

# THROUGH THE LOOKING GLASS

When it comes to threat migration, the lessons that we draw from the biological and technology worlds are very similar

**A VIRUS IS ONE OF THOSE THINGS WHOSE IMPACT TO** the human race ebbs and flows; its relevance to our daily lives is largely cyclical and this relevance is dependent on our ability to beat the threat into submission and contain its spread through technology.



**BY JASON LEUNG,  
SENIOR PRODUCT LINE  
MANAGER FOR SMB  
SECURITY, NETGEAR**

Am I writing about the 2009 H1N1 swine flu that's currently circulating the globe? Or am I talking about computer viruses?

I'm writing about computer viruses, but we can draw three important parallels between viruses of the biological sort and viruses of the computational sort:

## ➤ CONTAINMENT, NOT ERADICATION

Just like biological viruses, we can inoculate ourselves (use desktop AV), but viruses are adaptable. Viruses will mutate (whether by biological selection or by hacker design) and viruses will find some way to survive. The best that we can hope to do is to contain viruses — and be ever-vigilant that the threat is always just simmering underneath the surface.

**“VIRUSES WILL MUTATE (WHETHER BY BIOLOGICAL SELECTION OR BY HACKER DESIGN) AND VIRUSES WILL FIND SOME WAY TO SURVIVE. THE BEST THAT WE CAN HOPE TO DO IS TO CONTAIN VIRUSES — AND BE EVER-VIGILANT THAT THE THREAT IS ALWAYS JUST SIMMERING UNDERNEATH THE SURFACE.”**

In the biological world, Severe Acute Respiratory Syndrome, which was caused by the SARS coronavirus (SARS-CoV), was largely contained to bats until the virus mutated and made the jump from bats to humans in the spring of 2003. The result: 8,096 victims in 37 countries, with 774 deaths. Subsequent efforts to contain the virus through quarantine and the use of retroviral drugs have largely contained the spread of SARS-CoV in humans, but the virus continues to mutate in the wild: no one knows when SARS will hit us next.

## ➤ COLLATERAL DAMAGE

Every good intention will almost always have an unintended side effect. In 1976, swine influenza A-H1N1 caused severe concern among the American population as it suddenly sickened 13 people and killed one at the Fort Dix U.S. Army base. To stave off a major pandemic, President Gerald Ford rapidly introduced a program to inoculate all U.S. citizens. Unfortunately, this vaccination program had unintended consequences — it sickened 500 people with Guillain-Barré syndrome and caused the deaths of another 25.

Similarly, desktop antivirus software almost always has unintended consequences — performance slowdowns, hyperactive false-positives, application incompatibilities, and general system malaise are all common side effects of using desktop antivirus software.

## ➤ A LAYERED DEFENSE

The best way to protect yourself from a global flu outbreak is to utilize a multi-pronged approach to limit your risk exposure. Wash your hands. Don't touch your nose and mouth. Limit contact with others if you suspect that you are sick.

Similarly, in the technology world, it best to employ a multi-layered defense strategy:

- Use desktop antivirus software — and keep these packages up to date!
- Employ gateway antivirus systems to prevent users from drive-by-downloads or downloading malicious files — because desktop antivirus software will miss threats.
- Limit exposure by using URL content filtering systems to prevent users from visiting malicious websites in the first place.
- Employ anti-spam systems to prevent your users from being the target of phishing attacks.
- Utilize effective email security systems that scrub all incoming emails of malicious files.

In short, when it comes to threat mitigation and containment, the lessons that we can draw from the biological world and the technology world are very similar. Be safe, my friends. ■

*Jason Leung has led product management, marketing, support and IT consulting activities for more than a decade. He currently manages NETGEAR's channel and SMB relationships for all security infrastructure.*