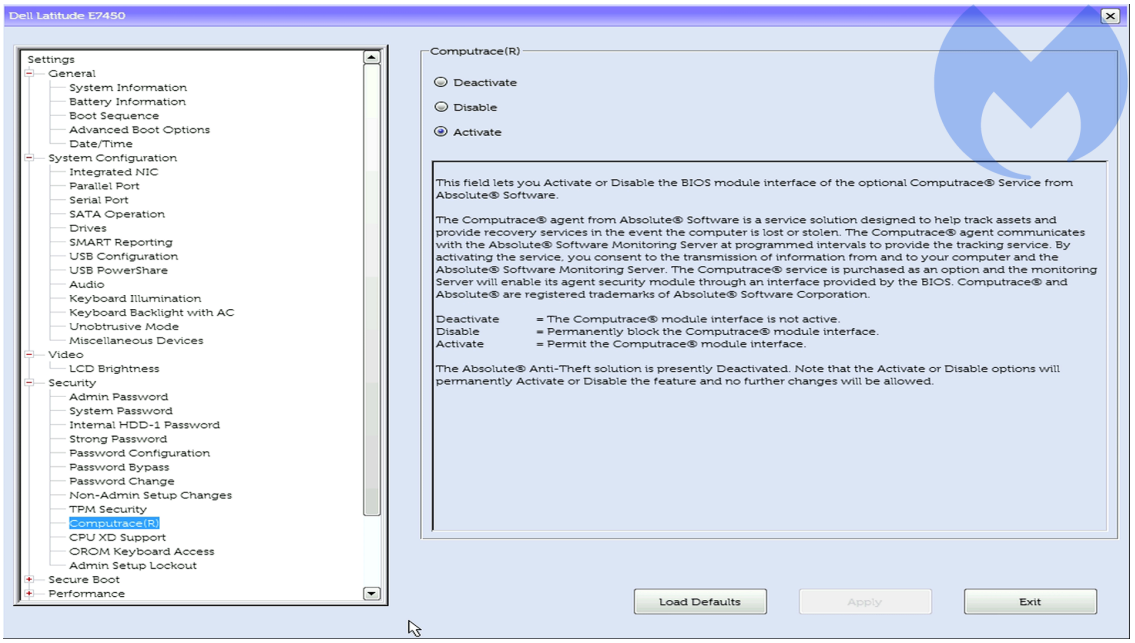
LoJack for computers used to attack European government bodies

By Malwarebytes Labs

Published: 2018-10-03 · Archived: 2026-04-06 00:55:56 UTC

Security researchers have detected the first known instance of a UEFI bootkit being used in targeted campaigns against government entities across Central and Eastern Europe. The attack focuses on UFEI-enabled computers and relies on a persistence mechanism that has been stolen from a legitimate, but often questioned, software called Computrace that comes by default on many computer systems.

This Computrace agent from Absolute Software is a service designed to recover lost or stolen computers, the underlying technology of which is based on the LoJack Stolen Vehicle Recovery System. In 2005, Absolute Software licensed the LoJack name and subsequent tracking technology to aid in recovery efforts of stolen computers. After negotiations with manufacturers, the Computrace agent from Absolute Software—or LoJack for computers—now comes pre-loaded on a large number of machines.



The Computrace software uses a novel method to maintain persistence on computers. This methodology allows the code to remain through a re-installation of the operating system or replacement of the hard drive. The software does this by tightly integrating into low-level operations that are stored within SPI flash memory modules located on the physical motherboard of the computer. These memory modules are where pertinent system resources, such as BIOS and UFEI procedures, are stored.

An Eset white paper details how Trojanized versions of the Computrace agent have been compromised to allow attackers the ability to execute arbitrary code on vulnerable machines. This code can be stored within the SPI flash modules, which prevents easy detection from many security solutions. This code execution ability, along with the

persistence and tracking capabilities of the Computrace software, makes for an extremely effective combination that is difficult to detect or remediate. Eset is calling this threat the LoJax malware.

As of this writing, use of this particular attack methodology appears to be limited in scope. Research indicates that the purpose of this novel attack vector has been to install the XAgent Remote Access Trojan, which others in the security industry have linked to the Russian hacking group that goes by many names including: APT28, Fancy Bear, and Sednit.

The successful execution of the malware payload is dependent upon a computer system that has been configured to disable the Secure Boot protections that come standard on newer Windows computers.

Secure Boot is a security feature of UFEI-enabled computers, and it requires a legitimate digital signature before the system is allowed to execute any code stored within the SPI flash memory module. This is a current limitation of the LoJax malware, as the code does not have a digital signature. This prevents code execution in environments where Secure Boot is enabled, such as Windows 8 and Windows 10.

Users of Linux or other unsupported operating systems will not have the built-in protections of Secure Boot due to incompatibility with those devices. Users who must disable such protections in order to use necessary or desired software will need to remain diligent.

Though currently limited in scope, we anticipate seeing this attack vector employed by other malware families and attackers in the future.
