7 of 998 DOCUMENTS

Network World

February 4, 2016 Thursday 12:39 PM EST

Ransomware is only getting worse. How do you prepare for it?

BYLINE: Michelle Drolet

SECTION: OPINION

LENGTH: 768 words

Click for image

Ransomware is big business. Over the last few years we've observed the steady rise of **ransomware**, with some trepidation. It is fast becoming a multi-billion dollar business, and it's getting surprisingly sophisticated. The **ransomware** industry is continually innovating, offering cybercriminals new technology, various business models, and all the support they need to conduct successful attacks on unsuspecting individuals and companies.

Changing face of **ransomware**

Ransomware has come full circle since it first appeared on the scene in 2005. Early crypto **ransomware** soon gave way to misleading apps, fake antivirus tools, and lockers. But it's back now, it's mature, and it's here to stay, according to Symantec's Evolution of **Ransomware** report.

In the early days of **ransomware**, attackers would use misleading apps and fake AV tools to alarm victims and then ask for fees to fix the fake problems. Or they might flash up bogus FBI warnings, threatening prosecution unless money was paid. Eventually they began to lock down systems, blocking access to specific apps or the whole system until the ransom was met.

The main threat today is crypto **ransomware**, where files are securely encrypted and victims have to pay to secure the key and unlock their own files, and it's very tough to beat.

"The **ransomware** is that good," said Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI's CYBER and Counterintelligence Program in Boston, talking to The Security Locker. "To be honest, we often advise people just to pay the ransom."

Cost of **ransomware**

There are lots of different **ransomware** packages out there. Just looking at one of the most popular examples, CryptoWall, the FBI's Internet Crime Complaint Center (IC3) received 992 related complaints between April 2014 and June 2015, with victims reporting losses of more than $18 million. That's just what was reported.

The Cyber Threat Alliance put together a report profiling the CryptoWall v3 threat and suggested that it had afflicted hundreds of thousands of users worldwide and caused damages in the region of $325 million.

Services for cybercriminals

In McAfee Labs' 2016 Threats Predictions report, **ransomware** features prominently and the report makes special mention of the success of the **ransomware**-as-a-service business model. Experienced cybercriminals are offering high-quality **ransomware** to would-be attackers with little or no technical knowledge or skills in return for a cut of the extortion profits. The **ransomware** is typically hosted on the Tor network, and payment is made almost untraceable with virtual currencies like Bitcoin.

Users of these **ransomware** services can expect to get helpdesk support, and it's in the interests of the extorters to ensure that data is returned to those who pay. These service providers will skim anywhere from 5% to 20% of each ransom, so they aim to make it as easy as possible for the cybercriminals who sign up.

What can you do?

Just like any other malware, you have to install **ransomware** before it can encrypt your files, so there are some simple precautionary steps that everyone can take to drastically reduce the risks:

- Install reputable anti-virus and anti-malware software.
- Don't open attachments in emails, unless you know what it is.
- Don't follow links in emails, close the email, and go directly to the website in your browser.
- Use strong passwords, and don't reuse the same passwords.
- Make sure all of your system software and browsers are patched automatically with security updates.
- You should apply all of these rules to whatever device you're using. Smartphones, tablets, and Macs are not immune to **ransomware**.
- Finally, make sure you have solid back-ups of all your data.

You can also mitigate the risk of **ransomware** by having a robust and regular backup routine. If your files are backed up and you can access them, there's no need to pay to unlock them, but it may still require some serious effort to rid yourself of the **ransomware** once your system is infected.

Ransomware is sure to be an even bigger issue in 2016, so it's very important that you take steps to prevent infection. If you do fall prey to something like CryptoWall v3, there's no way around it. Your only realistic prospect of getting the files back is to pay the ransom, or, better yet, restore from back-up!

When it comes to **ransomware**, the old saying, "an ounce of prevention is worth a pound of cure," could not be more fitting.

The opinions expressed in this Blog are those of Michelle Drolet and do not necessarily represent those of the IDG Communications, Inc., its parent, subsidiary or affiliated companies.

LOAD-DATE: February 5, 2016

LANGUAGE: ENGLISH

PUBLICATION-TYPE: Newspaper