Samsung R540S Laptops Clean:
No Keyloggers or Spyware of Any Kind Found

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Peter R. Stephenson, PhD, CISSP, CISM, FICAF is Director of the Norwich University Center for Advanced Computing and Digital Forensics and Chief Information Security Officer. The following report is entirely his own work with minor edits.

* * *

Dr Kabay requested that the Norwich University center for Advanced Computing and Digital Forensics perform a complete, unbiased investigation of the events leading up to the publication of the allegation that some Samsung computers contained a keylogger called StarLogger. I agreed to do that under the condition that Dr Kabay and Samsung not be part of the investigation. In my view it is necessary to separate the facts of the issue so that they may be analyzed critically using appropriate technology. Both agreed with minor exceptions that I will note in this report.

Before I start, it is important that readers understand why the Center in general and I in particular am qualified to conduct this investigation. The Center has, as its mandate, the responsibility for research and support for several advanced computing technologies including digital forensics and investigations. Our tools are best of breed commercial tools, our environment is controlled strictly and our security is maintained to avoid contamination. We conduct digital investigations routinely for Norwich University and such entities as the state of Vermont. My own background of nearly 50 years includes a PhD in digital investigation the designations CISSP, CISM and FICAF as well as decades of experience.

Samsung purchased two laptops from a retail location in New Jersey and flew them to Norwich University. They then conveyed the laptops personally where Dr Kabay received them and standard chain of custody procedures were followed. He confirmed that the manufacturer's security seal was still in place, added our own security seal over the factory seals without opening the sealed packages, logged the two computers by serial number into our system (which involves getting a chain of custody form signed) and locked the computers in our evidence locker. We retained the store's sales slip that showed the two purchased computers by serial number.

When I returned to campus that evening after off-campus travel I confirmed that the security seals were still intact (we use a special tape that is nearly impossible to remove without visibly damaging the tape) and opened the first box. I recorded on a digital voice recorder the entire process of opening the box, removing the hard drive and taking forensic images using FTK Imager, current version, and appropriate write blocking. I locked the door to my forensic lab and left the program to complete. When it finished I performed the same task with the other computer. I then processed both images using FTK 3.2. The images are raw (dd) images, uncompressed. In neither case was the Samsung computer ever powered on.

Upon completing the case processing I checked both disk images – now processed into a single case file – for the presence of the files that make up the StarLogger distribution (the forensic tool

can see inside cab and other archive files) as well as the presence of the default installation directory. None were present.

I then ran the most current release of Wetstone Technologies Gargoyle against both disks. I used the March dataset, which should be adequate since the laptops were manufactured well prior to March. Gargoyle particularly looks for malware including, specifically, keyloggers. There are two versions of StarLogger explicitly part of the dataset that I used.

I then created a hash set that consisted of some 8,400-plus hashes of keyloggers and spyware using the NSRL hash set included with Gargoyle. Using FTK I imported the hash set and ran the entire set against the two images from the Samsung computers. The results were that there were no keyloggers or spyware found on the Samsung laptops.

Throughout this process there was no participation or lab access by either Dr Kabay or Samsung. There was no evidence of the presence of StarLogger or any other keylogger or spyware on either computer. From that I concluded that StarLogger was not installed or ready to be installed on either computer.

Therefore, I conclude that the two Samsung R540 laptops are free from spyware and keyloggers and that the reported presence of StarLogger was a false alarm.

* * *

Peter Stephenson is a writer, consultant, researcher and lecturer in information assurance and incident investigation on large-scale computer networks with over 40 years experience in various technology fields. He earned his PhD at Oxford Brookes University in the UK and holds an MA in diplomacy from Norwich University with a concentration in terrorism. Dr. Stephenson has lectured in 11 countries plus the United States and has written or contributed to 16 books and several hundred articles in major national and international trade publications and technical/scientific journals for the past 25 years. He is the technology editor for *SC Magazine*. Currently, he is Director of the Norwich University Advanced Computing Center at Norwich University where he is also the Chief Information Security Officer and an instructor in digital forensics and network-centric warfare. Dr Stephenson's current research is on cyber attack attribution, and cyber profiling. He currently is working on a book on information assurance analytics, due to be published in 2011 and the second edition of his book on computer related crime investigation, also due out in 2011.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Associate Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >