Cyberattacks targeting health care must stop

blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

November 13, 2020

Two global issues will help shape people's memories of this time in history – Covid-19 and the increased use of the internet by malign actors to disrupt society. It's disturbing that these challenges have now merged as cyberattacks are being used to disrupt health care organizations fighting the pandemic. We think these attacks are unconscionable and should be condemned by all civilized society. Today, we're sharing more about the attacks we've seen most recently and are urging governments to act.

In recent months, we've detected cyberattacks from three nation-state actors targeting seven prominent companies directly involved in researching vaccines and treatments for Covid-19. The targets include leading pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea and the United States. The attacks came from Strontium, an actor originating from Russia, and two actors originating from North Korea that we call Zinc and Cerium.

Among the targets, the majority are vaccine makers that have Covid-19 vaccines in various stages of clinical trials. One is a clinical research organization involved in trials, and one has developed a Covid-19 test. Multiple organizations targeted have contracts with or investments from government agencies from various democratic countries for Covid-19 related work.

Strontium continues to use password spray and brute force login attempts to steal login credentials. These are attacks that aim to break into people's accounts using thousands or millions of rapid attempts. Zinc has primarily used spear-phishing lures for credential theft, sending messages with fabricated job descriptions pretending to be recruiters. Cerium engaged in spear-phishing email lures using Covid-19 themes while masquerading as World Health Organization representatives. The majority of these attacks were blocked by security protections built into our products. We've notified all organizations targeted, and where attacks have been successful, we've offered help.

These are just among the most recent attacks on those combating Covid-19. Cyberattacks targeting the health care sector and taking advantage of the pandemic are not new. Attackers recently used ransomware attacks to target hospitals and healthcare organizations across the United States. Earlier in the pandemic, attacks targeted Brno University Hospital in the Czech Republic, Paris's hospital system, the computer systems of Spain's hospitals, hospitals in Thailand, medical clinics in the U.S. state of Texas, a health care agency in the U.S. state of Illinois and even international bodies such as the World Health Organization. In Germany, we recently saw the resulting threat to human health become tragic reality when a woman in Dusseldorf reportedly became the first known death as a result of a cyberattack on a hospital.

Today, Microsoft's president Brad Smith is participating in the Paris Peace Forum where he will urge governments to do more. Microsoft is calling on the world's leaders to affirm that international law protects health care facilities and to take action to enforce the law. We believe the law should be enforced not just when attacks originate from government agencies but also when they originate from criminal groups that governments enable to operate – or even facilitate – within their borders. This is criminal activity that cannot be tolerated.

The good news is that we're not alone. Our voice at Microsoft is just one of many speaking up from the multi-stakeholder coalition that will be needed to make progress. In today's virtual Paris Peace Forum event addressing an audience of international leaders, Brad will discuss these issues with France's Minister for Foreign Affairs Jean-Yves le Drian, Ambassador Guilherme de Aguiar Patriota of Brazil and Ambassador Jürg Lauber of Switzerland. Ambassador Patriota is chair of the UN's Group of Governmental Experts, and Ambassador Lauber is chair of the UN's Open-Ended Working Group – both important bodies in determining the future of cyberspace.

In the leadup to this year's Paris Peace Forum, more than 65 health care-related organizations have joined the Paris Call for Trust and Security in Cyberspace. They include organizations like Merck working on vaccines, top hospitals like Hospital Metropolitano in Ecuador, and government health institutes like Poland's National Institute of Public Health. There is no question the attacks we've seen in recent months are creating energy for action across the health sector. The Paris Call remains the largest multi-stakeholder coalition addressing these issues, and its first principle is the prevention of malicious cyber activities that threaten indiscriminate or systemic harm to people and critical infrastructure.

In May, a 136-strong group of the world's most prominent international law experts, in what has become known as the Oxford Process, issued a statement making it clear that international law protects medical facilities at all times. In August, the Oxford Process issued a second statement emphasizing that organizations that research, manufacture and distribute of Covid-19 vaccines are also protected.

Earlier this year, the CyberPeace Institute and International Committee of the Red Cross led an effort by 40 international leaders calling on governments to stop the attacks on healthcare. They included former secretary of state Madeline Albright, Archbishop Emeritus of Cape Town Desmond Tutu, former Member of the European Parliament Marietje Schaake and former Secretary-General of the United Nations Ban Ki-moon among many others.

Organizations are also taking steps to protect themselves. In April, we announced that we were making AccountGuard, our threat notification service, available to health care and human rights organizations working on Covid-19. Since then 195 of these organizations have enrolled in the service and we now protect 1.7 million email accounts for health care-related groups. Any health care-related organizations that wish to enroll can do so here.

At a time when the world is united in wanting an end to the pandemic and anxiously awaiting the development of a safe and effective vaccine for Covid-19, it is essential for world leaders to unite around the security of our health care institutions and enforce the law against cyberattacks targeting those who endeavor to help us all. You can learn more about what Microsoft is doing to advance cybersecurity here.

Tags: COVID-19, cyberattacks, cybersecurity, Microsoft AccountGuard