



Doomsday: Virus Story
infectionvectors.com
October 2005

Overview

In 1996 a virus emerged that immediately grabbed the interest of researchers. The threat was compared to an earlier pandemic which wiped out thousands of hosts over the course of a year. Over the years, the threat continued to grow, albeit at a very slow pace. In 2005, the possibility that this virus would explode and become one of the most powerful threats in history ignited media attention and public fear. From this fear came an outcry for bolstering the response efforts at every level: government, private industry, and individual. It is presumed that the defense and remediation plans for this threat are under funded and do not have the requisite sponsorship of research groups.

Fear is considered the enemy of those charged with the security of any system, whether it is a small network or a large group of people. Fear, uncertainty, and doubt (FUD) is decried as a force that ruins good defense efforts; FUD places emphasis on the wrong areas, wasting money and stirring up panic when it isn't justified. Unfortunately, fear is often the only catalyst for change in stagnant, under evaluated defense plans. The criticism revolving around the scenario above, which briefly outlines the avian flu (H5N1) concerns, is probably suited to many information assurance (IA) programs as well: knowledge that threats exist (even very specific ones), knowledge that programs are not strong enough to effectively combat attacks, and a lack of internal/external collaboration to build a strategy. This paper examines the correlation between preparation and perception with regards to biological outbreaks and digital outbreaks.⁰

Fear and Loathing

There is rarely a casual threat of worldwide viral pandemic. When they reach the media, the tone is generally grave. Consider the following first and last sentences from an editorial in the "Bangkok Post,"

"All of a sudden the world seems to have awakened to the doomsday prospect of a killer pandemic influenza sweeping the globe and killing people by the millions, like the Spanish flu back in 1918-19 which killed about 50 million people worldwide...the world must unite and work together to meet the deadly challenge posed by a possible pandemic influenza. No single country can win this war no matter how well equipped it is in its control of the disease and in its preparations to confront the potential pandemic."¹

That's a fairly tough call to arms for the health professionals and governments of the world.

A similar call to or from the computer security community would likely not have the same strength. Hoaxes have strained many analysts' patience when considering the widespread distribution of worm warnings. In reality, there is no reason to take a worm as seriously as a deadly strain of influenza; the threat is simply not the same. Previous bouts with both viruses of both biological and digital composition prove this. Even cyber threats like Slammer, MyDoom, and Blaster have not been tied to a loss of life. However, they were expensive disasters nonetheless.

Impending

Catastrophes of all natures produce lessons that one can take into another arena. For example, after hurricane Katrina and the ensuing relief efforts, the United States government began revising disaster plans. Katrina itself helped to put large scale relief in perspective, and conversely, put future problems in perspective. For example, when discussing the possibility of a nationwide influenza outbreak, many analysts pointed to the scale of hurricane efforts and what would be required by contrast.² The same can be said (on an admittedly less life threatening scale) for Internet-based threats. The likelihood of another Blaster, Slammer, Sasser, or Zotob is high, and those previous outbreaks can help benchmark existing response plans.

With a survey of the "bird flu" press reports, one can gather a high level look of the processes required for dealing with impending threats. The first is some type of threat prognostication system. For H5N1, very informed, trained health professionals have been watching the virus since its initial detection. Most organizations will not have a person on staff to serve as the cyber counterpart to this role. However, they will have support from external security companies: antivirus vendor, monitoring service, or research/analysis firm. These sources will (or should) provide a look at emerging threats, tailored to the client company.

The plan is fleshed out with the following pieces:

Surveillance

Repeatedly noted in the health-related articles is the monitoring and notification system used to track pandemics. Whether or not such a system is organized and functional with regards to H5N1 will be seen. Early warnings for the Internet are overwhelmingly Internet-based. This certainly poses a problem when the system under attack is expected to successfully alert its administrators. Service desks, live support, and news from other networks (via security portals) are invaluable resources to IA departments.

Containment

Once infected hosts are detected and the spread of the threat is tracked, there must be a mechanism in place to slow/prevent the spread. In terms of the flu, the current actions have included quarantining and destroying infected birds. In the digital world, machines

may be taken offline, entire networks disconnected, or new filtering rules may be applied to the perimeter devices.

Remediation

Systems that are taken offline must be officially diagnosed and cleaned, where required. Most systems have some type of anti-malware software, capable of detecting and cleaning the majority of worms that exist, when functioning properly. For emerging threats, their repair capabilities need to be tested.

Tamiflu is currently cited as the treatment of choice for H5N1. It's undoubtedly a remediation tool, but its functions go beyond that. Not only does the drug help someone overcome the illness, it prevents the virus from spreading to another person. For the technically minded:

"Tamiflu inhibits the protein neuraminidase, which enables the virus to spread to other cells...if the virus can't escape from its host cell, it can't spread to other people."³

The digital equivalent (in theory) works the same way. Perimeter devices should work the same way: stopping outgoing worm traffic before compromised hosts can infect other Internet-connected machines.

The piece of the puzzle that remains is education. The professional/layman community will always struggle with how much impact education can affect the outcome of an attack. Numerous programs have emerged for the avian flu threat, targeting high-risk groups and the general population alike, with signs that they have been effective at stemming rampant infections at this point.⁴ Similar programs are provided by employers in a limited fashion. Corporations often offer specific awareness programs to customers as required (such as banks that host anti-phishing pages).

Sickened

Once a virus reaches the pandemic level the outcome is never good. The same is true for worms on the Internet. The expense involved in cleaning up a widespread piece of malware is great, sometimes too great for companies to overcome. Digital threats used to destroy targets with more regularity than modern worms. The need to keep hosts "alive" is built upon the desire to make a profit from the infected system, as well as propagate the malware. Within the H5N1 literature is what appears to be an interesting equivalent idea:

"If we were to have a pandemic of H5N1, it would be bad for two or three years...eventually, the population gains immunity. And the virus probably changes itself to become less dangerous and circulate in humans from year to year."⁵

On the Internet, worms peak and die as they are cleaned from hosts, added to antivirus definition updates, and systems are patched. Certain threats seem to hand around well

after conventional wisdom would dictate they should (see Netsky.P's story for an example).

In either case, waiting out a threat's lifecycle is not going to be "Plan A" for any commercial organization. There will be a detection, containment, and remediation strategy, hopefully involving multiple groups inside the company. Not many people would care about planning for an avian flu outbreak in Europe or the United States without experts calling out the possibility of thousands or millions of deaths. Fear, unfortunately is the motivator in many case for these plans. That should not prevent the plans from being formulated (as any reason that brings the commitment and resources to the table should be embraced), but it should be recognized when the emergency plans are established.

References

0. Information regarding the “evolution” of biological versus digital viruses can be found in an earlier [infectionvectors.com](http://www.infectionvectors.com) story:

http://www.infectionvectors.com/library/violution_iv.pdf.

1. Bangkok Post. “On guard against deadly challenge.” Editorial, October 12, 2005.

http://www.bangkokpost.com/News/12Oct2005_news17.php

2. Sternberg, Steven. “‘We’re not ready’ for bird flu; US toll could dwarf Katrina’s.” Tennessean, October 11, 2005.

<http://www.tennessean.com/apps/pbcs.dll/article?AID=/20051011/NEWS07/510110356/1024/NEWS>

3. Lisa Jones, “Big trouble.” NY Daily News, October 12, 2005.

<http://www.nydailynews.com/front/story/354906p-302413c.html>.

"Tamiflu inhibits the protein neuraminidase, which enables the virus to spread to other cells," he says. "If the virus can't escape from its host cell, it can't spread to other people."

4. Sonja J. Olsen, et al. CDC, Emerging Infectious Disease. “Poultry-handling Practices during Influenza Outbreak.” Volume 11, Number 10, October 2005.

<http://www.cdc.gov/ncidod/EID/vol11no10/04-1267.htm>.

5. Lisa Jones, “Big trouble.” NY Daily News, October 12, 2005.

<http://www.nydailynews.com/front/story/354906p-302413c.html> Quote from Dr. Scott

Harper, medical officer with the flu team of the Centers for Disease Control and Prevention's National Center for Infectious

Netsky.P information, as referenced in the column, can be found at:

http://www.infectionvectors.com/library/netsky_anniversary_iv.pdf.