Breaking Computrace's Lo Jack for Laptops
J. Oquendo
joquendo@hushmail.com
4/25/06

After a company I worked for purchased Absolute's Computrace "Lojack for Laptops" product, I decided to re-write up a "How-To Defeat LoJack For Laptops" article. Why re-write it? Vendor still has not implemented fixes to address what I consider "deficiencies" and "false advertisements" with their product.

According to Asbolute's advertisement:

> **LAPTOP SECURITY PREVENTS LAPTOP THEFT.**
>
> Computrace is laptop security and tracking software which deters laptop theft and recovers stolen computers – guaranteed. Absolute also provides software inventory, computer inventory, PC inventory, PC audits, IT asset management, asset tracking, software license management, and data security tools and services.

Included in this document are some diagrams which explain my qualms on this product and how Computrace can not live up to its marketed expectation.

Previously explained: Computrace is nothing more than a piece of software that details what your machine is running, what software is installed, and what IP information is allocated to your machine at the time it reports to Absolute's network. This is some the information the reporting contains for some for those machines running this gimmick:

Call Tracking Information (for my own laptop)
Computrace Agent first installed on (first call): 11/10/2005 9:06:38 AM
Computrace Agent version: 814
Computrace Agent last called on: 11/13/2005 2:20:17 PM
Computrace Agent last called from: 192.168.0.1
Computrace Agent next call scheduled for: 11/14/2005 2:50:17 PM
Asset tracking data last collected on: 11/13/2005 2:20:17 PM

MY_USERNAME
MY_LAPTOP_NAME
Assig. Username:
Make: Dell Computer
Model: INSPIRON_6000 **Serial#** XXXXXXX
Asset# 11/13/2005 2:20:17 PM 814 Active

Absolute generates a template e-mail to notify customer's of issues:

> Dear Customer Center User:
>
> This is an automatic e-mail notification generated by the Customer Center alerting system.
>
> Please visit https://www.Absolute.com/public/secure/login.asp to investigate your new alert.

The following alert(s) configured for your account have been triggered:

* Alert Name: Last called 20 days ago
* Description: Pre-defined alert - if you don't wish to use this alert, leave it in a suspended status (note that it will be recreated in a suspended status if deleted)
* Alert Type: Automatic Reset in 10 days
* Alert Condition: Last Call Time - Greater or Equal To - 20 day(s) since last call
* Detected on: 24 Dec 2005 00:28:34:5

You have computers that have not called within a specific time period (as defined by the alert condition).

For customers with the recovery guarantee: Note that the guarantee becomes invalid for computers that have not called in more than 30 days. Please refer to your Terms and Conditions for more information.

For customers with the recovery service: The chances of recovering a computer post-theft are reduced if the computer is not calling regularly.

For customers with asset tracking: your asset data is likely to be out of date for computers that haven't called in recently

All Customers: You can use the ctmweb management tool to confirm that the agent software is installed and, if necessary, reinstall it. If the agent is installed, the ctmweb management tool can be used to perform a test call. Once machines call into the monitoring center, they automatically meet the call-back criteria for eligibility for the guarantee.To retrieve the list of computers, log into the Customer Center and follow the instructions below:

a. Click on Reports.
b. Go to "Call History and Loss Control" , click on "Missing Computers".

In the box below "Show all Computers where...", under where it states: "group name is" use the drop down to select the group name: "Recovery Guarantee" then to the right, enter 20 days. Once done, click on "show results".This will provide you with a list of computers that need attention.

ESN: XXXXXXXXXXXXXXXXXXX PC Name: [MACHINE_X] Username: [username] Department: [departmentname]

That message is letting you know that MACHINE_X hasn't been online. It is up to you to report it stolen so Absolute can retrieve it. There isn't anything other than a little program which runs after Windows has started, that waits for connectivity in order to scream for help alerting you or Computrace that something is out of order.

So let's look at what Absolute is using to find a stolen machine.

Computrace Agent last called from: 192.168.0.1

Absolute is solely relying on an IP address to track a machine. One of the problems with this is that they will need to go to court and request the information from the ISP on who used that IP address, after getting this information, they can only hope they will find the machine at that location. How much would it cost Absolute to go through these motions? Even if they did go through these motions, why should they when they can just refund someone the cost of the Computrace software. Or, what happens when a stolen laptop is using stolen resources for

connections? Like say an open Wi-Fi hotspot? What does Computrace expect to do when someone reinstalls an operating system over the system with their software running. That software is useless. It's that simple. Reinstalling an operating system over a stolen laptop will automaGically make Computrace as useful as an industrial freezer in Antarctica, useless.

Supposing you stole a laptop with Computrace installed on it, and actually wanted to keep the data, you have one of a few choices: copy the data, wipe the drive and make a clean OS installation, or you can simply kill the process and modify the Windows registry to rid yourself of this gimmick.

What are you looking for? A program called **RPCNETP.EXE**. You could search the registry for it and rename it, delete it entirely, stop the services by going to the Windows Control Panel/Administrative Tools/Services and stop it from there. Use Sysinternal's Process Explorer, Knoppix. I could count numerous ways to disable this product. As for the service Absolute offers, I've logged in twice in six months because I was wondering who was sending me those annoying alerts, and I wanted to see exactly what information was being passed over to Absolute's databases.

Absolute was notified of these issues last year and they responded to me and the company I worked for offering a refund. However, here was their method of refund - a Non Disclosure Agreement which I did not agree to nor did my former employer:

1. Definitions

(a) **"*Activity*"** means the relationship between the parties that arose as a result of the purchase by xxxxxx of a license and subscription for Absolute's Computrace® Lojack® for Laptops™ product, including without limitation subsequent communications between xxxxxx personnel (including xxxxxx's Senior IT Engineer Jesus Oquendo) and Absolute personnel with respect to the product's performance and technology.

(b) **"*Affiliate*"** of a party means any corporation or other entity that a party directly or indirectly controls, or is controlled by. In this context, a party "controls" a corporation or other entity if it owns fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control for the corporation or other entity.

(c) **"*Confidential Information*"** means any business, marketing, technical, scientific or other information disclosed by either party (including its Affiliates) which, at the time of disclosure is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the parties (or its Affiliates), exercising reasonable business judgment, to be confidential.

Absolute did not seek to remedy my issues with their product instead they offered us a refund if I agreed to keep my mouth shut. So much for NDA's since they were never agreed to. Here is Rob Chase's email in response to my concerns keep in mind that was the last correspondence I'd ever had with them. It became insane at one point with Absolute claiming that no one there had ever even spoke with me. Anyhow:

From: Rob Chase [mailto:RChase@absolute.com]
Sent: Thursday, January 12, 2006 4:58 PM
To: J. Oquendo
Cc: cagule@xxxxxx ; Trevor Wiebe
Subject: RE: Defeating Computrace's products ... follow up

Jesus,

I understand that Mr. Agule is working with our Mr. Wiebe to arrange a time to meet. I don't believe we'll be able to meet next week. In any event, they will arrange.

Regards,

Rob Chase, CA
Chief Financial Officer

Absolute Software Corp.
Keep *IT* Simple. Keep *IT* Safe.

tel. (604) 628-5119
cell. (604) 512-1554
fax. (604) 730-2621
toll free 1-800-220-0733
email: rchase@absolute.com

Suite 800, 111 Dunsmuir Street
Vancouver, BC Canada, V6B 6A3
Website: www.absolute.com

From: J. Oquendo [mailto:joquendo@xxxxxx]
Sent: Thursday, January 12, 2006 11:59 AM
To: Rob Chase
Cc: cagule@xxxxxx
Subject: Re: Defeating Computrace's products ... follow up

Let me start from the beginning on this since this whole thing has been lost in translation. The Computrace Your product was purchased under the notion it would provide a service. That service hasn't been working "clearly" in accordance to what your company is advertising. On this note, I notified your company to this back near the end of November. Your company's response? They never responded.

Beginning of December... "Hey your service is not doing what it states it is supposed to do." Your company's response? They still didn't respond. Mid December: "Your product isn't working is anyone there?" Still no response. Thus on Christmas Eve I wrote a paper called Breaking Lo Jack for Laptops. I sent it to those listed on your contact page... Still no response.

Your staff called here stating I was "misinformed" "so misinformed" that your company was "tracking my machine". Tracking my machine I thought, Really? It was unplugged. So the question was posted back to your staff at that point... "If you're tracking my machine where is it coming from?".

Surely if your engineers and salespeople can call here stating I'm misinformed, so misinformed that "they can see that laptop" and "here is its address", then they could have explained how they managed to get the information they sent us provided my laptop was powered off. We asked your staff. Your company's response? "He's wrong. Way misinformed." My response... Prove it. To date I'm still waiting on this proof. What the sent me seemed to be fabricated beyond belief.

Where did they get the information they sent to me from supposedly on the laptop in question when it was powered off. There is no way on the planet that the machine in question could have given your company anything, it was powered off. So what did your staff do? Did they fabricate information to send it to me. This seems to be the case from my eyes since I know that 1) I could never log in from a Department of Defense network (which was gathered from the data YOUR staff sent to us) 2) the machine in question was powered off and 3) even if it were powered on, there was no connectivity.

Now, from what you're telling me in your email below is "your staff is too busy to deal with this right now." So does that mean if my assets are stolen and I report it they will be too busy to track it? Same rules apply here. My laptop is where? You're company touts this product as if it would find it. So where is it? Where is it logging in from and when was the last time it logged in. Supposedly your staff saw it at that moment yet they provided me false information. The machine is running right now technically if I called and told you to wipe the data, you should be able to.

So to restate, all I wanted was an answer, not a runaround. I could post all the technical questions I want - but I understand technology enough to know when I'm being told a lie. Especially when someone tells me they're seeing my machine when its off.

I will take some time out next week to speak with whomever you want. I will even take the time to draw out Visio diagrams of scenarios YOUR ENGINEERS should have thought about and should be thinking about. You name the time, I will be on the phone. Anything else will be wasting both of our time.

In my eyes your product hasn't been working as you advertise it to and I simply want answers. Answers someone there (when Les Jickling called) stated they would provide some time ago. If I needed data from the laptop in question wiped because a competitor stole our laptop, as it stands your product would fail. If someone stole my laptop and connected it behind a firewall, your product would fail. If someone stole a laptop and stopped the service which anyone can easily do, your product would fail.

On Wednesday 11 January 2006 07:55 pm, you wrote:
> Jesus,
>
> Thanks for your email. We would be glad to speak with you regarding
> your findings. In terms of your conclusions, I believe that we can put
> your mind at ease. However, our technical team has been busy running
> the business - which is why you've not yet had a response.
>
> To that end, please refrain from taking any further action at this time.
> We will get back in touch with you in short order. Please let us know
> how your availability is in the next couple weeks.
>
> I appreciate your patience.
>
> Regards,
>
> ---
> ---
> Rob Chase, CA
> Chief Financial Officer
> ---
> ---
> Absolute Software Corp.
> Keep IT Simple. Keep IT Safe.
>
> tel. (604) 628-5119
> cell. (604) 512-1554
> fax. (604) 730-2621
> toll free 1-800-220-0733
> email: rchase@absolute.com
>
> Suite 800, 111 Dunsmuir Street

> Vancouver, BC Canada, V6B 6A3
> Website: www.absolute.com http://www.absolute.com/

As for failures and concerns, they were never answered. Absolute at one point stated to my then corporate attorney that they didn't even have a record of anyone speaking to myself, or anyone else in the company for that matter. It seemed that there was some form of corporate amnesia concerning this matter.

From Trevor Wiebe Corporate Counsel for Computrace: (former employer is X'd out) only modifications to this email)

Thanks xxxxxx.

Your interpretation of the intent of Mr. Chase's email is incorrect. Let's leave it at that.

I see two separate issues to resolve here. The first has to do with making sure that X has whatever tech support it needs to use our products and services in the manner intended. I was very concerned when I read the specific allegations of non-responsiveness in Mr. Oquendo's latest email (in the thread below). Mr. Oquendo doesn't say exactly to whom his emails or calls were directed, so I had our tech support people check our records. Our tech support has no record whatsoever of incidents logged by Mr. Oquendo or by X since October 1, 2005. Why this is, I simply do not know, and I neither make nor intend to imply any allegations of fabrication, as Mr. Oquendo has done. I think that doing so gets us nowhere fast. All I know is that if X needs on the tech support side are not being addressed, we can start by ensuring that the concerns are addressed to the appropriate personnel.

The contacts for such incidents are: Technical Support at 1-888-999-9857 or e-mail techsupport@absolute.com. If those were the venues Mr. Oquendo tried, and if,for example, he has copies of the emails he sent, please do let us know and we will follow up, for that would be a problem in and of itself. For present purposes, I am cc'ing this email to our Director of Operations, Ms. Risa Zaleski, so that she can ensure that X initial tech support issues are identified and addressed. Since this is what our Technical Support team does each and every day, I do not expect scheduling of that to be an issue whatsoever. I would stress, however, that this may not be the proper forum for a detailed discussion of how an IT security power user with knowledge that the product is installed on their machines can purposefully damage or disarm the software. As mentioned in my prior email, this sort of feedback, while potentially very valuable from a product development perspective, is very likely inappropriate to address from a tech support perspective. To that end, our Technical Support team would be happy to discuss specific tech support issues and we leave it to Mr. Oquendo to decide which of X's support issues he would like us to deal with first.

To ensure that there are no other problems in communication, let me also give you Ms. Zaleski's phone number: 604-676-3653.

The second issue is completely separate and, unless I am missing something, almost certainly non-urgent. This is the question of addressing the plethora of extremely technical comments Mr. Oquendo has made, and of which we became aware only after his first posting on the internet. This is what I would call the "negative product review" issue, as opposed to any specific technical support issues requiring immediate attention. As you can appreciate, the negative product review issues can only be addressed by individuals here with the requisite degree of knowledge and I accordingly involved our CEO, CFO and CTO. Next week I will be away and I think it reasonable therefore to ask for this discussion to be scheduled for the first day the following week when we have me, our CFO and our CTO available. Please let me know your preference of the following slots and I will confirm and provide a dial-in number:

Tuesday, January 24, 2006 3:00 pm PACIFIC (not sure what time zone you are in)

or

Wednesday, January 25, 2006 3:00 pm PACIFIC

Thanks in advance.

Trevor Wiebe
General Counsel and Assistant Corporate Secretary

Absolute Software Corp.
Keep *IT* Simple. Keep *IT* Safe.

tel. (604) 628-5118
cell. (604) 318-7391
fax. (604) 730-2621
toll free 1-800-220-0733
email: twiebe@absolute.com

Suite 800, 111 Dunsmuir Street
Vancouver, BC Canada, V6B 6A3
Website: www.absolute.com

Firstly, I was contacted by Les Jickling of Absolute and made my concerns aware to him since he was calling on behalf of Computrace. If Mr. Jickling did not log my calls then there would be the issue of Absolute not having a record of me complaining. By stating no one there had spoken to me is absurd. Les Jickling is not a common enough name for me to fabricate nor would I be willing to break into my phone company and create records of incoming calls from Absolute.

The response I received from Mr. Jickling made me wonder even more about the validity of their product. According to Mr. Jickling, the reasons for the issues I was seeing was because “they hadn’t intergrated matching their front end with their back end.” Translation? Even though my machine was supposedly sending out data to Absolute, I could not see any updated information because they hadn’t implemented it yet. So how’s that for buying an “absolute” product which was supposed to protect me.

Mr. Jickling then went on to show me how great of a product Absolute’s Computrace was by showing that my computer was on at that moment in time. What Mr. Jickling didn’t know that a) my laptop was completely off and b) was running NetBSD at the time since I had wiped Windows XP. How was this possible? Maybe Absolute hires network magicians who knows.

In essence, here were my concerns that to date – have not been answered and likely are not resolved.

Computrace's "Host" Level Failures

Acme Corp's stolen laptop 10.10.10.1

Acme Corp's stolen laptop needs connectivity to send information out to Absolute's servers. If there is no connectivity, there is no way for Absolute to trace the machine.

Any clueful person can open up the "HOSTS" file in C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS and change Absolute's addresses to go wherever they'd like to send it. Absolute has no failover for this method of bypassing.

If stolen laptop has a firewall running, blocked ICMP's will not notify Absolute of the location of laptop, TCP/HTTP payloads informing Absolute of the status of the machine reach Absolute's network.

If stolen laptop is behind a proxy server, information will not reach Absolute's server.

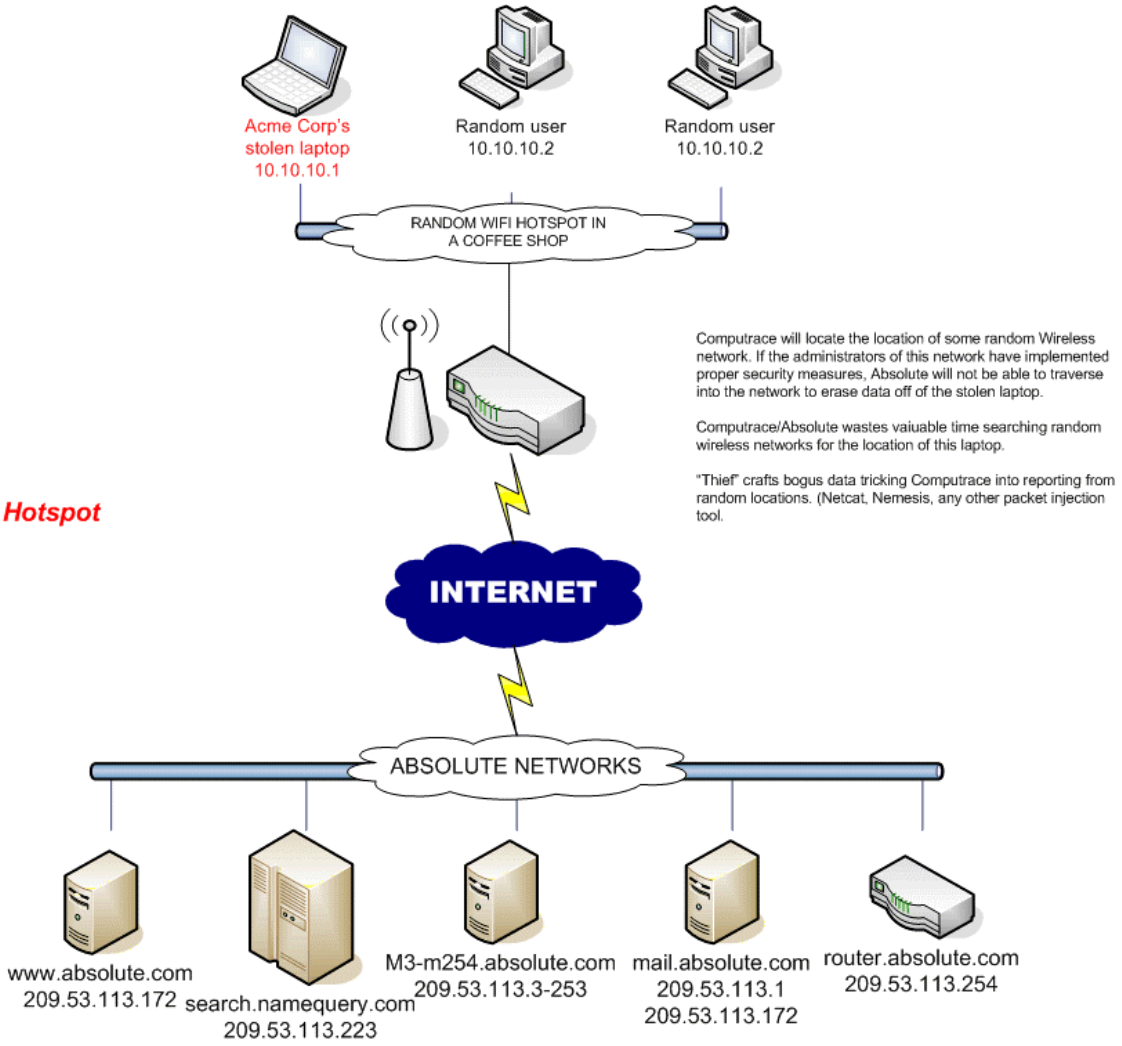
If laptop is behind a username/password based proxy server, Internet Explorer will open asking for a username and password making it known to thief that the stolen laptop is running Computrace and is trying to report its location.

If "thief" is aware of normal processes running on a machine, thief will disable RPCNETP rendering Computrace useless.

If "thief" is savvy, "thief" can "re-construct" bogus information to pass on to Computrace's servers via spoofing (Netcat, Nemesis, etc.)

If "thief" is logging in from an open "hotspot" Absolute will look for the laptop in any random location "thief" logged in from.

Computrace's Hotspot Failures



Computrace has to date to resolve these issues yet I still receive gimmicky alerts. I had originally wanted to pull their card and offer them the opportunity to find my machine and wipe it if they could, but my corporate attorney did not want me to bust their chops. I did ask them for a list of addresses I had logged in from and they first gave me a Department of Defense IP CIDR range to my amusement, they then returned an ISP in New Hampshire's block to more amusement, but they never answered the core problems.

So for the corporations out there looking to solve their woes with this program, I can tell you firsthand it is not all that "Absolute" and it can be defeated easily. If you're trying to protect your information from theft, follow SANS guidelines and have your IT staff get a clue on encryption. Perhaps wait until Absolute gets their act together. Your money waste it as you'd like.