We are taking new steps against broadening threats to democracy

blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

August 21, 2018

It's clear that democracies around the world are under attack. Foreign entities are launching cyber strikes to disrupt elections and sow discord. Unfortunately, the internet has become an avenue for some governments to steal and leak information, spread disinformation, and probe and potentially attempt to tamper with voting systems. We saw this during the United States general election in 2016, last May during the French presidential election, and now in a broadening way as Americans are preparing for the November midterm elections.

Broadening cyberthreats to both U.S. political parties make clear that the tech sector will need to do more to help protect the democratic process. Last week, Microsoft's Digital Crimes Unit (DCU) successfully executed a court order to disrupt and transfer control of six internet domains created by a group widely associated with the Russian government and known as Strontium, or alternatively Fancy Bear or APT28. We have now used this approach 12 times in two years to shut down 84 fake websites associated with this group. Attackers want their attacks to look as realistic as possible and they therefore create websites and URLs that look like sites their targeted victims would expect to receive email from or visit. The sites involved in last week's order fit this description.

We're concerned that these and other attempts pose security threats to a broadening array of groups connected with both American political parties in the run-up to the 2018 elections. That's why today we are expanding Microsoft's Defending Democracy Program with a new initiative called Microsoft AccountGuard. This initiative will provide state-of-the-art cybersecurity protection at no extra cost to all candidates and campaign offices at the federal, state and local level, as well as think tanks and political organizations we now believe are under attack. The technology is free of charge to candidates, campaigns and related political institutions using Office 365.

As a special master appointed by a federal judge concluded in the recent court order obtained by DCU, there is "good cause" to believe that Strontium is "likely to continue" its conduct. In the face of this continuing activity, we must work on the assumption that these attacks will broaden further. An effective response will require even more work to bring people and expertise together from across governments, political parties, campaigns and the tech sector.

An expansion of political targets

Last week's order transferred control of the six internet domains listed below from Strontium to Microsoft, preventing Strontium from using them and enabling us to more closely look for evidence of what Strontium intended to do with the domains. These six domains are listed here:

Importantly, these domains show a broadening of entities targeted by Strontium's activities. One appears to mimic the domain of the International Republican Institute, which promotes democratic principles and is led by a notable board of directors, including six Republican senators and a leading senatorial candidate. Another is similar to the domain used by the Hudson Institute, which hosts prominent discussions on topics including cybersecurity, among other important activities. Other domains appear to reference the U.S. Senate but are not specific to particular offices. To be clear, we currently have no evidence these domains were used in any successful attacks before the DCU transferred control of them, nor do we have evidence to indicate the identity of the ultimate targets of any planned attack involving these domains.

Microsoft has notified both nonprofit organizations. Both have responded quickly, and Microsoft will continue to work closely with them and other targeted organizations on countering cybersecurity threats to their systems. We've also been monitoring and addressing domain activity with Senate IT staff the past several months, following prior attacks we detected on the staffs of two current senators.

Despite last week's steps, we are concerned by the continued activity targeting these and other sites and directed toward elected officials, politicians, political groups and think tanks across the political spectrum in the United States. Taken together, this pattern mirrors the type of activity we saw prior to the 2016 election in the United States and the 2017 election in France.

Our new Microsoft AccountGuard initiative

AccountGuard will provide three services that will cover both organizational and personal email accounts:

1. **Threat notification across accounts.** The Microsoft Threat Intelligence Center will enable Microsoft to detect and provide notification of attacks in a unified way across both organizational and personal email systems. For political campaigns and other eligible organizations, when an attack is identified, this will provide a more comprehensive view of attacks against campaign staff. When verifiable threats are detected, Microsoft will provide personal and expedited recommendations to campaigns and campaign staff to secure their systems.
2. **Security guidance and ongoing education.** Officials, campaigns and related political organizations will receive guidance to help make their networks and email systems more secure. This can include applying multi-factor authentication, installing the latest security updates and guidance for setting up systems that ensure only those people who need data and documents can access them. AccountGuard will provide updated briefings and training to address evolving cyberattack trends.
3. **Early adopter opportunities.** Microsoft will provide preview releases of new security features on a par with the services offered to our large corporate and government account customers.

You can read a more complete description of Microsoft AccountGuard in today's blog by Tom Burt, the corporate vice president who heads Microsoft's Customer Security and Trust group.

Microsoft's Defending Democracy Program

Since we launched Microsoft's Defending Democracy Program in April, we have focused on four priorities: protecting campaigns from hacking, protecting voting and the electoral process, increasing political advertising transparency, and defending against disinformation campaigns. In the coming months, we will offer AccountGuard in additional countries, as we continue to invest in and evolve other aspects of the Defending Democracy Program.

Our Defending Democracy Program is an important piece of our work to protect customers and promote cyberdiplomacy around the world. While cybersecurity starts with Microsoft and other companies in the tech sector, it's ultimately a shared responsibility with customers and governments around the world. Together with our industry partners, we've launched the Cybersecurity Tech Accord, now endorsed by 44 leading tech companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace. And we will continue to call for stronger adherence to existing international norms and the creation of new international laws – like a Digital Geneva Convention.

As last week's court order and today's AccountGuard initiative reflect, we are committed not only to stronger principles and laws but stronger action as well.

A democracy requires vigilance

In 1787, as the American constitutional convention reached its conclusion in Philadelphia, Benjamin Franklin was asked as he departed Independence Hall what type of government the delegates had created. He famously replied, "A republic, if you can keep it."

We can only keep our democratic societies secure if candidates can run campaigns and voters can go to the polls untainted by foreign cyberattacks.

Democracy requires vigilance and at times action by citizens to protect and maintain it. No individual or company can hope to meet this imperative by itself. We all need to do our part. We're committed to doing our part by helping to protect candidates and campaigns in preserving their voices and votes no matter what party they support.

Tags: cybersecurity, Digital Crimes Unit, elections, Microsoft AccountGuard