Ransomware like Bad Rabbit is big business

October 26 2017, by Michael J. Armstrong And Teju Herath

October is Cybersecurity Awareness month, which is being observed in the United States, Europe, and elsewhere around the world. Ironically, it began with updates about a large-scale hack, and is ending with a large-scale ransomware outbreak.

Internet firm Yahoo kicked things off on Oct. 3 when it admitted that hackers in 2013 had accessed information about all three billion of its user accounts, not "just" the one billion first reported.

Ransomware "Bad Rabbit" is providing the finale with attacks that began Oct. 24. So far, the outbreak is mostly affecting business computers in Russia.

Both stories are fitting, in a way. The FBI considers computer break-ins and data ransoming the top two cyber threats we face. But while the former is old-fashioned e-crime, ransomware is much trendier. Much like online retailing, online advertising, and online currencies, ransomware is soaring.

Your money or your data

Traditional criminal hackers obtain their ill-gotten gains by stealing valuable data such as credit card numbers or passwords. They then look for customers, such as other criminals, to buy that data.

In contrast, ransomware hackers instead sell data back to the owners. If ransomware infects your computer, it encrypts your files to render them inaccessible until you pay a ransom. This simplifies cybercrime by replacing theft with extortion.

For example, in summer 2016, ransomware locked down the University of Calgary email system. The university paid $20,000 to unlock it.

Today, that looks cheap. In July, a Canadian company reportedly paid $425,000 to regain its data. The month before, South Korean firm Nayana paid $1 million, the highest ransom publicly admitted so far.

Growing scale and sophistication

Much like legitimate firms, some ransomware charges lower "prices" but targets larger volumes. Bad Rabbit demands only a few hundred dollars to decrypt each computer. But it is affecting machines across Russia.

Similarly, the Wannacry ransomware attack in May affected computers in about 100 countries. It forced many British hospitals to cancel surgeries.

An IBM survey found that almost half of businesses suffered ransomware attacks in 2016. Some 70 per cent of those paid a ransom to regain their data.

The survey also indicates small businesses are particularly vulnerable. They often lack the computer expertise to defend themselves. Only 30 per cent provided cybersecurity training to employees, compared to 58 per cent within larger companies.

Ransomware's sophistication is growing too. Ransomware "worms" like ZCryptor spread themselves across networks, rather than riding on infected emails.

Some ransomware specialists are selling their services to organized crime. This crime-as-a-service business model allows criminals to outsource their technology needs. User-friendly ransomware "kits" can be purchased for $175.

Future possibilities

What might come next? Imagine state-sponsored hackers using ransomware. Host countries might give—or even sell—permission for local hackers to attack rival countries' computers.

These cyber-privateers could plunder commerce abroad, without the host country's direct involvement or accountability. Think of regional rivals like North and South Korea, or major powers like the U.S., Russia and China.

Sound far-fetched? Russian security services have already been accused of working with organized crime on cyberattacks. The Russian government denies any involvement. But its president, Vladimir Putin, did suggest independent "patriotic hackers" may have tampered with the U.S. election process.

How about virtual protection rackets? Instead of one-time payments for decryption, users might be "convinced" to pay ongoing fees for the "service" of avoiding encryption.

Or instead of hiding virtual data, ransomware could shut down physical objects. The Internet of Things is exposing new targets. Control systems for factories, utilities and our homes are increasingly online.

What if ransomware turned them off? Businesses begrudgingly pay thousands to recover emails. Imagine what they'd pay to restart assembly lines.

Precautions to take

To defend themselves, computer users need to do the basics. Run antivirus programs to detect threats. Think before clicking on unexpected email attachments. Keep application software and operating systems updated. (Surely you're not still running Windows XP?)

Users should also back-up files regularly. If ransomware strikes, backups allow ransom-free recovery. But keep them on removable drives to prevent their infection.

Infected users can also try decrypting files with tools from sites like NoMoreRansom.org. But these might work only on simple cases.

Corporate and government action

Software makers should do more to facilitate safe computing practices. For example, it's great that Windows now has self-updating antivirus protection. Unfortunately, it's still awkward to back-up data onto removable drives.

Business insurers could also play a role. They might require corporate computers to be updated and backed-up to qualify for coverage.

Co-operation among independent agencies is needed to fight ransomware's breadth. Canada's Communications Security Establishment set a good example two weeks ago when it made its Assemblyline malware analysis software publicly available to tech professionals.

In contrast, the U.S. National Security Agency sets a bad example: It had known about a weakness in Windows for years, but didn't tell Microsoft until early 2017.

Law enforcement likewise needs to cooperate across jurisdictions. September's Interpol-Europol Cybercrime Conference was a good step in this direction.

As foreign hackers increasingly "tax" domestic businesses, ransomware becomes a national security issue. Governments may need to negotiate agreements like those covering seaborne piracy.

Finally, firms might consider keeping key systems disconnected from the internet, as some military computers have always been. Just because anything can be online, it doesn't mean everything should be.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Ransomware like Bad Rabbit is big business (2017, October 26) retrieved 27 April 2024 from https://phys.org/news/2017-10-ransomware-bad-rabbit-big-business.html