RansomWare – Reactive or Proactive Protection?

The FBI estimated last year that RansomWare payments in the United States were on pace to hit $1 billion in 2016, compared with $24m paid to cyber attackers in 2015. The U.S. government also estimated that RansomWare attacks averaged more than 4,000 per day in 2016, up from the approximately 1,000 attacks per day in 2015.

The Los Angeles Community College District has admitted handing over $28,000 in bitcoin payment to cyber attackers to regain access to data encrypted by malware commonly known as RansomWare. The attack hit Los Angeles Valley College on 30th. December 2016, locking college staff out of the computer network, including college email and voicemail systems. The college said in a statement that it had obtained the funds for the ransom and assistance of cyber security experts from a cyber security insurance policy created to deal with such incidents. They were lucky that the bad guys kept to their side of the bargain and released the key to decrypt their data after payment was received.

Not all are so fortunate. Kansas Heart Hospital admitted to paying ransom demands in May 2016 and they only received a key to release part of the data. It was accompanied by a further demand for more payment to release the rest. The hospital refused to pay more.

The Los Angeles Valley College said the decision to pay the ransom was made in consultation with district and college leadership, outside cyber security experts and law enforcement.

“It was the assessment of our outside cyber security experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost,” the college said.

Fortunately for the college, the attackers delivered a key for decrypting the data after payment was made. “The process to unlock hundreds of thousands of files will be a lengthy one, but so far, the key has worked in every attempt that has been made,” the college said.

Patently this approach is solely reactive, expensive, time consuming and ultimately unreliable. How can you provide maximum protection?

For optimum protection against RansomWare, organisations should assume they're going to get hit, said Robert Rhame, a research director at Gartner who focuses on backup and recovery. "Backup and recovery remains the top protection," Rhame said.

Jason Buffington, a principal analyst at Enterprise Strategy Group Inc., in Milford, Mass., focusing on data protection, said there are three keys to protection against RansomWare that organisations should make a priority:-

- What can you do to increase the frequency of protection?
- How can you increase the length of retention?
- How can your backup and recovery platform integrate with a malware detection tool?

"If you're using your backup solution as your mitigation against malware attacks, you're 99% there," Buffington said, stressing that back-up protection is proactive, while recovery is reactive.

As RansomWare is usually delivered through malicious links in email messages or through an infected website and typically encrypts all data on the infected machine and all other connected computers - it also makes sense to cut it off at source. Forcing all external traffic through a malware detection tool. Here all known variations are detected, isolated and then quarantined. The user can also use tools such as sandboxes to safely run the dubious content to check out unknown items. This is very proactive and a major frontline defence against attack.

Finally there are now packages available to scan existing data for slightest signs of infection that can also be applied to backup copies. It's even possible even on encrypted data.

All in all the best protection is a mixture of both reactive and proactive counter-measures. But it also must be accompanied with good practice and continuous education of the business to restrict, inadvertent, self-infection. Worryingly, the trend for 2017 is attack the smaller businesses. They are seen as 'easy meat' that lacks the protection of their bigger cousins. So be warned it's not if but when.