Global Information Assurance Certification Paper

Spyware - Recent Evolving Issues
Daniel M. Replogle
November 13, 2000

Overview

Since the inception of the Internet there has been an overwhelming curiosity by a range of interests to know who does what on the web. An expected level of privacy by an Internet user is decreasing and may cease to exist because of this curiosity. This temptation to invade individual privacy is not limited to freelance hackers and has lured not only small 'dot coms' like Doubleclick and Conducent/Timesink, but the Intels as well.

Processes are evolving to reduce personal privacy and among the different processes is an evolving system recently defined as Spyware.

Spyware Definition

Steve Gibson of Gibson Research Corporation has created a definition of Spyware:

Any software communicating silent background use of an Internet 'backchannel' connection which does not truthfully disclose the proposed backchannel usage and does not receive receipt of explicit, informed consent for such use.

There are efforts being made by many to identify these Spyware 'backchannel' programs.

Two Examples

The OptOut freeware software program (http://grc.com/optout.htm) is one of those efforts.

In the OptOut documentation, an attempt is made to graphically characterize these software packages and creates an Index of Known Spyware. See Figure A.

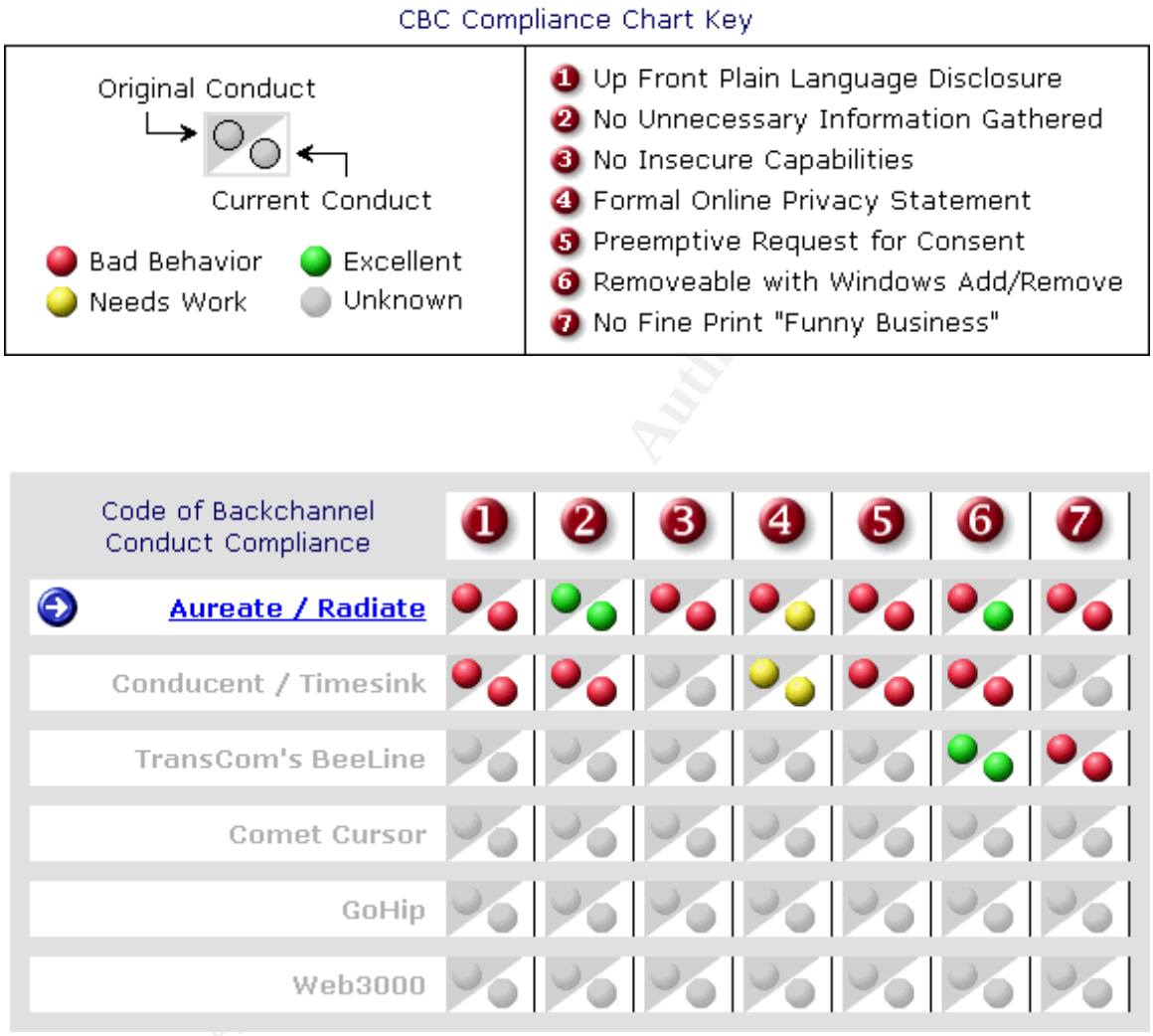

Figure A

Steve Gibson in his Optout program creates a table listing the Spyware company along with 7 categories which directly relates to the definition of Spyware along with his interpretation of their (non)-compliance, both original form and current. This is an excellent mechanism for a more complete understanding of the Spyware situation which is constantly evolving. This type of table could become a living document which describes the current condition at any given time.

There is also another spyware detection and removal tool which should be mentioned. It is called Ad-aware version 3.61 by Lavasoft.(http://www.lavasoft.de) Below is a brief description of it. It is mentioned here because it detects additional Spyware components which the Optout tool does not detect. These are both excellent tools but are separate systems which indicate a need exists for more than one tool to detect spyware components on a client. See Figure B.

Figure B

With the OptOut freeware spyware detection and removal utility, among other actions, it searches the PC for:

Adimage.dll, advert.dll, advertx.ocx, advert203.ocx, amcis.dll, amcis2.dll, c:\windows\amc*.*, c:\windows\amcdl*.*, htmdemg.dll, ipcclient.dll, msipcsv.exe, tadimage.dll, and tfde.dll.

This looks to be an excellent start on the identification process of known spyware programs and along with suspected spyware activity, Gibson Research is developing systems to detect the **CONTENT** of what is being transferred back via the backchannel.

Future Detection Systems in Development

Steve Gibson is currently working on a commercial version of the OptOut program and it is reported that it possesses the ability to update itself to detect future violators who use defined backchannel stealth activity.

An ability like this will mimic today's anti-virus programs and while virus authors may or may not be widely known, a corporation who sponsors Spyware may not want to have its name exposed as a participant. This will hopefully have an effect on the decline in future Spyware.

Spyware Tag not Appreciated?

However, some personal findings indicate that there may be a movement by corporate free enterprise to fight security efforts at being tagged as Spyware possibly threatening legal action for libel and at the same time continue their private information gathering activity.

There is a marketing company named Conducent/Timesink (www.conducent.com) whose involved in the production and bundling of certain advertising plug-ins designed for forwarding advertisements to the software that will run them when it is being used. One of the components of these plugins is a file named **tsadbot.exe.**

This file was initially identified by TrendMicro, a major anti-virus company, as a Trojan because of the activity displayed.when installed onto the clients machine. See Figure C.

Figure C.

Like many Trojans, it, in conjunction with the other system components, establishes a 'backchannel' on the client's internet connection and sends 'content activity information such as advertising impressions and click through data back to Conducent for daily reporting'. That activity is known and documented. About two weeks after TrendMicro began to identify the Troj_Tsadbot entity, TrendMicro **removed** the detection of this Trojan from their pattern files and future pattern files!

Let's go over this again in detail.

On approximately October 7, 2000 (give or take a day or two) TrendMicro rolled out the 785 pattern file, lpt$vpn.785. This was the **first** pattern file to detect and remove the above described Trojan. Less than two weeks later, the 788 pattern file was rolled out. This was the **last** pattern file to detect Troj_Tsadbot.

On pattern files later than 788, the ability to detect Troj_Tsadbot was removed.

After communicating with a Technical Account Manager from TrendMicro, it was learned that the reason for detection removal of this Trojan was that it was considered harmless and was not destructive in nature.
The creation and release of pattern files by any major anti-virus company has to be described as a continuous activity. Under normal conditions, a pattern file is released by TrendMicro once every week, in many cases, more often than once a week.

In addition, TrendMicro's pattern files contains detection mechanisms for dozens of what are called Joke programs which are non-destructive in nature but do range from funny to annoying to insulting and TrendMicro has made the decision to include these Joke programs as subject to detection and removal.

Decision Conflict or Consistent Philosophical Move?

The decision to **detect** and remove non-destructive 'Joke' programs produced by virus and malware writers and the decision to **not detect** and remove a backchannel Trojan produced by a marketing oriented corporation seems to be in conflict. It suggests there may have been communications between these companies and an agreement by TrendMicro to not detect this backchannel trojan.

There is another explanation for this decision which sheds a positive image on TrendMicro. This more likely motive for this supposedly conflicting decision maintains their high level of integrity as a major anti-virus company.

That is they recognize the nature of this Trojan and that their anti-virus system is not designed, nor should it be, to deal with this type of software entity. The detection and removal of only the tsadbot.exe file is a completely inadequate method of dealing with the detection and removal of these types of backchannel trojan systems.

How Do We Detect and Remove?

Systems to detect and remove these backchannel Trojan spyware have already been mentioned and are still being refined and developed. However, these systems like Optout and Ad-aware have recognized limitations. They are reactive systems which detect and remove after the fact.

Other means of protection against backchannel spyware systems include the development of Personal PC Firewalls such as Zonelabs ZoneAlarm and other personal PC firewall products.

The ZoneAlarm personal PC firewall product is able to alert the user and identify both

incoming network traffic and applications which are on the users machine which attempt to communicate with the Internet. This alert and identification system can prevent user information acquisition by a backchannel spyware system. However, the user still has to determine how to remove the Spyware system from their machine once identified.

In A Perfect World

The perfect situation would entail the producers of these spyware systems to completely and honestly disclose the usage of the backchannel and report how it is being utilized. It would be naive to believe this will occur.

In some cases, the producers of these spyware systems argue that they do completely and honestly disclose this backchannel usage when they embed its usage in the small print of the End Users License Agreement (EULA).

Range of Motivations

It's possible to catagorize the range of motivations of these evolving spyware systems and they are broken down into 3 arbitrary increasing levels of compromising action

Low Compromise Actions - The above description of the Troj_Tsadbot spyware system and other spyware systems like it may be classified as low compromise actions. It is believed at this time that marketing information and tracking of users across the internet is what is being collected. It could easily be argued that this is not a low compromise activity because it puts at stake the loss of personal anonymity and freedom.

Who is/has doing/done this?

Conducent/Timesink, Doubleclick, AOL, Disney, Mattel, Microsoft, Intel, Broderbund, there are too many names to mention.

Medium Compromise Actions - This level of activity breaks away from the corporate free enterprise involvement and moves into definite areas of illegal activity. It involves the theft of personal information such as social security number, credit card numbers, passwords and other personal information.

There are dozens of Viruses, Worms, and Trojans in the wild whose interests lie in obtaining personal information such as stated above. These 'In the Wild Trojans' which set up backchannel connections on the compromised infected client and are very dangerous forms of Spyware. Personal Firewalls such as Zone Alarm have been developed to thwart these evolving Spyware systems.

High Compromise Actions - This level of activity involves Information Theft at the highest level. It includes Industrial Espionage and an excellent example of Spyware activity at this level is the actions and accomplishments of the Troj_QAZ worm. The Troj_QAZ worm is responsible for the recent hack of the Microsoft Corporation.

Summary

This backchannel activity is occurring in the personal and coporate environment right now. Since many of these Spyware products are bundled with Freeware or Shareware programs, they get loaded on the users desktop PC when the user downloads the program from the Internet. In most cases, user desktop PC's are safe from Medium and High Compromise Actions when inside the corporate firewall. In the corporate environment, it is the remote user who is at the greatest risk being exposed to all levels of compromise unless the remote machine is being protected via a personal PC firewall product or other means of protection. It is this section of the population that the corporation should be aware of and consider for protection.

References:

Gibson, Steve - Gibson Research Corporation - Opt out: Code of Bacchanal Conduct. Laying Down the Law to Spyware! URL: <http://grc.com/oo/cbc.htm.> October 18, 2000

LavaSoft, Ad-Aware 3.61, URL: <http://www.lavasoft.de>

Smith, Kenneth - Is Your Freeware Spyware? October 16, 2000
URL: http://www.voiceofthepublic.com/IsYourFreewareSpyware.html#mattel

Conducent/Timesink - URL: <http://www.conducent.com.> Software, Technology. November 12, 2000.

TrendMicro URL:
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_TSADBOT
Nov 12, 2000

ZoneLabs URL: <http://www.zonelabs.com.> As of November, 2000

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS