GreenTec-USA

FOR IMMEDIATE RELEASE
http://www.GreenTec-USA.com

February 18, 2015
Contact: Bob Waligunda
Tel.: (703) 391-6325 ext.: 2005
Email: BWaligunda@greentec-usa.com

HIGH TECH WORMDISK SOLUTION PREVENTS EQUATION CYBER SPYING ATTACK

Kaspersky Lab warns of “spying” malware in 30 countries

The security company Kaspersky Lab claims to have found what it calls “The Equation Group” virus that infected computers in 30 countries with spying programs that targeted groups including government and military institutions, telecommunication companies, banks, energy companies, nuclear researchers, media, and activists (http://reut.rs/1L5knm0)

According to Kaspersky, the hacker made a technological breakthrough by figuring out how to lodge malicious software in the obscure code on disk drives called firmware that launches every time a computer is turned on. Disk drive firmware is viewed by cybersecurity experts as the second-most valuable real estate on a PC for a hacker, second only to the BIOS code invoked automatically as a computer boots up.

"The hardware will be able to infect the computer over and over," lead Kaspersky researcher Costin Raiu said in an interview. This approach allows the hacker to establish full remote control over any PC the malware is launched in giving them the ability to steal files or eavesdrop on anything they wanted.

In 2013, GreenTec-USA, in cooperation with Seagate Technologies, developed a secure electronic information storage product breakthrough referred to as the WORMdisk™, which cannot be re-flashed, overwritten, reformatted, deleted, or otherwise changed. The WORMdisk™ functions as a normal HDD with zero performance degradation from its additional built-in capabilities.

The WORMdisk™ is the only HDD of its type available that makes it impossible to alter, modify, edit, re-format or delete data on the disk, the master boot sector, **or the on-board technology that controls the disk**, regardless of computer operating system or access permissions.

In short, a hacker attempting to use an attack as described by Kaspersky Lab’s recent claim will not work and cannot effect a company’s important data, launch malware to take control of the PC, delete, modify or impair the master boot record or re-flash the firmware. Additionally, other important files such as log files, access permission and user rights cannot be deleted or modified by hackers.

A devastating attack like the ones directed at these targets is not the only problem facing companies today. Attacks by hackers or from malicious employees may cause an even greater loss by making small changes, for example, to corporate records, access rights, or financial accounts which may go undetected for a long period of time. Case in point: **“Large financial corporations’ losses amount to billions of dollars by insiders directing automated payments to offshore bank accounts”**. With WORMdisk™ this unauthorized change would not be possible.

Use of the WORMdisk™ is easy and intuitive since it installs and operates like a standard HDD.

The WORMdisk™ is also the only storage device of its type to allow full encryption to provide an additional level of protection to company's data.

If you would like more information about this topic, or to schedule an interview with GreenTec-USA, please contact Bob Waligunda at (703) 391-6325, ext.: 2005 or email: bwaligunda@greentec-usa.com