The Rise of Ransomware

Cyber criminals are becoming more sophisticated with the financial-fraud schemes known as ransomware, and SMBs are prime targets. Here's how to protect your business.

By Debbi G. McCullough

SMB owners already have a lot to worry about—profits, staff efficiencies and client demands, to name a few. It's time to add "ransomware" to the list.

Ransomware is a type of malware that promulgates a financial fraud scheme; the bug enters your network—via phishing emails, drive-by emails, out-of-date operating systems, even websites—and encrypts the contents of your hard drive. The criminal then holds the files hostage until the victim pays a ransom. Experts see more ransomware attacks than five years ago, using more sophisticated efforts.

Researchers at Trend Micro, a global security software company headquartered in Tokyo, recently studied the operations of two persistent and high-volume file-encrypting ransomware creators: TorrentLocker and CryptoWall. Over 67% of users clicking on CryptoWall—currently the largest form of ransomware—came from SMBs in June and July 2014.

Also, SMBs comprised 42% of clicks on TorrentLocker URLs, while consumers accounted for 46% of clicks. Most of TorrentLocker's compromised websites, which hide re-directions and avoid detection, are hosted in the U.S.

The FBI's Internet Crime Complaint Center (IC3) also tracked 992 CryptoWall-related complaints between April 2014 and June 2015, with victims reporting losses totaling over $18 million. The financial impact usually exceeds the ransom fee. "Victims incur additional costs such as network mitigation, network countermeasures, legal fees and IT services," the report says.

"We're talking lost revenue, lost data and a huge disruption to your business lasting a week to 10 days," says Andrew Conway, research analyst with Cloudmark, a network security firm in San Francisco, Calif. "Imagine losing your desktop or laptop with minimal backup. That's what ransomware schemes are like; it takes considerable time to get your data back, and unencrypted."

He adds that while ransomware has been around for 10 years, the more sophisticated generation of CryptoWall targets millions of victims at once. The advent of bitcoin, by which most criminals receive the ransom, is helping to drive the growth, allowing victims to make anonymous, untraceable payments that law enforcement can't follow, he says. "Ransomware creators know [small- and medium-sized business] owners will often pay up."

Why are criminals targeting SMBs?

Experts find other reasons why SMBs make likely targets:

- SMBs typically possess less sophisticated security and backup. Robert Siciliano, a security expert with Carbonite, a company in Boston, Mass., that provides cloud and hybrid data collection, sees many SMB owners not realizing the risks and therefore not investing in security. "The chances of getting malware are high without basic preventative security and backup—it's like not locking the door when leaving the office," he says.
- SMBs are more likely than larger companies to have all critical data on a single machine, and less likely to conduct frequent data backups, Conway says.
- SMBs—the source of 74% of all new jobs since the end of the last recession—receive more unsolicited emails and attachments from job seekers than larger enterprises, Conway adds. In May, Cloudmark detected spam attacks containing a ransomware loader in a fake resume from 14 countries on five continents. Most spam targeted U.S.-based SMBs. "SMB owners seeking new employees will more likely open unsolicited resumes than a randomly selected spam victim," Conway says. Trend Micro says the social-engineering lures in ransomware—for example, order requests—tend to be more appealing to small businesses.
- SMBs are more likely to pay up because files essential to their operations are stored in their servers rather than off-site, says Mark Parker, senior product manager at iSheriff, a security protection provider for corporations.

What to look for

Ransomware infections surface in dozens of ways, but experts see patterns as well:

- The Cloudmark study found the fake resumes embedded in simple emails containing a female first name, an attached zip file containing HTML using an IFRAME tag to download another zip file, containing a Windows screen saver with a .scr suffix. "Criminals frequently use this format to deliver malware as it arouses fewer suspicions than an .exe file," Conway says.
- Phishing emails often contain funny pictures your friend apparently posted on Facebook, asking you to click to see, Siciliano says.
- Criminals are localizing ransomware emails. Trend Micro found TorrentLocker ransomware gangs in Italy, Turkey, and Australia frequently send emails imitating notices from local courier services, post offices, mobile operators or utility companies.

How to protect your business

Consider these essential steps to protect your SMB from the risks of ransomware:

- Train employees not to open attachments or click on links from unknown sources, Parker says. "Your staff is your strongest line of defense."
- Invest in legitimate antivirus protection, rather than free ones. Siciliano says antivirus software, including Symantec, Kaspersky, Trend Micro and Intel's McAfee, can cost as little as $100 for an SMB.
- Add firewalls from reputable companies and enable pop-up blockers because criminals regularly use pop-ups to spread malicious software, the FBI recommends.
- Invest in backup. "Having external drives and servers backing up your data will minimize the cost and disruption," Siciliano says. Trend Micro researchers suggest data backup using the 3-2-1 rule—at least three copies in two different formats with one copy stored off-site.
- Don't pay the ransom. Double-check you've backed up the encrypted files, wipe your system clean and restore the data, Siciliano says.
- Apply patches and updates to your operating system and software, especially Adobe products and Microsoft products and browsers, Conway adds. "Then, if you do visit a malicious website and encounter a watering hole attack, you're far less likely to get this malware installed on your computer."

Related: Biometric security is coming to an SMB near you.

Related: Is cloud storage secure enough for high-privacy SMBs?

Related: The next step in data backup is security.

ILLUSTRATION: RAWPIXELIMAGES | DREAMSTIME.COM