

TECH TIDBITS, vol. 20

Software Viruses on your Rig?

During a recent rig survey, WEST's Systems and Controls surveyors identified multiple software virus threats with varying potential impacts on the bridge and other critical integrated systems. A closer look identified the root cause in several instances. Anomalies were found in the fire and gas, ballast control, blowout prevention, mud, vessel management, vertical connection (VCS) and dynamic positioning (DP) systems.

Various attempts were made to remove the threats. However, several of the viruses continued to reappear. To find the source of these viruses, the configuration of the rig networks was reviewed. Given the existing network configuration, several potential paths for virus propagation were found. Other unaddressed network nodes were also identified.

Description of Issue

WEST's Systems and Controls team has found multiple viruses and other software issues on virtually every rig that has been surveyed. In the case described above, all computers and systems were scanned and a number of threats found. Just for the sake of example, some of these viruses are listed below:

- ***INF: AutoRun-gen3**
- ***INF: AutoRun-AA**
- ***Win32: MalOb-BZ**
- ***Win32: Rimecud-B**
- **Decompression Bomb or zip.bomb**
- **Trojan Horse Generic13.ZIN**
- **Trojan Horse Downloader.Agent2.BWY**

*** Viruses found on both the DP and VCS automation machines:**

Once a virus infiltrates your security, it can quickly infect your system; destroying files, corrupting data, rendering applications useless, and generally leading to expensive NPT (non-productive time). WEST has seen several cases of this kind of damage, ultimately affecting systems such as the DP, BOP controls and acoustic systems. Systems have been seen to reboot without warning, to lose communication with other systems, to lose the ability to failover, or even to not start up at all. More stories like this are appearing daily.

The recent Stuxnet virus has raised the stakes with its potential to take control of a system and actually operate controls without human assistance. While this particular virus was deliberately aimed at a very specific target or targets, experts say that a variant of this virus has already been backwards engineered and released to attack more common targets. Though little in the way of direct evidence has appeared yet, several industry OEMs have released bulletins outlining any known threats to their systems from the original Stuxnet virus. The impact of the new variant is as yet unknown, but it could potentially be catastrophic.

Some viruses are able to move through networks from one system to another without human intervention. Today's advanced generation rigs have a number of integrated control systems that 'talk' to each other via the rig networks. Many rigs are also linked to shore-based networks that make them vulnerable to viruses on these networks. Because of all this, it is possible and even likely that a virus that entered your rig from a single point has spread itself to other systems on your rig. Some viruses are also capable of carrying payloads of multiple threats that will work together when released.

Viruses can enter your rig from any number of sources. Some of the common paths of infection include email, internet connections, downloaded software, personal or corporate laptops, thumbdrives, and other systems connected via a network. Even backups can be suspect if the virus infected the system before the backup was made. In addition to these, WEST has also confirmed viruses on commercial CDs shipped directly from OEM vendors. There is even evidence that these threats have migrated to other OEM products across a network.

Solutions

If any one of your systems has been compromised, WEST strongly recommends a methodical, risk-managed approach. Simply running anti-virus software at this point can actually complicate the recovery. It may remove the obvious threats, but it won't reveal the damage that was done, or the other connected systems that now need to be checked for infection. WEST recommends that the system be disconnected, cleaned and all existing software and data restored to original condition before continuing work. You should contact WEST's Systems and Controls group or another expert for guidance.

WEST has put together several documents with more specific information about viruses, their effects, and how to deal with them. For a copy of these, you can contact Michael Van Gemert of WEST Engineering Services at michael.vangemert@westengineer.com, or call 281-375-5515.

WEST's System and Controls team is available to work with your technical teams, OEM's, the shipyard, etc. to scan for and detect a virus. They will then coordinate with the appropriate OEMs to create a procedure to quickly remove the virus and restore your systems. WEST will also recommend a process for keeping your systems virus free. If desired, we will perform a forensic analysis of all the threats to help reduce improper security practices onboard rigs.

Other planning, procedural and risk assessment services are available to help you create and maintain a secure rig environment. These procedures cover areas such as permissions, controls, access requirements, shared networks, storage access, backup/restore, auditing and documentation.

Prevention is always the best policy. A secure system and procedures will minimize vulnerable entry points and the risk of damage. If a virus has penetrated your security, consider changing or enhancing your current security practices, e.g., are you currently using updated anti-virus software to scan your systems and connected devices **before** they have a chance to infect your rig?

For more information or technical questions, please contact Michael Van Gemert of WEST Engineering Services at michael.vangemert@westengineer.com, or call 281-375-5515. You can also visit our website at www.westengineer.com.