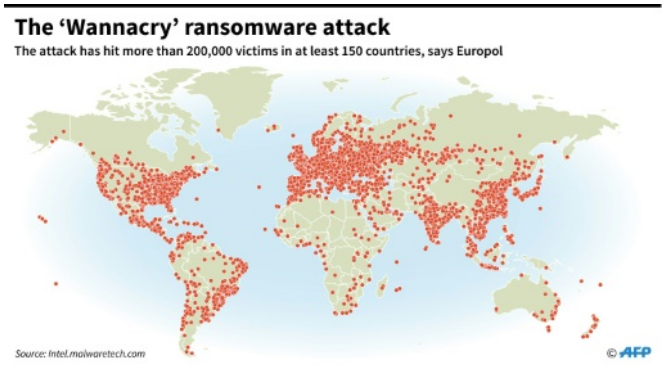
Who's to blame for ransomware outbreak?

15 May 2017, by Rob Lever



The 'Wannacry' ransomware attack

Questions are swirling over who is responsible for the security flaws exploited by hackers in the world's biggest ransomware attack to date, which crippled thousands of businesses and public organizations around the world. Here are some answers:

Who bears the blame?

Because hackers exploited a security hole in some Windows versions discovered by the National Security Agency, Microsoft says the intelligence agency bears some responsibility.

"This attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem," Microsoft president and general counsel Brad Smith said in a weekend blog post.

Steven Weber, faculty director at the Center for Long-Term Cybersecurity at the University of California, said "the fault is pretty distributed—there are plenty of people to blame."

Weber said the NSA's primary mission is intelligence: "If I were sitting at the NSA I would push that argument right back to Microsoft," he argued. "They would say, 'It's our job to stockpile those weapons and use them against our adversaries.'"

Other factors were the large number of old, outdated software programs in use and often ineffective security systems.

Cornell University computer scientist Stephen Wicker blamed "profound ethical lapses" both on the part of the US government and the computing public.

The flaws "were known to the NSA and CIA, but were kept secret by those organizations to be exploited for their own data collection purposes," Wicker said.

But he added that a large number of businesses and other users failed to install a patch issued by Microsoft in March, and also share the blame for spreading the malware.

President Donald Trump's homeland security advisor Tom Bossert dismissed the idea that the US is to blame.

"This was not a tool developed by the NSA to hold ransom data," Bossert told reporters.

"This was a vulnerability exploit as one part of a much larger tool that was put together by the culpable parties and not by the US government."

How did hackers get this tool?

Microsoft effectively confirmed analysts' diagnosis that the ransomware known as "WannaCry" was designed to exploit NSA software that was leaked earlier this year by a group calling itself Shadow Brokers.

President Vladimir Putin has said Russia—which has been accused of cyber meddling in several countries—had nothing to do with the massive cyberattack, and criticized the US intelligence community for creating the original software.

But Bruce Schneier, chief technology officer for IBM Resilient Systems, has suggested that a state-sponsored actor, most likely Russia, was probably responsible for the initial hack of the NSA.

"Whoever got this information years before and is leaking it now has to be capable of hacking the NSA and/or the CIA, and willing to publish it all," Schneier said in a recent blog post.

"The list of countries who fit both criteria is small: Russia, China, and... and... and I'm out of ideas."

James Lewis, a cybersecurity specialist with the Center for Strategic and International Studies, said he believes the exposure of the flaw likely "leads back to Moscow"—but that the hackers who designed the malware are probably not Russian.

"One of the rules in Russia is that Russian criminals are not allowed to hack Russian targets," Lewis said. "This does not fit the pattern of Russian-sponsored activity."

"The cybercrime market is really innovative," he added, "and they are quick to take advantage of vulnerabilities."

What about computer security at large?

The attacks came a day after US President Donald Trump signed an executive order calling for improved cybersecurity in the federal government and better cooperation with the private sector.

But few see this or any single initiative as a silver bullet.

Weber said the attacks show the risks of an overreliance on computerized systems that are not fully secure.

"We have built an increasingly digital society on a very insecure foundation and we are starting to see the consequences of that," he said.

Weber warned there is no single entity capable of fixing this problem in the near future, since security depends on so many factors.

"If you want to look for an upside, it would be this would be a wakeup call," to improve computer security, he said.

At the same time, Weber noted that the attack could prompt more people to shun digital technology and turn back to analog systems that can't be hacked.

Weber said there are already some signs that the public is losing confidence in the digital world as a result of security problems.

"For Silicon Valley and technology companies, their future depends on these underlying systems working," he said.