. This two sided-approach aids in removing computer cycles from criminal control and making the larger networked community more resilient against attacks of all types.

National CERT (Computer Emergency Response Team)

Japan began a five year project in 2006 called the Cyber Clean Center <https://www.ccc.go.jp/en_index.html>. The project is structured with a steering committee over three specialized working groups. The steering committee consists of two government ministries while the working groups include ones that specialize in infection prevention (IPA), virus removal (JPCERT) and countermeasures (Telecom-ISAC.)

Internet Service Providers (ISPs) voluntarily participate and receive data that helps them identify their infected customers from the Telecom-ISAC working group. ISPs notify their customers by postal mail and sometimes email, including a special link codified for the type of infection that was detected. About four out of ten who are sent a notification visit the special link. There they get help to understand the problem, fix it for free with a dis-infestation tool, and are offered additional options for connecting with paid-for help.

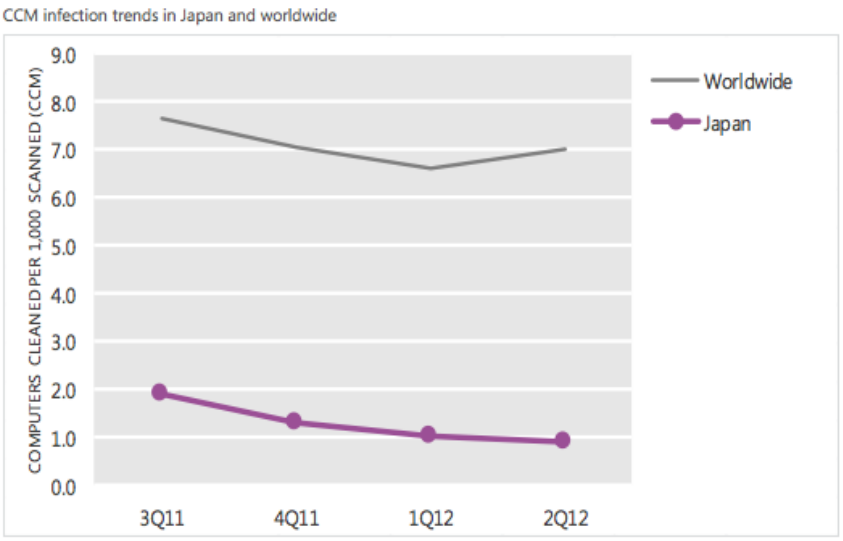
One of the working groups operates malware honeypots, collecting new malware samples, analyzing and monitoring the activity of malware to find both infected hosts and command and control computers located within the participating ISP networks.

The Cyber Clean Center started with eight large ISPs participating in 2006 and quickly grew to what is now 72 participating ISPs listed on the CCC website.

Benefits

Independent measurement can be used to confirm the success of the Cyber Clean Center in reducing the number of infected computers in Japan. For example, the Microsoft Security Intelligence Report for the period ending June 2012 shows Japan's computer infection rate nearly an order of magnitude smaller than the worldwide average. For each 1,000 computers in Japan scanned by the Malicious Software Removal Tool in the second quarter of 2012, less than one was found to be infected. This compares to the worldwide average of 7 computers per 1,000 scanned.

Measuring the results is also built into the system design of the Cyber Clean Center program. Privacy of the infected user is preserved because the Cyber Clean Center does not know the identity of the user. The type of infection cleaned and the count of how many notified users visit the site is known by the codified link passed to the ISPs for use with each infected host report.



JPCERT's own figures support the independent evidence, showing 2005 starting at a measured 2.0 ~ 2.5% of users with infected PCs declining to 0.6% of users by 2010.

As a result of creating the Cyber Clean Center ISP consensus was developed for working together to counter the effects of botnets. This led to establishing industry-wide incident reporting. The abuse response culture improved at many levels, including a commitment to work together on the remaining challenges and evolving attack vectors.

Yurie Ito, Director of Global Coordination, JPCERT/CC typifies the cooperative spirit: "I think this international movement about clean up the cyber space as one of the measures to reduce the global cybersecurity risk is great. JPCERT is working with APCERT members to promote the idea among AP region. We will keep making agreements with experts resources for clean-up, catalogue useful data and make it available for our members."

JPCERT/CC next plans to focus specifically on measurement. "Measuring the bot infection and the reduction rate could be one of the indicators of the international cross-comparable Cyber Risk Metrics.", says Ms. Ito.

User Experience

Prior to implementing such a program there are often concerns voiced about privacy, how to notify potentially infected customers in a trusted manner, and what reaction may be encountered. JPCERT reports that users seem to be grateful to find out they may be infected. They also are appreciative of the assistance. Great care has been taken to insure that their privacy is preserved and the actions they take after notification are voluntary.

Users are notified by their own ISP, given access to a free tool to remove the infection where possible, education plus additional options for prevention of future infection. The notification may come by snail mail (postal mail), email or both.

Cost

There is no cost to ISPs to participate in the Cyber Clean Center program and their participation is voluntary. The dis-infestation tool is free to users as are the educational aspects of the Cyber Clean Center websites. For customers who need or prefer paid assistance or subscriptions to anti-virus software, a number of different options are provided as a resource.

NGO (Non-Governmental Organization)

In 2010, the iCode initiative began in Australia. The aims of iCode are centered around four cyber security principles of Education, Detection, Action and Reporting.

Although ISPs are the primary action-takers, the initiative was designed in cooperation with stakeholders from government, industry and consumer protection sectors. “The process was as important as the outcome”, says Peter Coroneos, who is credited as the original architect of iCode when he served as the Chief Executive of the Internet Industry Association of Australia. “We made sure we listened to the concerns and needs of every group. Internet security is a shared responsibility and people have to feel ownership for the initiative to be successful.”

ISPs voluntarily participate in the initiative, making a declaration that they are complying with the iCode provisions. In exchange for the declaration the ISP is allowed to use the iCode trustmark.

Detection

One of the ISP responsibilities is to connect with sources of data about which of their customers may be infected. The iCode implementation materials provide contact information for these resources for Australian ISPs.

Action

The ISP pledges to take action when it has discovered indications of an infected customer and notify that customer. Any appropriate direct notification method may be used and some detailed examples are given in the iCode Compliance Checklist. If the ISP has properly prepared the customer with the knowledge that this could happen, they can even change the account password to prompt the customer to contact the ISP.

Education

iCode provides ISPs with uniform language to use when notifying potentially infected users and a website where the ISP can point the user for unbiased solutions and education. Visit http://www.icode.net.au/ to see the site that infected users arrive at.

Reporting

iCode compliant ISPs report serious criminal and security incidents to both CERT Australia and relevant law enforcement agencies. The implementation guide provides the details of when and who to contact.

Infrastructure

The infrastructure required for the iCode initiative going forward is essentially a web server.

Similar to the other desktop clean up initiatives, this is an effort of true collaboration where cooperation between diverse components creates the magic of the end result. Malware research organizations keep up a steady flow of data on which machines may be infected; ISPs identify and notify their users; users and security vendors cooperate to clean the machines, and government agencies look out for the legal aspects.

The architects of the initiative who work carefully and tirelessly to bring all of the collaborators together and provide the ideal guiding documents may be the most critical to success.

Cost

All materials and use of the iCode trustmark are free to ISPs who comply with iCode. Consumers likewise pay nothing to access the resources of the iCode clean up and education website.

Benefits

One of the reasons for iCode's success may be the inclusion of consumer advocacy groups (Choice Australia) and the Australia Privacy Commission early on in the process. Great pains were taken to protect consumer privacy in the design of the initiative. Media coverage was thus positive and accurate and users were more prepared for contact.

"The first reaction from the user is usually surprise to hear that their machine may be infected." says Peter Coroneos, now the President and Founder of iCode.org. "Then they express gratitude for the assistance."

By the measure of Microsoft reported Computers Cleaned per 1,000 (CCM) - Australian infection rates have been cut in half since 2010 Q1, prior to when the iCode initiative began vs the most recently reported 2012 Q2.

Today over 90% of Australia's Internet users are served by an iCode compliant ISP.

Trade Association

In 2010 the Anti Botnet Advisory Center (ABAC) began operations in Germany. ECO, the German Internet Industry Association, carries out the work with support from two government agencies, the Federal Office for Information Security (BIS) and the Federal Ministry of the Interior.

ABAC is unique in that it offers telephone support where users can be talked through solving their infection problems where possible. Another unique feature of the ABAC program is the distribution of a bootable CD which can automatically clean the infected users computer. The CD was distributed for free in a computer magazine and is also available on the ABAC website. As some newer computers don't have a CD drive, the scan and clean operation can also be initiated from a bootable USB drive.

Running a scan and clean operation from a bootable CD has the advantage of taking most opportunities for control away from malicious software. Anti-virus solutions that run under Windows booted from the hard drive are more likely to be circumvented by the infection, since the malicious software may be able to control everything that happens within the compromised Windows system.

Another unique feature of ABAC is the inclusion of security and protection products for Mac, Linux and mobile devices on the Private Sector Security Products page.

Cost

The ABAC program has made a serious investment to mitigate the infected host problem in Germany, spending in the first year about 1.2 million Euros. However, the cost per scanned computer in the first year has been only 1.65 Euros for all computers scanned, and less and six euros per infected computer that was cleaned.

Infrastructure

Many different players are collaborating to make the Internet safer as part of the ABAC effort. Banks and ISPs are part of the detection methods that inform their own customers privately about the likely infection of a computer at their home or business.

The user then visits https://www.botfrei.de. The website focuses tightly on three points - to Inform, to help the user Clean the computer, and to Prevent future infections. Within each section are very comprehensive and detailed instructions. ABAC has taken the time to provide the website in multiple languages to increase the effectiveness of the site to more users: German, English, French, Spanish, Danish and Turkish.

Some 99% of users have been able to carry out self-help and 1% have needed personal assistance from the telephone hotline. The hotline number is given out privately along with a code for that particular user who then calls anonymously. No identity data is shared from the ISP or bank to the ABAC hotline call center.

Benefits

ABAC was created with the goal of getting Germany out of the top 10 of botnet infected computers worldwide. Significant progress has been made toward this goal even while the number of malicious attacks has increased worldwide in the same time period. By the measure of Symantec Intelligence Quarterly report 2011 Q2, Germany's rank has gone from 3 to 22 for Spam Zombies, dropping from rank 3 to rank 7 for Malicious Activity, and dropped from rank 2 to rank 8 for bot infections.

Millions of pages on the BotFrei website are read each year by site visitors. Hundreds of thousands of computers are scanned each year using the free DE Cleaner software provided by ABAC and about 30% of those suspected of being infected have malicious files found and cleaned.

A 2012 version of the Symantec Intelligence Quarterly was not available online for comparison purposes. Using the Microsoft Security Intelligence Report as yet another independent measure, Germany is making steady progress since the inception of ABAC. Microsoft shares statistics from the Malicious Software Removal Tool as a count of computers cleaned per thousand scanned. A lower number indicates fewer malware infected computers found by Microsoft's Malicious Software Removal Tool (MSRT.)

Germany has achieved a low of 3 CCM in 2012 Q2, dropping from 5.6 CCM in 2010 Q3. The 2012 Q2 worldwide average is 7 Computers Cleaned per Thousand scanned, according to stats from Microsoft for the Malicious Software Removal Tool.

Sustainability

The initial plan for the project was guaranteed government funding for two years plus a guarantee from the trade association ECO that they would continue it for at least another year.

Commercial Internet Service Provider (ISP)

ISPs have also started programs to detect, notify, and help customers clean up infected computers. Less detail is known about the inner workings of these commercial offerings as they are often seen as a competitive advantage in the for-profit environment.

In the United States, AT&T, Cox, Sprint, Time Warner Cable, Verizon, CenturyLink and Comcast all either have a working program or have pledged to create them. Advantages for the ISP have been reported as reduced customer churn as users perceive an enriched service through automatic protection, notification and what is often a free suite of premium anti-virus software for all computers in a household. Speed is now a less important competitive factor vs security and protection features.

The user experience for a typical US ISP anti-botnet program is similar to those provided by other countries. Education regarding bots and malware is offered to all customers. If a household or business is detected as a possible location of an infected machine, a notice is sent either by email or displaying in the user's web browser. Sophisticated help mechanisms that are aware of the site visitor operating system (PC vs Mac for example) assist the user in obtaining anti-virus software, diagnosis and other help. Where

the issue is too severe to solve by self-help, paid help options are offered. After clean up, the user is further supported with education and encouragement regarding avoiding future infections and may be provided with free protection software.

SUMMARY DISCUSSION

Each type of effort profiled has had significant success in helping clean up infected machines and educate users. In many instances users have been able to solve their own problems with just well-organized steps from a trusted source plus free software.

Tougher cases of infection have been successfully addressed by directing users to their choice of paid services or assisting them via a free telephone hotline. Users are reported as being appreciative of both the notification and assistance.

Each successful program with measurable results involved strong public / private partnerships. The successful program designs were all centered around voluntary participation and careful preservation of user privacy.

The cost per clean up may turn out to be substantially lower than the financial losses estimated to be caused by each malware infected machine, and is certainly less than the fees a user will pay carrying their desktop machine into a repair shop.

Several of the non-profit programs state as their next goal to expand to more countries and to have collaboration between the programs operating in different countries. The iCode.org website has been launched for the purpose helping numerous countries implement their own regionalized version of iCode.

Local governments, trade associations, ISPs and other interested parties are encouraged to work with their regional CERTs (Computer Emergency Response Teams) and the architects of existing programs to find a model that is right for their own budget and population, building on the accomplishments of successful programs.

RESOURCES

Anti Botnet Advisory Center - Germany
https://www.botfrei.de

Peter Coroneos, President of iCode.org - Australia
http://www.linkedin.com/pub/peter-coroneos/2/553/260

Online Trust Alliance ABC's for ISPs
https://otalliance.org/resources/botnets/index.html

Cyber Clean Center - Japan
https://www.ccc.go.jp/en_ccc/

Comcast ConstantGuard - US

https://security.comcast.net/constantguard

Irish Anti-Botnet Initiative – Ireland

http://botfree.ie

Cyber Curing System / e-Call Center 118 – Korea

http://eng.krcert.or.kr/service/cyber.jsp

Anti-Botnet Working Group – Netherlands

Abuse Information Exchange – Netherlands

Autoreporter – Finland

http://www.tietoturvaopas.fi/

Malware Free Switzerland – Switzerland

http://www.swissinfo.ch/eng/swiss_news/Cleaning_up_Switzerland_s_internet_sites.html?cid=33433970

Advanced Cyber Defence Centre – European Union

http://botfree.eu