A Virus Of Biblical Distortions

John BumgarnerCommentary

Taking a second look at the Stuxnet 'myrtus' text string

Special To Dark Reading

John Bumgarner is the Chief Technology Officer for the U.S. Cyber Consequences Unit. He has served as an expert source for various publications, including Business Week, BBC, CNN, Jane's Defence, The Economist, The Wall Street Journal, and The Guardian in London.

In the summer of 2010, security researchers serendipitously discovered Stuxnet, a highly sophisticated cyberweapon deeply embedded within Iranian computers. The weapon's main function was to attack the gas centrifuges used by the Iranians for uranium enrichment, believed to be part of an effort to build nuclear weapons in defiance of a resolution by the United Nations Security Council.

Within weeks, the cyberattacks against Iran's nuclear facilities became a classic detective story. As the investigations progressed, The New York Times suggested that Stuxnet's source code contained Biblical references, as in the text string "b:\myrtus\src\objfre_w2k_x86\i386\guava.pdb." The New York Times speculated that the word myrtus referred to the Book of Esther, which appears in both the Jewish Tanakh (the Hebrew Bible) and in the Old Testament of the Bible. The idea was that Stuxnet's authors were using this reference to send the Iranians a message.

A Jewish girl, Esther ultimately became the queen of Persia and saved her fellow Jews from annihilation by the Persians. Esther's Hebrew name, Hadassah, refers to myrtle, a healing plant with the scientific name myrtus communis. In ancient times the plant was considered to have divine powers and was used by Israelites in religious ceremonies. The Israelites also associated myrtle with acts of generosity, love, peace, and justice.

Ralph Langner, a German computer security expert who is credited with deciphering the Stuxnet targeting code, proposed the Biblical interpretation of myrtus within the Stuxnet text string. When asked about its significance, Langner said, "If you read the Bible, you can make a guess." The New York Times supported Langner's analysis with comments from an Old Testament scholar, confirming the connection between myrtle and Hadassah, or Queen Esther. This scholar concluded that "someone was making a learned cross-linguistics wordplay."

The New York Times further noted that the word guava appeared in the same text string as myrtus. In botany, the Myrtus family contains two subfamilies, Leptospermoideae and Myrtoideae. The Myrtoideae subfamily

includes numerous species of guava.

According to The New York Times, some security experts interpreted the allusion to Esther as a clear warning by Israel to Iran. Other prominent news outlets, including The Guardian, The Huffington Post, and The Christian Science Monitor, have further propagated the idea that Stuxnet contains Biblical and botanical references. The Christian Science Monitor suggested that the myrtus reference could reveal Stuxnet's author in a "Da Vinci Code-esque fashion." Others have argued that the myrtus reference is a red herring intentionally inserted by Stuxnet's authors to misdirect researchers toward Israel.

In late 2010, F-Secure, a Finnish antivirus company, suggested that the RTU portion of myrtus could actually be an abbreviation for Remote Terminal Units, which is an electronic device containing a microprocessor that is used for remotely monitoring or controlling industrial equipment. RTUs are designed to operate in a wide range of contexts, including air traffic control systems, nuclear power facilities, offshore drilling platforms, space shuttles, and other critical systems. They are usually a component of larger supervisory control and data acquisition systems (SCADA), which are used to control industrial operations. Stuxnet specifically targeted devices called programmable logic controllers (PLCs) that were built by Siemens. PLCs are sometimes described informally as a variety of RTU if they use a regular programming language rather than a more specialized PLC "ladder logic," and PLCs are sometimes managed with the aid of RTUs. The Siemens PLCs attacked by Stuxnet were a type of RTU. Within the context of Stuxnet, the idea that myrtus refers to industrial control systems seems far more likely than the idea that it refers to the Hebrew Bible.

This argument is strengthened by applying standard forensic and software design principles to the rest of the Stuxnet string "b:\myrtus \src\objfre_w2k_x86\i386\guava.pdb". When I applied these principles, a number of interesting points emerged.

The first part of the string is the drive letter used by the authors of Stuxnet to store the project files for their cyberweapon. Drive letters are normally assigned based on drive type. For instance, the drive letter commonly assigned to the default hard drive on a computer running Microsoft Windows is "C." The specific drive letter in Stuxnet's case is "B." Drives with the assignment of "B" are usually reserved for a second floppy drive, if present, but can also be used as a "virtual" floppy drive mapped onto the physical drive. Based on the drive letter and the sensitivity of the Stuxnet project, it appears that the developers likely locked the weapon's source code in a safe at the end of the workday.

The next part of the string is myrtus, which was a directory used by Stuxnet's authors to store the source code for specific modules used in the cyberweapon. The next two parts of the string are src and objfre_w2k_x86, which are common names for subdirectories. The abbreviation src stands for source or the more common vernacular source code. The

objfre_w2k_x86 segment of the string was created by the Microsoft development tool (Microsoft Windows Driver Kit) , which was used to write portions of the source code for Stuxnet. Objfre is related to the x86 Free Build Environment of this development tool. The W2K portion of the string is commonly used to reference computers running Microsoft Windows 2000 operating systems. The term x86 is the common reference for the family of programming instructions originally developed for central processing units (CPU) manufactured by Intel. The i386 reference in the string is the common nomenclature used for 32-bit microprocessors manufactured by Intel.

The .pdb file extension is an abbreviation for program database, which is a proprietary file format development by Microsoft. PDB files are used to store information related to an individual module of a specific software component under development. The WDK development tool automatically generates a PDB file when debugging has been selected by the developer. These PDB files are stored in the local directory, which in Stuxnet's case was b:\myrtus\src\objfre_w2k_x86\i386\. Internal references to PDB files are not commonly included in production code. By accident, Stuxnet's authors left the program database reference in a customized driver file named MRxNet.sys. Drivers are used by a computer program to control or operate a specific device attached to a computer. For example, a printer commonly requires particular driver files to be installed on computer prior to its initial use. Writing device drivers requires an in-depth knowledge of specific functionality between interconnected hardware and software components.

Finally, with regard to guava, others have previously speculated that this reference is related to botany, but my research suggests otherwise. I believe that in this context guava refers to a piece of scientific equipment, known as a flow cytometer, from a specific manufacturer. Flow cytometry is a technique used in various fields, such as biology, chemistry, ecology, and medicine, for counting and examining microscopic particles.

Flow cytometry can also be applied in the development of nuclear weapons. Industry-specific methodology shows that a flow cytometer can be used to accurately measure uranium isotopes. Based on this methodology, I theorize that Iranian scientists working at the Natanz Fuel Enrichment Plant used flow cytometry to gauge their effectiveness in separating uranium 238 and uranium 235 isotopes. An extremely high concentration of the latter is required to achieve the necessary explosive yield for a nuclear weapon. Stuxnet needed to manipulate the flow cytometer and associated components without being detected by the human operators. This manipulation probably included falsifying analysis readings and suppressing threshold alarms that were supposed to be transmitted to control software within the Natanz facility.

Stuxnet, according to my analysis, was programmed to manipulate the flow cytometer manufactured by California-based Guava Technologies. Millipore Corp. acquired Guava Technologies in 2009. The following year, German-based Merck, which specializes in chemicals and pharmaceuticals,

acquired Millipore. The company produces a flow cytometer called the Guava EasyCyte Plus, which can be configured for fully automated data acquisition. Automation can be achieved using robotics systems, such as the PlateCrane (robot arm) manufactured by Hudson Robotics. In addition, flow cytometers can be integrated with various industrial control systems including Siemens' PLCs.

The U.S. Department of Commerce requires that flow cytometers being exported to Iran be registered in accordance with Trade Sanctions Reform and Export Enhancement Act of 2000. It is unclear how Iran acquired the flow cytometer manufactured by Guava Technologies. What is clear is that the authors of Stuxnet not only had a deep technical understanding of how industrial control systems work, but also how connected components, such as the gas centrifuges, flow cytometers and coolant towers are engineered and how they function.

To achieve these levels of expertise, the authors of Stuxnet had to have substantial financial resources to employ top-notch technical people and to operate an advanced research facility. This research facility needed to possess examples of the industrial devices used by the Iranians, or to be able to model them with software, or both.

The technical challenges in the development of Stuxnet would have absorbed all the energy and attention of its creators. There is no reason to believe that the labels remaining in the final program served anything other than a utilitarian purpose. Stuxnet caused Iran's uranium centrifuges to break down, over and over again, for several months. By the time Stuxnet was discovered, its message could not have been clearer: the opponents of Iran's nuclear program were willing to employ impressive technology to stop it. There was no need for obscure Biblical hints, buried in the program's many lines of code.

John Bumgarner is Chief Technology Officer for the U.S. Cyber Consequences Unit, an independent, non-profit research organization that investigates the strategic and economic consequences of possible cyber attacks. He has work experience in information security, intelligence, ...
View Full Bio

More Insights