Why installing software updates makes us WannaCry

May 16 2017, by Elissa Redmiles

Credit: AI-generated image (disclaimer)

The global ransomware attack called "WannaCry," which began last week and continues today, could have been avoided, or at least made much less serious, if people (and companies) kept their computer software up to date. The attack's spread demonstrates how hundreds of thousands of computers in more than 150 countries are running outdated

software that leaves them vulnerable. The victims include Britain's National Health Service, logistics giant FedEx, Spanish telecom powerhouse Telefonica and even the Russian Interior Ministry.

The security flaw that allowed the attack to occur was fixed by Microsoft in March. But only people who keep their computers updated were protected. Details of the flaw were revealed to the public in April by the Shadow Brokers, a group of hackers who said they had stolen the information from the U.S. National Security Agency.

Attackers got into computers through that weakness and encrypted users' data, demanding a ransom from anyone who wanted the data made usable again. But they didn't win the race to exploit the flaw as much as people and computer companies collectively lost it. Our human tendencies and corporate policies worked against us. Research, including my own, tells us why, and offers some suggestions for how to fix it before the inevitable next attack.

Updating is a pain

All people had to do to stay safe from WannaCry was update their software. But people often don't, for a number of specific reasons. In 2016, researchers from the University of Edinburgh and Indiana University asked 307 people to discuss their experiences of installing software updates.

Nearly half of them said they had been frustrated updating software; just 21 percent had a positive story to tell. Researchers highlighted the response of one participant who noted that Windows updates are available frequently – always the second Tuesday of every month, and occasionally in between those regular changes. The updates can take a long time. But even short updates can interrupt people's regular workflow, so that study participant – and doubtless many others – avoids

installing updates for "as long as possible."

Some people may also be concerned that updating software could cause problems with programs they rely on regularly. This is a particular concern for companies with large numbers of computers running specialized software.

> Ever wonder why people dont update software? The latest version of Instagram includes a time-saving feature of crashing every time I open it
>
> — Adrienne Porter Felt (@__apf__) May 15, 2017

Is it necessary?

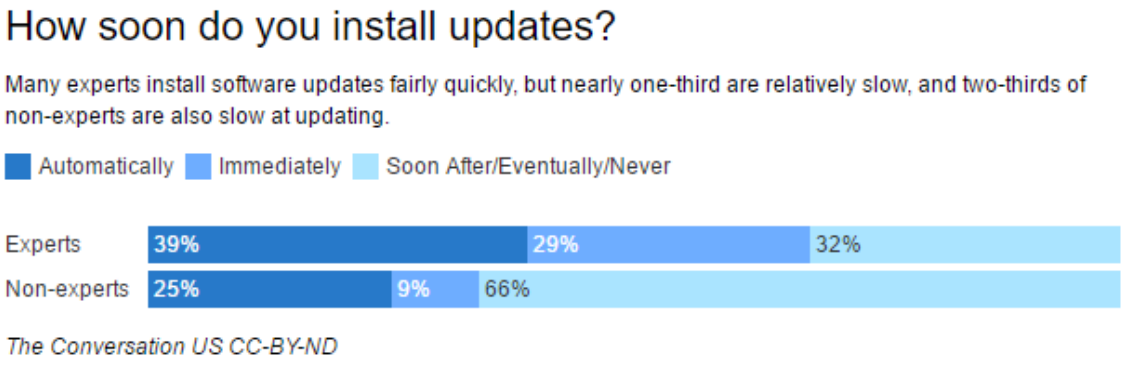
It can also be very hard to tell whether a new update is truly necessary. The software that fixed the WannaCry vulnerability came out in a regular second-Tuesday update, which may have made it seem more routine. Research tells us that people ignore repeated security warning messages. Consequently, these monthly updates may be especially easy to ignore.

The companies putting out the updates don't always help much, either. Of the 18 updates Microsoft released on March 14, including the WannaCry fix, half were rated "critical," and the rest were labeled "important." That leaves users with little information they could use to prioritize their own updates. If, for example, it was clear that skipping a particular update would leave users vulnerable to a dangerous ransomware attack, people might agree to interrupt their work to protect themselves.

Even security experts struggle to prioritize. The day the fix was released, Microsoft watcher Chris Goettel suggested prioritizing four of the 18

updates – but not the one fixing WannaCry. Security company Qualys also failed to include that specific update in its list of the most important March updates.

Security pros, and everyone else



The most common recommendation is to update everything immediately. People just don't do that, though. A 2015 survey by Google found that more than one-third of security professionals don't keep their systems current. Only 64 percent of security experts update their software automatically or immediately upon being notified a new version is available. Even fewer – just 38 percent – of regular users do the same.

Another research project analyzed software-update records from 8.4 million computers and found that people with some expertise in computer science tend to update more quickly than nonexperts. But it's still slow: From the time an update is released, it takes an average of 24 days before half of the computers belonging to software engineers are

updated. Regular users took nearly twice as long, with 45 days passing before half of them had completed the same update.

Making updates easier

Experts might be quicker at updating because they understand better the potential vulnerabilities updates might fix. Therefore, they might be more willing to suffer the annoyances of interrupted work and multiple restarts.

Software companies are working on making updates more seamless and less disruptive. Google's Chrome web browser, for example, installs updates silently and automatically – downloading new information in the background and making the changes when a user quits and then reopens the program. The goal is for the user not to know an update even happened.

That's not the right choice for all kinds of updates, though. For example, the Windows update needed to protect against the WannaCry attack requires the computer to restart. Users won't tolerate their computers shutting down and restarting with no warning.

Getting the message out

So computer companies must try to convince us – and we must convince ourselves – that updates are important. My own research focuses on doing just this, by producing and evaluating entertaining and informative videos about computer security.

In our first experiment evaluating the video, we conducted a month-long study to compare our video with an article of advice from security firm McAfee. The video was effective for more of our participants than the McAfee article was. Our video was also equally or more effective,

overall, at improving people's updating practices. Trying new approaches to teaching security behaviors such as our edutainment video, or even security comics, may be a first step toward helping us stay safer online.

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

Provided by The Conversation

Citation: Why installing software updates makes us WannaCry (2017, May 16) retrieved 25 April 2024 from https://techxplore.com/news/2017-05-software-wannacry.html