

LOCKS THAT SECURE LAPTOP COMPUTERS

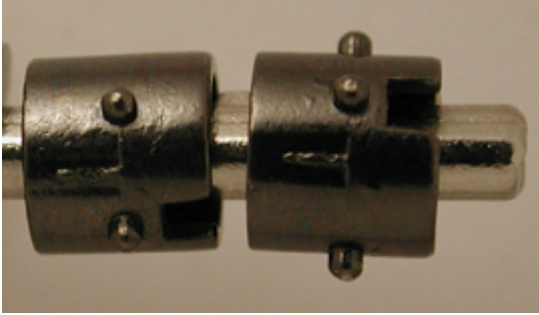
Consumers have relied upon the security of various cable locking devices to protect their laptops from theft. Previous security alerts exposed the ease in which two specific devices could be bypassed. This has resulted in a heightened awareness of the potential for theft by users of these products. An analysis of these devices is deemed relevant because of their widespread use and the mistaken belief by their owners or IT and security professionals that the locks are secure or can prevent theft from non-destructive entry. Any information regarding other known defects in these devices would be appreciated. The author may be contacted directly at mwtobias@security.org.

TARGUS DEFCON[®] CL MODEL PA410U COMBINATION CABLE LOCK



Users of the Targus Defcon CL to secure their notebook computers are at risk of theft. The author does not recommend the use of this device, as it is not secure against a simple method of bypass which can be accomplished within seconds, does not damage the lock, and requires no real expertise. No special materials are required to decode the lock. Time to learn the procedure is minimal. Anyone who is concerned about theft of their laptop from covert means should not use this lock to secure their computer. Further, the combination can be easily changed, once it is decoded, resulting in serious inconvenience or other unforeseen results.

The decoding procedure is possible because of the design of this device. Four individual thumbwheels are utilized to derive the combination. They are linked to rotating disks that each contain a gate, shown in the photograph. Each of these gates must be properly aligned to allow a fence, controlled by the push button, to move through the gates in order to retract the mechanism that engages with the laptop. The two disks are shown with different gate positions. Probing of each disk would provide an indication of the location and alignment of each gate, which would yield the correct combination. The position of the gate for each wheel corresponds to the number of the combination for that wheel. No correction must be made. Thus, the paper or plastic probe is run over each wheel until the gate is found, as shown in the photograph. The identified digit for each wheel is the correct number, although it does not appear in the window where the combination is read. To open the lock, simply move each thumb-wheel so that the number appears in the window.



A piece of plastic, paper, shim, or other thin material may be inserted, as shown, behind each wheel in order to feel the position of each gate. This results from the poor tolerance between the lock body and each thumb wheel. This bypass technique is a well known procedure with other similar types of combination locks. Decoding of the gates takes a few seconds, resulting in the correct combination being derived. In the photograph below, a thin piece of plastic (.003") is used to feel the gate for each wheel. The corner of the plastic is run across each wheel as it is rotated. The plastic or paper will catch in the gate during rotation.

Once decoded, the lock may then be removed from the laptop, or programmed for another code, which would result in a lockout of the owner. The ability to derive the combination and reprogram the lock is clearly worrisome and constitutes a security risk.



All computer owners and administrators should be aware of the potential for theft if you utilize this device.

DISCLAIMER: All versions of this lock have not been tested. Therefore, no representation is made with regard to the security of other like models, or different manufacturing runs of this device. Only one model of this lock was tested. Reader is responsible for determining the security of this product. Security alert is valid as of the date of issue, and may not apply to subsequent models.

COMPUCAGE BENJI 1, BENJI 2, and MODEL L4000

See the video that demonstrates bypass at <http://video.security.org/compucage.wmv>

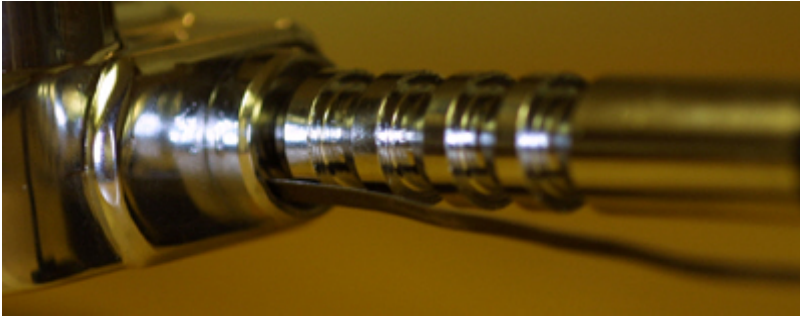


Compucage <http://www.compucage.com> is a Canadian manufacturer that produces a series of products that are designed to physically protect laptops from being stolen by enclosing them in an anchored two-point locking devices. Each of the devices can be fastened to the desk with a screw, or attached by means of a cable. The Benji 1 anchors the laptop diagonally in a closed position, or across the display in an open position, while the Benji 2 locks around the display for open use only. The Model L4000 actually has a closed loop that surrounds the display and connects to a locking mechanism that sits next to the computer and is anchored to the desk.

A sliding cross-member joins the two individual sections and prevents their movement, once locked into place, as shown in the photographs. Three models have been tested, as provided by the manufacturer. Each were found to be easily bypassed. Laptops made by IBM, Apple, Dell and HP were used for the test procedure. Other laptops may not yield the same results, depending upon their size and geometry. The problem with these devices relates to their ability to tightly lock against the laptop, and the clearance between the movable bar and locking dog, allowing the insertion of a shim. If the locking dog were not spring-loaded, these devices could not be opened with a shim, and would be secure.

In all of the tests that we ran, there was enough play to allow the insertion of a shim, which allowed each laptop to be easily removed in seconds. The shim measured .009" x .125".

In practice, the shim is inserted as shown in the photograph, in order to abut against the locking dog. The movable locking bar is compressed slightly as the shim is forced forward. If done properly, it will engage under the locking dog, thus preventing the dog from locking into the grooves of the movable bar. The shim is moved forward so as to cover the entire dog, then the bar can be withdrawn without difficulty.



The company has adopted a unique approach to securing a laptop. However, the design of the ratchet mechanism allows for a very simple form of bypass. Even when the Benji devices are locked tightly against the laptop, they can be easily removed. No specific tests were run against the dimple pin tumbler lock that is utilized in each of these devices, although most of these locks can be picked or impressioned.