GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Nishantha Karunaratne
July 15, 2003
SANS Security Essentials
GSEC Practical Assignment
Version 1.4b

Understanding the GATOR – A Brief introduction to Spyware

Abstract

Spyware is any software program that uses a background Internet connection to gather and disseminate information to an individual or organization without the user's knowledge and consent. This information includes the user's private data, secret data and corporate data. Some of the examples are: user web habits ranging from consumer behavior, traffic patterns, computer system details, and password, credit card numbers etc. Today, with the wider presence of more effective "web-based Behavioral Marketing Techniques", the usage of the spyware and adware are ever increasing, threatening all the information security pillars - confidentiality, integrity and availability. In marketing aspects, spyware and adware are two of the most useful tools. However, for information security these are two of the most problematic tools.

This paper aims at discussing the basics of "spyware" using the famous adware tool Gator e-wallet. The methodology includes setting up a test lab, installing Gator in the test lab, and comparing the "pre" and "post" installation status using existing tools such as anti-virus, firewall, task manager, windows explorer and system registry. This paper also continues to introduce new spyware-tools to further analyze gator behavior and briefly discuss techniques used by gator to penetrate the available security boundaries. In conclusion, this paper will highlight some of the risks spyware is posed with and, counter measures to minimize the risk level.

Setting up the Test Lab

Throughout the discussion, the following definition on Spyware by Steve Gibson was used.

"**Spyware is ANY SOFTWARE** which employs a user's Internet connection in the background (the so-called "back channel") without their knowledge or explicit permission. Silent background use of an Internet "back channel" connection **MUST BE PRECEDED** by a complete and truthful disclosure of proposed back channel usage, followed by the receipt of explicit, informed, consent for such use. **ANY SOFTWARE** communicating across the Internet absent these elements is guilty of **information theft** and is properly and rightfully termed: **Spyware" –** Gibson [(1)]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Prerequisite: Stand-alone computer running windows 98 or above, Anti-virus Solution, Personal Firewall, Internet Connection. Please note that the presence of additional software will make some changes to the test results. (The test lab used in this study contained the following specification – OS=Windows 2000 Professional, Antivirus=Symantec Antivirus Corporate Edition 8.0, Personal Firewall=Sygate 5.1, Internet Explorer 5.0, Sygate Personal Firewall is available for download at http://smb.sygate.com/download/download.php?pid=spf or http://download.com.com/3001-2092-10184369.html

The first step of the exercise is to get the print out of all the security logs and mark these documents set as the "pre" status. The logs should obtain from the following sources: Anti-virus, Firewall, and Event Viewer. In addition to that, the list of running processes, (Press Ctrl + Alt + Del -> Task Manager > Process), copy of the registry, (Start -> Run > regedit > export registry file. The export range should be "all") and the list of file names available in the Program Files -> Common files folder.

Installing Gator in the Test System:

Some of the reasons behind the selection of Gator are: It could be easily installed. (Definitely free of charge) Gator was in the field for last few months and continues as the fastest emerging spyware. [2] Gator is the main product of the largest behavioral marketing network the Gator Advertising Information Network (GAIN).

As listed in the spyware-guide "Gator is a software product that can automatically fill in passwords and other form-elements on Web pages. However, its main purpose is to load an advertising spyware module called OfferCompanion, which displays pop-up ads when visiting some Web sites. Gator boasts that since it's software is always running, it can spam users with "Special Offers" and other ads anywhere they go (even competitors' sites) with remarkable targeting capabilities, since it can spy on what sites the user is visiting. Gator stays resident in the background, hides itself from user, shows advertisement to the user, does some changes to the web browser, and connects to the Internet itself." [3] – Spyware-Guide

Information URL:
http://www.gator.com/ and http://www.gatoradvertisinginformationnetwork.com/

The easiest way of installing the Gator in the Test System is simply downloading **the Gator eWallet or "the world's most popular digital wallet"** from www.gator.com. It is important to print the Gator home page, and all the installation instructions pages and End User License Agreement and Privacy Statement. The document set should be marked as "Gator information" or some sensible name.

Now you could press "Download" button and follow the simple instruction on screen. Once the installation is completed, restart the computer.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

After the restart, you will see three consecutive messages. First message is an advertisement on “Date Manager and Precious Time”. Second Advertisement would be on “Memory Blaster” and third advertisement on “5% discount”. (This offer could be changed in time to time and/or region to region.) Install the “Date Manager and Precious Time” and “Memory blaster” and Skip the third advertisement.

Using existing tools to Understand Gator.

Anti-virus: Anti-virus is the primary security tool most of the users defend on information security threat. Most of them believe that with an updated “anti-virus-software” they are protected. The first log we should compare is the Anti-virus log.

The system should be scanned using the “scan all files” option. Once the scan completes, print the Anti-virus Log and insert this print out to a document set named “post” status.

After a comparison between the “pre” and “post” logs (specially the virus history part) you will not notice any changes. If you try changing your Anti-virus software and do some full system scans you will hardly see any changes to the anti-virus log.

Finding: **Anti-virus software could not be used to track “Gator” attacks.**

Registry: In Windows environment Registry is the Database repository stores all the computer configuration information and therefore, sometimes the whole system will become collapsed or unusable with a smaller Registry change. Hence, do not change any registry settings.

As the next step, the print copy of the registry should be added to the “post” status document set. If you compare these two registry settings the “pre” and “post”, you could notice some additions in the “post” registry copy. The four entries you could notice here are:

HKEY_LOCAL_MACHINE\software\gator.com
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run|cmesys
HKEY_CLASSES_ROOT\clsid{21ffb6c0-0da1-11d5-a9d5-00500413153c}
HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\uninstall\{6c8dbec0-8052-11d5-a9d5-00500413153c}

A Google Search [4] using keyword “cmesys” will help identifying this component as a “spyware” component.

Finding: **The Gator changes Registry Entries and adds “spyware” component to the Registry.**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Task Manager: Windows task manager is the next important source, you should consider here. In the list of running process, you could notice four additions made by Gator. You could use the "pre" document set to do the comparison. Those are CMESys.exe, Gator.exe, PrecisioTime.exe and DateManager.exe. You could notice that, with the Internet Explorer running or not, the Gator and CMESys are continuously running and consumes computers CPU time and Memory.

Finding: **Gator adds few processes to the tasks Manager and the processes remain active and consuming some computer resources.**

Windows Explorer: Next step is to identify the new files added to the system. Here we only consider one important directory called "scripts". You could locate the script directory in the following location: \root directory\program files\GMT\Scripts\.

Now you have to write down the names of the files listed in this directory.

Gator generates few script files based on the web sites that the user browses. To understand the Gator script generation process, we could do a very simple exercise by simply logging in to your hotmail e-mail account. Once you enter your password and login name, Gator will generate a pop up window and waits for user inputs. Based on the user input Gator should remember the users details. The user does not need Gator to remember his password and select "no" as the input to the Gator pop up window.

Now you have to switch back to the script folder and look for changes. Here you could notice a new file (hotmail.com.eps) was added to the directory. You could use "peek" [(5)] a free tool available at the following URL: http://www.simtel.net/product.download.mirrors.php?id=50399, to read the content of the script file. Peek has the ability of reading most of the file types without original associate file.

If you read the contents of scripts file using Peek, you could see some sensitive fields such as "password" and "credit card number".

One important observation here is Gator does not generate script file for unpopular web sites.

In the Gator.com home page, it clearly displays a web banner informing users, that Gator collects only the User's first name, Zip code and Country. Therefore, if gator uses this script to collect the user data, script should contain only about three fields and it should not contain any fields to capture sensitive data.

Finding: **Gator generates some secret script files, which could be used to capture the "sensitive information" without the knowledge and consent of the user.**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Firewall Log: The firewall is the next important point you should use here. If you analyze the traffic log, you could notice two applications connects to the Internet. The application names are GMT.EXE and CMESys.exe. You could easily block these two applications at the firewall level. As our aim is to understand the Gator behavior, you should not block the applications at this time. (During this time, you should not visit any www.gator.com or www.gainadvertisingnetworks.com.)

The following observation could be done using the firewall traffic log. CMESys.exe uses some assigned local ports such as 1110 (Client status info Cluster status info – used in NFS Communications) and 1106 (ISOIPSIGPORT-1), while GMT.exe uses both assigned and unassigned ports including -1126 (unassigned) 1103 (adobeserver-2) and 1109 (reserved iana port), 1191 (unassigned), 1187 (unassigned) 1179 (unassigned) 1170 (unassigned) 1169 (tripwire) 1161 (health poling) 1147 (unassigned) 1144 (unassigned) 1126 (unassigned) [6]. If you continuously check the traffic log, you could notice the gator changes its local port in time to time.

If you notice the above log, you could see the same application uses different randomly available unassigned ports. GMT was designed using a port hopping technology where it uses random dynamic ports other than the assigned ports making the traditional port-based blocking methodology ineffective. [7]

Another technology used by the GMT is HTTP tunneling. Using HTTP Tunneling GMT exchange requests and data through a standard Port 80 restricted firewall to and back from external Application Servers as easily as they can with no firewall in place. [8]

Finding: **Gator uses Internet Back Channel without the knowledge and consent of the user and Firewall is not the best solution for as the spyware uses new technologies like port hopping and http tunneling to skip the traditional firewall rules.**

Another one important observation you could see using your firewall log: most of the time is the spyware traffic volume is very low when you compare it to the other web based applications. This was implemented to hide from the user notification.

Finding: **Gator sends and receives packets in very low quantities to avoid the user notification.**

A new tool to analyze Gator behavior

With the lack of proper tool to identify, minimize and eliminate spyware attacks a new set of tools were introduced by several vendors and few academia. There are many "spyware removal tools" available both free and on commercial based. For this illustration lets use "PestPatrol"[9]. Also you could try some other spyware removal tools such as Lavasofts Ad-Aware (basic version free) Spy-

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ware eliminator, BPS Spyware /Adware remover, Spybot Search and Destroy (free) [10]

PestPatrol evaluation version could be downloaded form http://www.pestpatrol.com/downloads/eval/download.asp. Once the download is completed, install it to the test system and restart the computer. Once you finished scanning you could see a very detailed log file including the name of the spyware, its threat level and type, the location the spyware hides, and removal instructions.

Before we use the pestpatrol we could only identify very few numbers of the spyware, but now the result should show more than 150 spyware entries in your system. Most of the spyware you could simply delete using the Pespatrol.

Before you delete and completely remove the gator from you system, go through the log file. One interesting observation is Gator use "txt" file and (C:\Program Files\common files\cmeii\gatorsupportinfo.txt) and six "gif" (e.g. C:\Program Files\common files\gmt\Banners\13145\17826.0\memory-032803-pua.gif) to do its intended activities. As you are aware the txt and gig files are non-executable, you need some other technology to make this file executable. Gator uses steganography tools to hide the executable source code from its original file. You could use some of the stego tools such as s-tools4 [11] available in the Internet to reveal the hidden source code or executable files. However, Gator uses steganograpy together with encryption hardening the revealing of executable code.

Another important observation here is Gator use its uninstaller to further spread its activities. Whenever the uninstaller is activated, the spyware part bundled with the Gator also executed. Hence, uninstaller bundled with spyware could not properly used to eliminate the spyware from the infected system.

If you go through the information you collected during the Gator installation process, you could notice little important technique Gator uses to mislead the user. The End User License Agreement is a very lengthy and it hides most of the very important information from user eye. Once the user scroll down only he could notice the most strongest and important clauses in the Agreement The EULA contain so much information that it is difficult to extract meaningful information that deals with the information-gathering functionality. In addition, the meaningful data that deals with the information-gathering functionality is ambiguous.

During the installation process, first the Gator only asks "non-sensitive" information. After the completion of "password protection" form it starts requesting more sensitive information from the user. After user sees the Password screen, he usually feels somewhat protected, and compels to give information that is more sensitive. The sensitive information Gator try to get from the user includes even the card numbers. Here the Gator applies some non-technical kind of intrusion that relies heavily on human interaction and often

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

involves tricking other people to break normal security procedures. First Gator tries to gain the confidence of user in order to get the user to reveal sensitive information to the Gator.

Finding: **Gator uses new technologies like steganography to hide from the detection and some times uses non-technical techniques such as social engineering to mislead the user**.

Gator as a Spyware:

The following summary obtained during testing helps profile the Gator. Gator is a common spyware uses newest technology available.

Gator uses Internet Back Channel without the knowledge and consent of the user to send and receive information. When Gator uses the web to communicate, it uses new technologies such as http tunneling and web hopping to skip the firewalls. Steganography and encryption is used to hide from the user visibility. Low quantity of the traffic is another strategy Gator uses to hide from the user notifying. Its lengthy EULA and privacy statement includes few confusing clauses and the clauses related to risk is hidden from the users. Script generation and social engineering is used to collect information that is more sensitive from the users. Gator adds few processes to the tasks Manager and the processes remain active and consuming some computer resources. Anti-virus and firewalls alone could not be properly used to control the spyware problem. Un-installation of Gator is not a good solution to remove the Gator from the infected system, as its' uninstaller bundles with spyware component. Spyware removal tools are available to completely remove or minimize the danger of the Spyware tool.

Impacts or damages caused

As it is logged in, the PestPatrol Log Gator is responsible for "low" "medium" and "high" risks. The confirmed threatens of Gator by the PestPatrol are the Liability and Confidentiality. The Gator Privacy Statement and EULA include a clause referring to the Liability.

"Protected Parties assume no liability hereunder for, and shall have no obligation to defend you or to pay costs, damages or attorneys' fees for, any claim arising from: (i) any method or process in which Licensed Materials may be used by you; (ii) any results of using Licensed Materials; (iii) any use of other than a current unaltered release of Licensed Materials; or (iv) the combination, operation or use of any Licensed Materials furnished hereunder with non-Licensed Materials if such infringement would have been avoided by avoidance of the combination, operation, or use of the Licensed Materials with other programs, data, or other materials."

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This simply means the user of the Gator software is liable for whatever the damages caused by the spyware. Within the existing law frames, the custodian of the information system is accountable for the security of the information and the system. This creates major problem as the Gator's hidden communication is invisible and purpose of the usage is not clear.

If the Gator use infected computer and back channel to cause harm to other computers in the Internet the custodian of the system is liable to the damaged caused by the Gator. One other important point to consider here is the infected servers sometimes act as an AdServer and spam other users in the Internet.

Gators script Generation process and social engineering techniques to capture the sensitive information from user, creates doubts about the Gators real intention and objective. Whatever the sensitive information captured by the Gator is not accessible to the owner of the information (or the user) as it is encrypted. User does not have any thing about the information captured by Gator. In the "Privacy Statement and EULA" of Gator says, "We sometimes use third party contractors who may be given access to any information we have so they may perform tasks that might otherwise be done by our employees". Without clearly understanding the "Third Party" the users of Gator is giving their information to Gator. The user does not have any idea about the reputation of this third party, the measures the Third party has taken to protect the Sensitive information and the purpose of the usage of sensitive information.

Gator poses some threat to the "availability". Because Gator is closely monitoring the users Web behavior and based on that behaviors Gator targets some advertisement to the infected users desktop. This target-oriented advertising prevent the users from having the access to the original advertisement. This could result situations like those that the user is prevented from getting the original advertisement, which may consist more benefits.

By displaying the some unnecessary advertisement, (though the gator says "targeted advertisement"), unnecessary services running on the computer and usage of bandwidth to communicate with other ad servers creates problems in availability and productivity.

The Counter Measures to minimize the Spyware Attacks

As it is mentioned earlier, with the growth of Behavioral marketing, the new adware and spyware tools are added to the market from time to time. The updated spyware removal tool will be the solution from the technology side. Few important things should be addressed in the organizational or management level. Introducing a good IT policy and standard documents addressing the Spyware threat is one of the key thing the all IT and Management personal should think of.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The new application testing and authorization procedure should be implemented within the organization.

Discouraging free download minimize the spyware threats into some extent. Where the free download is necessary for organization, before the use of free download clarification and understanding of the EULA and privacy statement is more important. Developing and Implementing a Risk and Security Management Plan is another thing you have to consider. Regular IT Security Audit helps identify the new threat and solution of the organization. Most important thing in this whole exercise is to educate users about the damage the spyware caused to personally to them and all of you as a whole organization.

Reference:

1. Gibson, Steve. "What is Spyware"
   URL: http://grc.com/optout.htm (01 July 2003)
2. PestPatrol Inc. "Fastest Emerging Pests" last revised 10 July, 2003
   URL: http://www.pestpatrol.com/support/stats/fastest_emerging_pests.asp
   11 July, 2003
3. Spyware-guide.com "Gator"
   URL: http://www.spywareguide.com/product_show.php?id=10
   (20 June 2003)
4. Google.com "Search the web for cmesys"
   URL: http://www.google.com/search?hl=en&ie=ISO-8859-1&q=cmesys,
   (1 July 2003)
5. Simtel, "PeekPok.zip"

   URL: http://www.simtel.net/product.php?id=50399, 15 July 2003
6. IANA, "Port Numbers" (11 July 2003)
   URL: http://www.iana.org/assignments/port-numbers, 15 July 2003
7. Sandvine, "Press Release – P2P a Moving Target" 18 March 2003
   URL: http://www.sandvine.com/news/pr_detail.asp?ID=22 (15 July 2003)
8. dbovernet.com "HTTP Tunneling/Port 80 Cloaking"
   URL: http://www.dbovernet.com/httptunnel.htm (15 July 2003)
9. PestPatrol Download page
   URL: http://www.pestpatrol.com/downloads/eval/download.asp
   (15 July 2003)
10. PepiMK Software, "Spybot Search and Destroy download page"
    URL: http://beam.to/spybotsd (15 July 2003)
11. s-tools download page
    URL:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://webphysics.davidson.edu/Applets/Download_Files/Java11.html
(15 July 2003)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.