The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack

Posted May 14, 2017 by Brad Smith - President and Chief Legal Officer

Early Friday morning the world experienced the year's latest cyberattack.

Starting first in the United Kingdom and Spain, the malicious "WannaCrypt" software quickly spread globally, blocking customers from their data unless they paid a ransom using Bitcoin. The WannaCrypt exploits used in the attack were drawn from the exploits stolen from the National Security Agency, or NSA, in the United States. That theft was publicly reported earlier this year. A month prior, on March 14, Microsoft had released a security update to patch this vulnerability and protect our customers. While this protected newer Windows systems and computers that had enabled Windows Update to apply this latest update, many computers remained unpatched globally. As a result, hospitals, businesses, governments, and computers at homes were affected.

All of this provides the broadest example yet of so-called "ransomware," which is only one type of cyberattack. Unfortunately, consumers and business leaders have become familiar with terms like "zero day" and "phishing" that are part of the broad array of tools used to attack individuals and

Featured Posts

Growing consensus on the need for an international treaty on nation state attacks

This week, the Group of 7 (G7) published a declaration ... *Read more »*

Microsoft joins NoBully, UNESCO in upcoming global campaign to stop online bullying

Microsoft has joined NoBully and UNESCO (United Nations Educational, Scientific ... *Read more »*

Join us: Working together to help people with autism enter the workforce

As we celebrate National Autism Awareness Month throughout April and ... *Read more »*

Stay Connected

Have the latest posts sent right to your inbox. Enter your email below.

Email Add SUBS

Popular Posts

infrastructure. We take every single cyberattack on a Windows system seriously, and we've been working around the clock since Friday to help all our customers who have been affected by this incident. This included a decision to take additional steps to assist users with older systems that are no longer supported. Clearly, responding to this attack and helping those affected needs to be our most immediate priority.

At the same time, it's already apparent that there will be broader and important lessons from the "WannaCrypt" attack we'll need to consider to avoid these types of attacks in the future. I see three areas where this event provides an opportunity for Microsoft and the industry to improve.

As a technology company, we at Microsoft have the first responsibility to address these issues. We increasingly are among the first responders to attacks on the internet. We have more than 3,500 security engineers at the company, and we're working comprehensively to address cybersecurity threats. This includes new security functionality across our entire software platform, including constant updates to our Advanced Threat Protection service to detect and disrupt new cyberattacks. In this instance, this included the development and release of the patch in March, a prompt update on Friday to Windows Defender to detect the WannaCrypt attack, and work by our customer support personnel to help customers afflicted by the attack.

But as this attack demonstrates, there is no cause for celebration. We'll assess this attack, ask what lessons we can learn, and apply these to strengthen our capabilities. Working through our Microsoft Threat Intelligence Center (MSTIC) and Digital Crimes Unit, we'll also share what we learn with law enforcement agencies, governments, and other customers around the world.

Second, this attack demonstrates the degree to which cybersecurity has become a shared responsibility between tech companies and customers. The fact that so many computers remained vulnerable two months after the release of a patch illustrates this aspect. As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems. Otherwise they're literally fighting the problems of the present with tools from the past. This attack is a powerful reminder that information technology basics like keeping computers current and patched are a high responsibility for

Safety, privacy and the Internet paradox: solutions at hand and the need for new trans-Atlantic rules

Today at the Center for European Policy Studies, Brad Smith, … *Read more »*

Is life online stifling young people's self-expression?

Young people have been cautioned: For years, they've been told … *Read more »*

White House endorses student privacy pledge in call for comprehensive privacy reform

Today, I had the privilege of listening to the president's … *Read more »*

Latest Tweets

RT @Microsoft_Green: Making the grid more resilient through cloud tech is a triple win for the environment, consumers & utilities: https://…

MT @Safer_Online Learn how you can defend your computer & personal information from cybercriminals: https://t.co/56plyrujq1

Microsoft commits to implement new @isostandards anti-bribery standard & fight corruption worldwide. Here's why: https://t.co/g0ITjEFeyh

everyone, and it's something every top executive should support.

At the same time, we have a clear understanding of the complexity and diversity of today's IT infrastructure, and how updates can be a formidable practical challenge for many customers. Today, we use robust testing and analytics to enable rapid updates into IT infrastructure, and we are dedicated to developing further steps to help ensure security updates are applied immediately to all IT environments.

Finally, this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action.

The governments of the world should treat this attack as a wake-up call. They need to take a different approach and adhere in cyberspace to the same rules applied to weapons in the physical world. We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. This is one reason we called in February for a new "Digital Geneva Convention" to govern these issues, including a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them. And it's why we've pledged our support for defending every customer everywhere in the face of cyberattacks, regardless of their nationality. This weekend, whether it's in London, New York, Moscow, Delhi, Sao Paulo, or Beijing, we're putting this principle into action and working with customers around the world.

We should take from this recent attack a renewed determination for more urgent collective action. We need the tech sector, customers, and governments to work together to protect against cybersecurity attacks. More action is needed, and it's needed now. In this sense, the WannaCrypt attack is a

wake-up call for all of us. We recognize our responsibility to help answer this call, and Microsoft is committed to doing its part.

About the Author

Brad Smith

President and Chief Legal Officer

Brad Smith is Microsoft's president and chief legal officer. Smith plays a key role in representing the company externally and in leading the company's work on a number of critical issues including privacy, security, accessibility, environmental sustainability and digital inclusion, among others.

Back to top

Share this post:

Related Stories

Widening our 'Gateway to the Pacific'

With 40 percent of all jobs in Washington state tied to trade, the Seattle region

Read more »

FBI and DOJ take on the Coreflood botnet

Today, the FBI and U.S. Department of Justice announced a legal and technical operation to

Read more »

White House endorses student privacy pledge in call for comprehensive privacy reform

Today, I had the privilege of listening to the president's speech at the Federal Trade

Read more »

