Ransomware: No Honor Among Thieves and More Expensive

By Sharon D. Nelson, Esq. and John W. Simek

The FBI says that ransomware nets cybercriminals $1 billion a year. No wonder so many people want a piece of that pie.

Computerworld recently reported that hackers spreading ransomware are getting greedier. In 2016, the average ransom demand to provide the decryption key for encrypted data rose to $1,077, up from $294 the year before, according to a report from security firm Symantec. Symantec also reported a 36% increase in ransomware in 2016 from the prior year. We are aware of small law firms in Virginia that paid $1200 and $3000 to get their data back – the damage being furthered by the length of time it took to restore the data.

Helping to fuel the ransomware boom is the digital black market, where hackers can sell ransomware kits for as little as $10 and as much as $1,800, making it easier for other cybercriminals who can't code to get a piece of the action.

Cybercriminals also spread ransomware through exploit kits, or automated hacking toolsets, that operate on compromised websites. The kits can work by scanning a victim's web browser for any unpatched software vulnerabilities and then exploiting them to serve ransomware. We are guessing that most readers didn't know that this was an attack surface – most people think ransomware can only be contracted by opening an e-mail and clicking on a link or attachment – that's certainly the most common way, but there are others!

Symantec's report found that 34 percent of victims pay the ransom. However, only 47 percent of that number reported getting their files back. In a business where trusting the bad guys is important, figures like these may diminish the number of victims willing to "pay up."

Dark Reading also recently reported that about 40% of small and midsized businesses hit with ransomware paid their attackers, but less than half got their information back. This data came from a Bitdefender survey of 250 IT pros working in small and medium businesses (SMBs).

This survey, conducted by Spiceworks, discovered that one in five SMBs was hit with a ransomware attack within the past 12 months. Of the 20% targeted, 38% paid attackers an average of $2,423 to release their data. Less than half (45%) got their information back. The honor among thieves is clearly evaporating.

As attackers seek weaker victims, SMBs are favored targets. Larger businesses have strongly engineered backups and high level security tools. Researchers have found SMBs are appealing targets for ransomware because they handle the same sensitive business information (customer data, financial records, product info) as larger organizations, but lack the strong security measures to protect it. Attackers know they're more likely to receive payment from SMBs, which have more sensitive data than consumers.

E-mail, cited by 77% of SMBs – as mentioned above - is the most popular vector of attack.

Most SMBs hit with ransomware attacks were able to mitigate the attack by restoring data from backup (65%), or through security software or practices (52%). One-quarter of those targeted could not find a solution to address the infection and lost their data as a result. Since our clients are largely SMBs, we can affirm that they are more vulnerable - and sometimes resist a well-engineered backup system because they don't fully appreciate the danger and are resistant to the costs - which tend to seem **very** minor once they've become a ransomware victim. After being hit with ransomware, they tend to ask us for a proposal to enhance their backup system so they can in fact get their data back.

Though the FBI and other law enforcement agencies counsel ransomware victims not to pay, if they haven't properly engineered their backups to recover the data, many say they have no choice but to pay. Payments (usually in bitcoin) used to be in the $300-$500 range but we are seeing much larger demands these days. Some entities are even stockpiling bitcoins so they can pay the cybercriminals quickly. Some entities make a business decision that the cost of paying the ransom is cheaper than being out of business for some period of time while data is recovered. A good example is hospitals, which are likely to be sued if there are errors made because of the inability to get to data.

While the FBI counsels victims not to pay, agents are apt to whisper “but you gotta do what you gotta do.”

Calls we’ve received from ransomware victims are panicky conversations – and most of the panic stems from not having a properly engineered backup. This is a classic case – don’t be pennywise and pound foolish. Invest in a good backup system and, even if no one is completely impervious to ransomware, you’ll sleep better knowing that you can quickly recover from a ransomware infection.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com