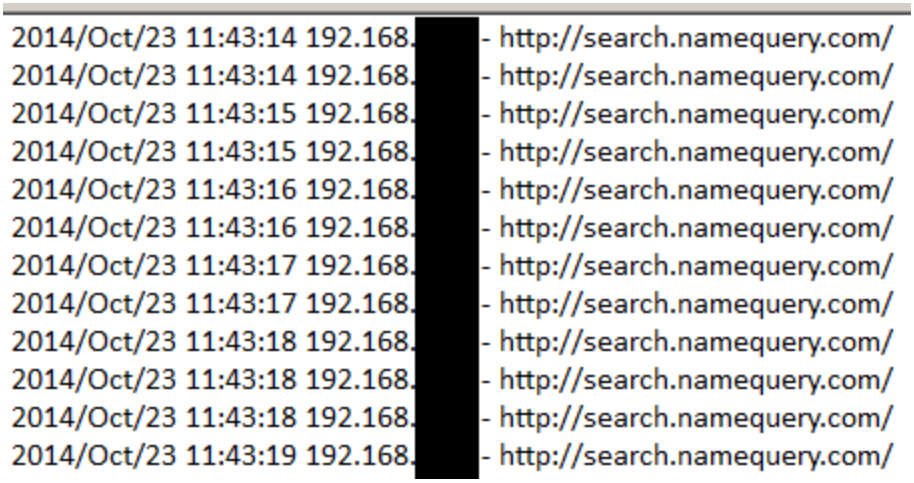
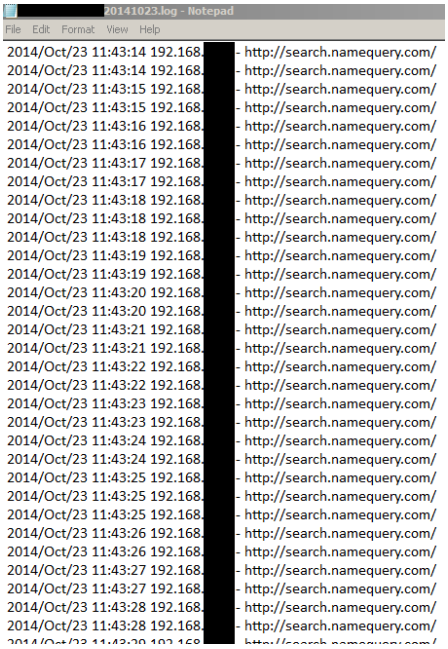
Thoughts on Absolute Computrace

bartblaze.blogspot.de/2014/11/thoughts-on-absolute-computrace.html



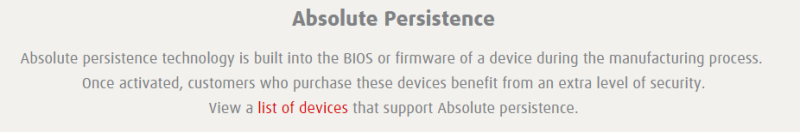
Introduction

Not too long ago my friend and colleague from Sweden, Jimmy, contacted me in regards to a strange issue. In the firewall, he saw tons of outgoing connections to a certain server:



Each second outgoing connection to search.namequery.com

A quick Google search revealed this was actually part of Absolute's Computrace tool - aka Absolute Persistence. Doesn't ring a bell? Try Lojack. From their website:



List of BIOS & firmware compatibility: http://www.absolute.com/en/partners/bios-compatibility

Why would this be an issue? First of all, there has been some excellent research by Anibal Sacco and Alfredo Ortega here: Deactivate the Rootkit, in which they describe attacks on BIOS anti-theft technologies, which Absolute also offers. An excerpt from their paper:

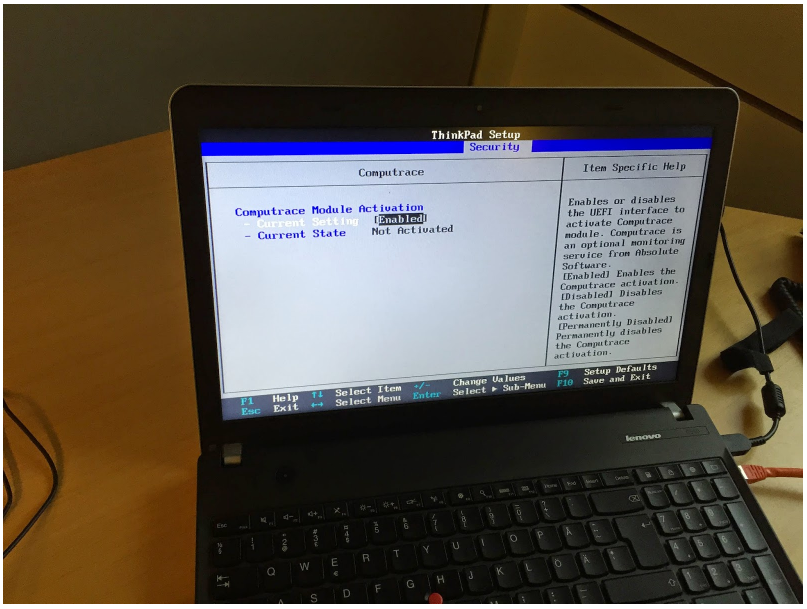
> *In order to be an effective system, the anti-theft agent must be stealthy, must have complete control of the system, and most importantly, must be highly persistent because wiping of the whole system most often occurs in the case of theft.*
> *This activity is also consistent with rootkit behavior, the only difference being that rootkits are generally malicious, while anti-theft technologies act as a form of protection against thieves.*

Secondly, there has been research from Kaspersky as well on the subject, read their blog post here: Absolute Computrace Revisited

I advise you to read their post, as it provides excellent information as well. I'm not going to repeat their research here, as it's pretty extended. What you should remember however:

> *While Absolute Software is a legitimate company and information about Computrace product is available on the company's official website, the owner of the system claimed he had never installed Absolute Computrace and didn't even know the software was present on his computer. It could be assumed that the software was pre-installed by an OEM manufacturer or reseller company, but according to an Absolute Software whitepaper this should be done by users or their IT service. Unless you have a private IT service or your PC vendor took care of you, someone else has full access and control over your computer.*

Back to our post. After booting the machine and pressing F1 to access the BIOS settings, we are presented with the following screen:



Lenovo ThinkPad (BIOS version: J9ET58WW)

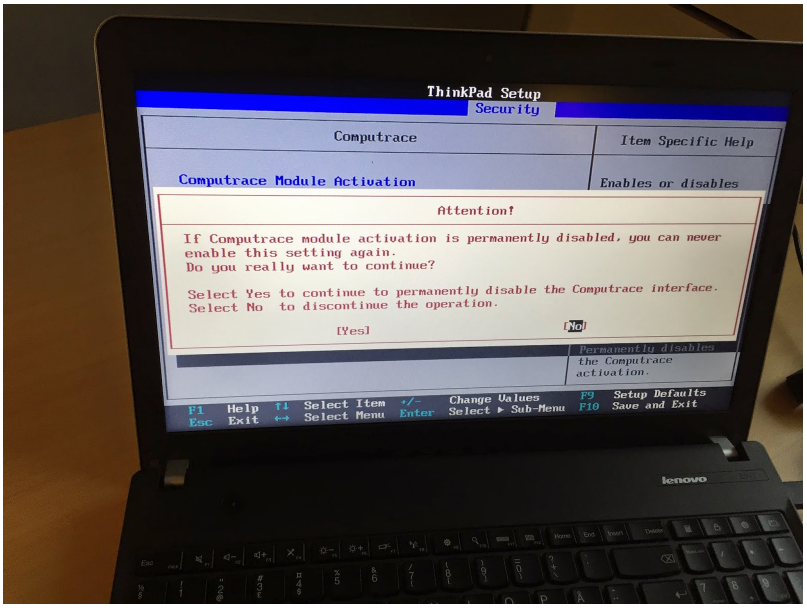
This was the initial state of Computrace in the BIOS. The setting was Enabled and the state indicated Not Activated. This suggests Computrace is not active on the machine... Wrong!

The Item Specific Help reads:

Enables or disables the UEFI interface to activate Computrace module. Computrace is an optional monitoring service from Absolute Software.
[Enabled] Enables the Computrace activation.
[Disabled] Disables the Computrace activation.
[Permanently Disabled] Permanently disables the Computrace activation.

The machine was freshly bought and the user never ordered, installed or even heard of Computrace software. In this case, the reseller didn't install it either. This leaves the option the manufacterer or a possible previous owner [or someone else] installed Computrace.

... When we want to permanently disable Computrace:



Computrace module activation warning

Here comes the fun part: even after permanently disabling the Computrace module, the software was still active and running; contacting the server (*search.namequery.com*) like crazy.

I decided to contact Absolute Software in order to get an answer as to why this behaviour was occurring. Since neither of us are customers, I used the form here to contact them.

After two days I got a reply from their customer service. In reply as to why permanently disabling didn't seem to work:

> It is also worth noting that many used or refurbished devices may have motherboards with a Computrace BIOS module that was activated by the previous owner. In these cases, my recommendation would be the following:
>
> 1. Obtain and install any missing or outdated HECI\Intel Management\IMEI drivers from the manufacturer. Once these drivers are in place, any potential Absolute software installed on the computer will correctly communicate with the BIOS and it should automatically deactivate itself over the course of a few days.
>
> 2. Contact the manufacturer and request a motherboard replacement. Activated motherboards should not be re-sold by manufacturers or retailers if the necessary de-activation steps are not taken first.

Reason for seeing numerous outgoing connections to their server is probably due to their module wanting to receive instructions from the server that the original license should no longer be active, or to download new binaries.

Binaries & BIOS information & characteristics

There's already a good list available by Kaspersky which I'm not going to repeat here. You can find that list on this link.

However, the following points are worth noting:

> Two new binaries (different hashes) have been identified:
> **ad73c636bb2ead416dfa541a74aea016** (wceprv.dll)
> **4011590af6f13a42a869ae57d6174f4f** (rpcnetp.exe)
>
> Several files are packed with UPX

- The wceprv.dll module has a Digital Signature which is issued to *Absolute Software Corp.* Serial Number: **35:ba:ec:87:59:d7:84:62:c3:d2:b7:ff:d4:c4:6e:51**
- Machines will have an altered Master Boot Record (MBR); this is because Computrace parses the MBR and partition table - it writes some data into the sectors before the primary partition. According to the patent (US 20060272020 A1):
  In another embodiment, the CLM is stored in a substitute Master Boot Record (MBR), or a combination of the foregoing.

CLM or Computrace Loader Module is one of Computrace's main modules. (besides the Adaptive Installer Module (AIM) and the Communications Driver Agent (CDA) - see the patent for reference)

How to determine if you have Absolute Computrace installed

First things first: check in the BIOS if there's a mention of Absolute Computrace somewhere: (re)boot your machine and access the BIOS with one of the Function keys on your keyboard.

Typically, this is **F2**, but may differ. See here for a complete list:
BIOS Setup Utility Access Keys for Popular Computer Systems

Secondly, see if any of the files mentioned in Kasperky's blog post are running or exist on the file system. For the full list see here, but keep in mind the two new additional hashes added above.
Note that new hashes may pop-up as well.

Thirdly, network activity as mentioned in above blog post.
(but mainly to *search.namequery.com* or *209.53.113.223*)

How to remove or uninstall Absolute Computrace

I won't provide any specific information on how to remove or uninstall Computrace, as its main purpose is still - and I quote:

> *[...] to perform preemptive and reactive security measures to safeguard a missing, lost, or stolen device and the data it contains. With Computrace Mobile you can determine the location of the device and whether or not it's on the move. You can also freeze it to prevent unauthorized access and send a message to the user to validate the status of the device. If the device contains important information, you can remotely retrieve files or delete them immediately. And you can generate an audit log of the data that's been removed so you can prove compliance with corporate and government regulations.*

However, should you have bought (what you believe is) a new machine and it is apparent Computrace is active, download the latest drivers fit for your system:
Download BIOS drivers Also find information on How to Update Your Computer's BIOS.

When correctly executed and the option for Computrace in the BIOS is set to Permanently Disabled, it should correctly disable itself - **taken into account the original license has expired or the original owner deactivated it**, if existent.

Another option would be to request a motherboard replacement for your machine, as suggested above. Additionally you may reinstall the Operating System afterwards.

Absolute Computrace FAQ

Is Computrace malicious?
No.

Which devices does Computrace support and may be installed on?

- Android 2.3 and later
- BlackBerry® Mobile Versions 4.5 and later
- Internet connection
- Linux: Ubuntu 14.04 and Debian 7
- Mac® OS X 10.6 and later
- Symbian S60 Third Edition and later
- Windows® 7™ (32 & 64-bit versions)
- Windows® 8™ (32 & 64-bit versions)
- Windows® 2000
- Windows Mobile® 5, 6, 6.1, 6.2, and 6.5
- Windows® Server 2003
- Windows® Server 2008
- Windows® Vista™ (32 & 64-bit versions)
- Windows® XP® (32-bit only)

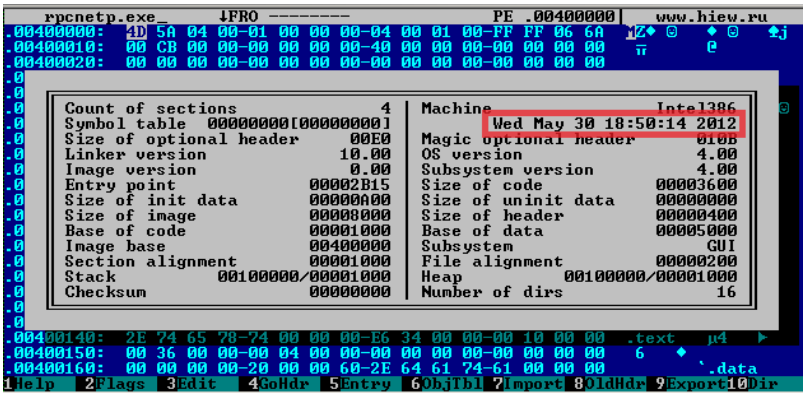
(Source)

So yes, it's possible Computrace is installed on any other of your (mobile) devices. If you're looking for pointers, once again look for outbound connections to *.namequery.com or *.absolute.com.

Which firmware or BIOS brands does Computrace support and may be installed on?

- Acer
- Apple
- ASUS
- Daten
- DELL
- Fujitsu
- GammaTech
- General Dynamics Itronix
- Getac
- HP
- Lenovo
- Microsoft
- Motion
- NEC
- Panasonic
- Samsung
- Sony
- Toshiba
- Winmate
- Xplore Technologies

How recent was the Computrace agent variant you found?
I added this question as to compare it with Kaspersky's binary- which was compiled in June 2012



This variant of the Computrace agent was compiled in May 2012 (assuming it's not altered)

Another version of Computrace was found. Note that this is possibly due to small updates of the loader or agent module.

Will flashing the BIOS remove Computrace?
No, as it resides in a non-flashable portion of the BIOS.

Will downloading the latest BIOS drivers for my machine remove Computrace?
See "How to remove or uninstall Absolute Computrace".

I'd like to see more information about my BIOS/EFI/coreboot/firmware/optionROM.
You can use the excellent tool flashrom. If you are using anything but Windows, Anibal and Alfredo have also written a Python program to to dump the BIOS firmware and search for a CompuTrace Option ROM: dumpComputrace.py (*Note*: you'll need to apt-get flashRom/dmiDecode/UPX)

What if I'm a customer of Computrace and have doubts or want more information?
Best thing to do is call them directly: *+00 1 877 337 0337* (US number), choose option #1. The general number in Europe is: *+44 118 902 2005* and for Asia: *+65 6595 4594*

More information on how to contact them as existing customer can be found here:
Absolute Software Support

What if I'm not a customer of Computrace and have doubts or want more information?
You can still use the numbers above if you like, or you can use the Absolute Software Contact Form.

What if I suspect I bought a stolen machine which has Computrace installed?
Contact Absolute Software (see above)! They will set up a case together with you and law enforcement.

Is there similar software out there like Computrace?
Yes, but it is not exactly the same as Computrace. An example is Prey. Another example is Intel's Anti-Theft Technology - which apparently will cease to exist in January 2015.
Source:
Intel Anti-Theft Service FAQ

Nowadays, most Antivirus vendors also offer some form of anti-theft. For more information, refer to the corresponding websites of the vendors.

Why did you decide to write this blog post?
To provide even more additional & useful information, as well as out of sheer interest.

Do you have any additional information to share?
Yes, see right below in the Resources section.

Resources

Absolute Software - Perspective on Kaspersky Report & FAQ
Absolute Software - Persistent servicing agent (Patent US20060272020 A1)
Corelabs - Deactivate the rootkit (PDF)
Kaspersky - Absolute Computrace Revisited
Kaspersky - Absolute Computrace: Frequently Asked Questions

Acknowledgements

I'd like to thank, in no particular order:

- Anibal Sacco and Alfredo Ortega for their initial research.
- Alfredo Ortega for a refreshing chat and answering some additional doubts I had.
- Vitaliy Kamlyuk and Sergey Belov for their additional/follow-up research.
- Absolute Software's service desk/support specialists for their service & answering any questions I had.

Thank you for reading.