CASE STUDY

Following the Breadcrumbs

Christine M Orshesky
i-secure corporation, USA

Many people and organizations are still puzzled about where viruses come from and how they get into their systems. Traditional wisdom about not opening suspicious messages from unknown individuals seems to have given the impression that viruses come from strangers – either those who unknowingly forward them or those who actually want to do harm.

Is it really the strangers that bring or send the viruses and other suspicious things into your organization or is it your trusted employees, co-workers, and professional acquaintances? This has to be a key question when trying to determine effective ways to protect your organization and its resources.

One such organization, *Anycompany.com*, decided to find out how and where the viruses in their organization were being obtained so they could do more to protect their environment. 'Anycompany.com' is a pseudonym given for purposes of this report to an actual organization where the following research was performed. *Anycompany.com* is a very large organization with over 40,000 systems in its decentralized computing environment and a diverse population of over 20,000 employees spread over various departments and networks. This article is a corporate case study on the process *Anycompany.com* used to trace its virus problem and from where it hailed.

Anycompany.com started by researching some of their virus infections to see if there was any way to trace back to the first introduction of a particular virus into their environment. They reviewed their incident tracking information and discovered that they had experienced several instances of the W97M.Marker virus, which maintains a log of all systems that it infects – a travel itinerary of sorts for the virus. So, they began to follow the breadcrumbs that Marker left for them.

Collecting and Analysing the Breadcrumbs

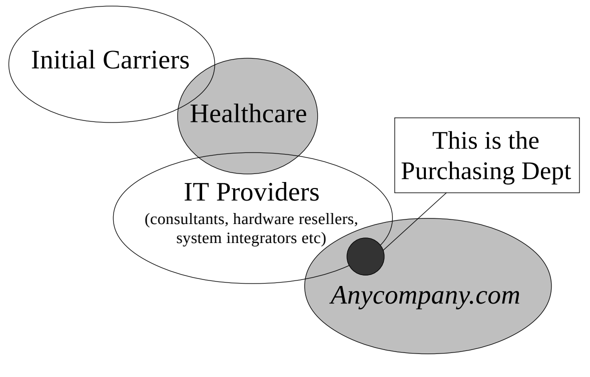
Anycompany.com had been finding it difficult preventing the Marker virus from infecting their organization. As in many organizations, *Anycompany.com* had found it hard maintaining and updating the anti-virus protection on the desktops across multiple networks. It should be noted that the basis of the information and samples for this case study were taken in February and March 1999 prior to the W97M.Melissa virus infection that opened many organizations' eyes to the need for anti-virus protection for their email servers. As a result, the desktop was the primary defence or protection point.

To help determine the scope of their infections and to track down systems which were infected, *Anycompany.com* specifically blocked all outgoing traffic to the FTP site to which the Marker virus attempted to send the log file. *Anycompany.com* then monitored for systems attempting to access that FTP site. Even though the FTP connection was never successful, *Anycompany.com* did not want its systems attempting to make the connection since it could alert the maintainer of the FTP site to their repeated infections and expose a vulnerability.

A daily check of all systems attempting the FTP connection was performed and the 'offending' systems were identified. For each system identified, *Anycompany.com* alerted the appropriate system administrator and the system was reviewed, the anti-virus protection updated, and the system cleaned. The administrator was also asked to submit a copy of the log file that the virus created to *Anycompany.com*'s information security staff before removing it from the system. At the end of one month, *Anycompany.com* had collected fifteen distinct samples and began its analysis.

Anycompany.com took the samples and began breaking down the entries. The logs provided names, organizations, and dates for each infection captured in the log. While some entries were not complete, the entries were sufficient, based on the information in the system registry that was captured by the virus, to begin establishing patterns of travel. *Anycompany.com* was able to construct diagrams of each infection path and show intersections between the paths, including types of organizations that had been infected. The diagram below is a graphical representation of the relationships between the various entities that became infected by the Marker virus in *Anycompany.com's* samples. This kind of exercise, and graphical tool, helped *Anycompany.com* to identify their relationship with the others in the log and the path the virus had taken to reach their organization.

The Breadcrumbs...


Initial Carriers
Healthcare
This is the Purchasing Dept
IT Providers
(consultants, hardware resellers, system integrators etc)
Anycompany.com

Following the Breadcrumbs

Anycompany.com found during its analysis that, while many of the log files had a variety of individuals listed, there were some very clear patterns in the travel of the virus and the types of organizations the virus had infected before it arrived in their systems.

The following points illustrate some of the observations consistent in all of *Anycompany.com's* samples as suggested by the relationship representations shown in the diagram.

- The virus had infected the same four initial systems in each sample – captured in the "Initial Carriers" set in the diagram.
- The virus travelled from the 'Initial Carriers' to at least three other systems before reaching a system in the healthcare industry.
- Once the virus infected a system in the healthcare industry, it moved throughout the organization and infected at least one other system in the same organization but at a different geographical location.
- The virus travelled from the healthcare industry to various information technology (IT) providers, including consultants, system integrators, and hardware resellers.
- The virus infected various systems throughout the IT providers and then infected individuals related to both the purchasing departments and vendors for *Anycompany.com.*
- The relationship between *Anycompany.com* and its purchasing departments, vendors, and its own IT providers was the point of entry of the virus into *Anycompany.com* systems.
- Once inside *Anycompany.com*, the virus was able to infect multiple systems throughout various departments and networks.

Finally, *Anycompany.com* were able to determine through their analysis that the virus did not in fact arrive from unknown individuals or individuals with malicious intent. Rather, their analysis clearly demonstrated that the infected items arrived through their electronic mail communications with and between other organizations that they had 'trusted' relationships with such as their employees, consultants, IT providers, and vendors.

It should be noted this company had no direct relationship to the healthcare industry. Nevertheless, *Anycompany.com* was able to ascertain that this recurring development was an important discovery, since it suggested that the health-care industry's connection with their IT providers was the point of entry for the virus. This also served as a poignant reminder to *Anycompany.com* that they were exposed to the same things as their direct connections. This was especially true if the direct connection, in this case the IT provider, did not have adequate anti-virus protection and acted as an unknowing conduit.

Learning Lessons

While the analysis *Anycompany.com* performed was with the W97M.Marker virus, they reviewed their findings and conclusions in conjunction with many of their other experiences with virus infections, such as the viruses and worms that perform mass mailings. These mailings provided similar results when looking at where the email attachment or message originated. Again, the infected items were not received from unknown entities but rather individuals and organizations where there was an existing and trusted relationship.

Given that the viruses and other 'Bad Things' can be shown to be coming from 'trusted' people and organizations, how does an organization or individual protect against infection? Like many organizations, *Anycompany.com* exchanges documents and other files frequently over its email systems and it has become a familiar way to share and disseminate corporate information.

As a result, traditional practices and guidance provided to computer users, such as being wary of things arriving from unknown sources or blocking incoming traffic from sites and organizations known to be spreading infected items, are obviously no longer sufficient or acceptable.

If the patterns that *Anycompany.com* saw in its environment are representative for organizations at large, digital signatures and encryption will not offer the level of protection currently purported. Digital signatures and encryption are a good way for an organization to establish a level of assurance that the item received is from a specified individual or organization and that the item has not been tampered with since it was signed or encrypted.

Neither of these technologies, however, do anything to establish that the item was not infected before it was signed or encrypted. So, these technologies will simply make it easier for the infected item to infiltrate your organization and more difficult for you to educate your users and your applications about when to trust and when not to trust.

In essence, for a corporate organization to protect itself, a variety of anti-virus protection strategies must be implemented and maintained at the points of entry to the business, thereby providing layers of defence. In addition to this, user education becomes even more crucial in order to keep users aware of the changing threats and ways that the infected items will arrive. Remind your users that items received from so-called 'trusted' individuals should also be treated as suspicious until they are found to be free from any infections. 'Trust' should no longer be viewed as the default answer.

Based on *Anycompany.com's* real-life experiences and analysis, the moral of this corporate case study seems to be that the ones you 'trust' in your business actually pose your biggest threat. Something to think about finally is the fact that once you trust one entity, you inadvertently inherit everyone they trust.