Managing Malware Masterfully

By: Kevin Kalinich | September 1, 2016

Kevin Kalinich is the global cyber risk practice leader for Aon Risk Solutions, focusing on identifying exposures and developing insurance solutions. He can be reached at riskletters@lrp.com.

As ransomware morphed from low-severity consumer phishing to targeting entire networks of computers in hospitals, universities and businesses, it became more costly.

It also looks like email recipients have a lot more learning to do.

According to 2016 Verizon research, 23 percent of recipients open phishing messages and 11 percent of recipients click on attachments.

Ransomware, however, is just one version of "malware," which includes all types of hostile or intrusive software, such as computer viruses, worms, trojan horses, spyware, adware, scareware, and other malicious programs. Malware, which stands for "malicious software," can take the form of executable code, scripts, active content, and other software.

Entities should consider malware risks on an enterprise level. It's not just about IT. All employees, partners, customers and third-party outsourced providers should be considered.

The number of unique kinds of malware jumped from six million at the beginning of 2015 to just over 12 million by the end of the year, and the category of malware specifically targeting mobile phones has seen dramatic growth.

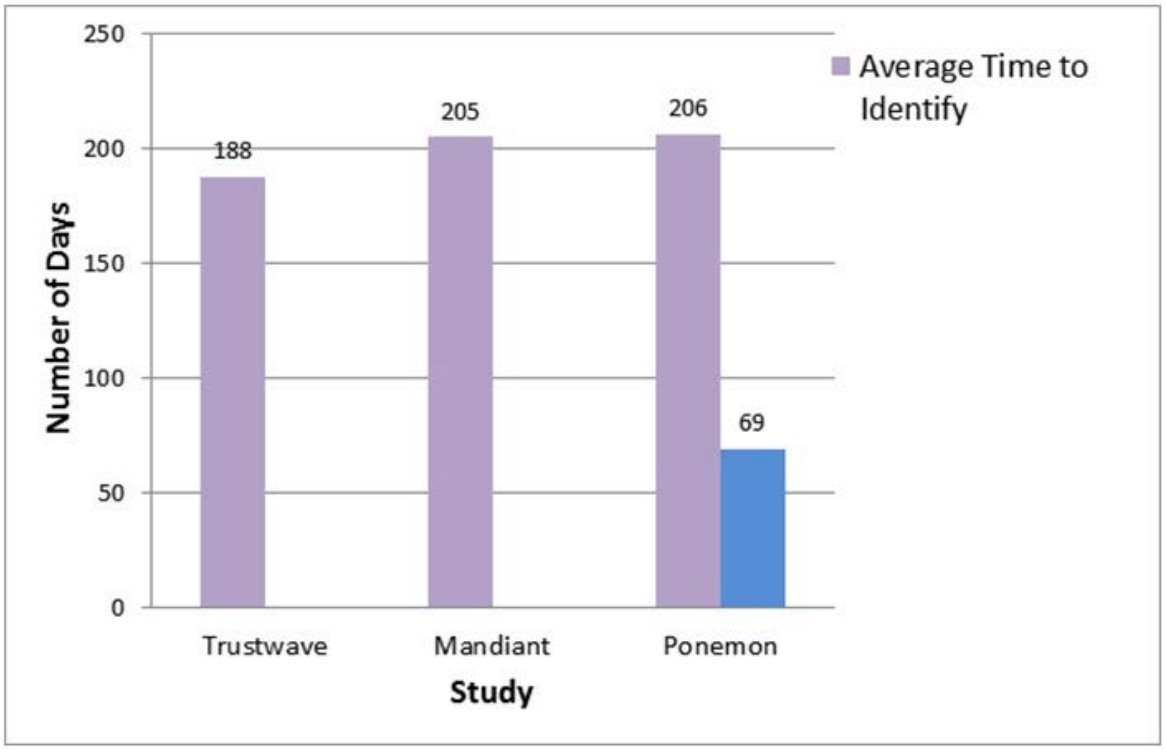
Organizations should quantify potential malware exposures in terms of financial statement impact and review potential available insurance coverage.

Malware could trigger a number of different lines of insurance, such as crime ($81 million Bank of Bangladesh heist), kidnap & ransom (Hollywood Presbyterian Medical Center's $17K bitcoin ransom), property (Stuxnet in Iranian nuclear facility & other grid/manufacturing), general liability (Jeep Cherokee and medical device hacks), professional liability (Internet of Things service interconnectivity) and marine/supply chain (Islamic Republic of Iran Shipping Lines 2011).

Entities should consider malware risks on an enterprise level. It's not just about IT. All employees, partners, customers and third party outsourced providers should be considered.

Even with top notch defenses, however, how do you defend against something that may be inevitable? Is there anything a business can do to protect against losses from malware? Many malware attacks exploit known bugs in software, and attackers depend on victims not installing patch updates. There are a number of technological and procedural risk management methods to help reduce the financial statement impact from malware, including:

- Vet software purchases from a security standpoint as well as an operational standpoint.
- Train employees regarding phishing, mobile apps, attachments, links and the like. Instruct employees not to open email from unknown sources and to verify sources before opening attachments or clicking links in any email, IM, or posts on social networks.
- Ban workplace usage of unnecessary file types, software applications, websites, and BYOD downloads.
- Improve detection and remediation of malware incidents.
- Segregate data by priority classification.



According to the recent book, Dark Territory: The Secret History of Cyber War (June 2016):

"The only completely secure computer is a computer that no one can use … They have given up on the idea that they can somehow make a black box that nobody can get into."

It turns out that incident response is as important as prevention from a balance sheet impact standpoint. Is there a contingency plan or business continuity plan in place? Some suggested actions to take if your computer is infected with malware:

- Immediately stop using any computers on an infected network that performs sensitive activities.
- Contact your IT department or a qualified IT professional to analyze your computers and network, and to remove the malware.
- After you have taken appropriate steps to remove malware, change the passwords for any user accounts or systems that were accessed while using the infected computer.
- Promptly notify the appropriate insurance carriers.