New cyberattacks targeting U.S. elections

blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

September 10, 2020

In recent weeks, Microsoft has detected cyberattacks targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns, as detailed below. We have and will continue to defend our democracy against these attacks through notifications of such activity to impacted customers, security features in our products and services, and legal and technical disruptions. The activity we are announcing today makes clear that foreign activity groups have stepped up their efforts targeting the 2020 election as had been anticipated, and is consistent with what the U.S. government and others have reported. We also report here on attacks against other institutions and enterprises worldwide that reflect similar adversary activity.

We have observed that:

- Strontium, operating from Russia, has attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants

- Zirconium, operating from China, has attacked high-profile individuals associated with the election, including people associated with the Joe Biden for President campaign and prominent leaders in the international affairs community
- Phosphorus, operating from Iran, has continued to attack the personal accounts of people associated with the Donald J. Trump for President campaign

The majority of these attacks were detected and stopped by security tools built into our products. We have directly notified those who were targeted or compromised so they can take action to protect themselves. We are sharing more about the details of these attacks today, and where we've named impacted customers, we're doing so with their support.

What we've seen is consistent with previous attack patterns that not only target candidates and campaign staffers but also those they consult on key issues. These activities highlight the need for people and organizations involved in the political process to take advantage of free and low-cost security tools to protect themselves as we get closer to election day. At Microsoft, for example, we offer AccountGuard threat monitoring, Microsoft 365 for Campaigns and Election Security Advisors to help secure campaigns and their volunteers. More broadly, these attacks underscore the continued importance of work underway at the United Nations to protect cyberspace and initiatives like the Paris Call for Trust and Security in Cyberspace.

Strontium

Strontium is an activity group operating from Russia whose activities Microsoft has tracked and taken action to disrupt on several previous occasions. It was also identified in the Mueller report as the organization primary responsible for the attacks on the Democratic presidential campaign in 2016. Microsoft's Threat Intelligence Center (MSTIC) has observed a series of attacks conducted by Strontium between September 2019 and today. Similar to what we observed in 2016, Strontium is launching campaigns to harvest people's log-in credentials or compromise their accounts, presumably to aid in intelligence gathering or disruption operations. Many of Strontium's targets in this campaign, which has affected more than 200 organizations in total, are directly or indirectly affiliated with the upcoming U.S. election as well as political and policy-related organizations in Europe. These targets include:

- U.S.-based consultants serving Republicans and Democrats;
- Think tanks such as The German Marshall Fund of the United States and advocacy organizations;
- National and state party organizations in the U.S.; and
- The European People's Party and political parties in the UK.

Others that Strontium targeted recently include businesses in the entertainment, hospitality, manufacturing, financial services and physical security industries.

Microsoft has been monitoring these attacks and notifying targeted customers for several months, but only recently reached a point in our investigation where we can attribute the activity to Strontium with high confidence. MSTIC's investigation revealed that Strontium has evolved its tactics since the 2016 election to include new reconnaissance tools and new techniques to obfuscate their operations. In 2016, the group primarily relied on spear phishing to capture people's credentials. In recent months, it has engaged in brute force attacks and password spray, two tactics that have likely allowed them to automate aspects of their operations. Strontium also disguised these credential harvesting attacks in new ways, running them through more than 1,000 constantly rotating IP addresses, many associated with the Tor anonymizing service. Strontium even evolved its infrastructure over time, adding and removing about 20 IPs per day to further mask its activity.

We are also working with our customers to assist them in proactively hunting for these types of threats in their environments and have published additional detail and guidance on Strontium activity.

Zirconium

Zirconium, operating from China, has attempted to gain intelligence on organizations associated with the upcoming U.S. presidential election. We've detected thousands of attacks from Zirconium between March 2020 and September 2020 resulting in nearly 150 compromises. Its targets have included individuals in two categories.

First, the group is targeting people closely associated with U.S. presidential campaigns and candidates. For example, it appears to have indirectly and unsuccessfully targeted the Joe Biden for President campaign through non-campaign email accounts belonging to people affiliated with the campaign. The group has also targeted at least one prominent individual formerly associated with the Trump Administration.

Second, the group is targeting prominent individuals in the international affairs community, academics in international affairs from more than 15 universities, and accounts tied to 18 international affairs and policy organizations including the Atlantic Council and the Stimson Center.

Zirconium is using what are referred to as web bugs, or web beacons, tied to a domain they purchased and populated with content. The actor then sends the associated URL in either email text or an attachment to a targeted account. Although the domain itself may not have malicious content, the web bug allows Zirconium to check if a user attempted to access the site. For nation-state actors, this is a simple way to perform reconnaissance on targeted accounts to determine if the account is valid or the user is active.

Phosphorus

Phosphorus is an activity group operating from Iran that MSTIC has tracked extensively for several years. The actor has operated espionage campaigns targeting a wide variety of organizations traditionally tied to geopolitical, economic or human rights interests in the Middle East region. Microsoft has previously taken legal action against Phosphorus' infrastructure and its efforts late last year to target a U.S. presidential campaign. Last month, as part of our ongoing efforts to disrupt Phosphorus activity, Microsoft was again given permission by a federal court in Washington D.C. to take control of 25 new internet domains used by the Phosphorus. Microsoft has since taken control of these domains. To date, we have used this method to take control of 155 Phosphorus domains.

Since our last disclosure, Phosphorus has attempted to access the personal or work accounts of individuals involved directly or indirectly with the U.S. presidential election. Between May and June 2020, Phosphorus unsuccessfully attempted to log into the accounts of administration officials and Donald J. Trump for President campaign staff.

Bolstering Cybersecurity

We disclose attacks like these because we believe it's important the world knows about threats to democratic processes. It is critical that everyone involved in democratic processes around the world, both directly or indirectly, be aware of these threats and take steps to protect themselves in both their personal and professional capacities. We report on nation-state activity to our customers and more broadly when material to the public, regardless of the actor's nation-state affiliation. We are taking extra steps to protect customers involved in elections, government and policymaking. We'll continue to disclose additional significant activity in our efforts to defend democracy.

We also believe more federal funding is needed in the U.S. so states can better protect their election infrastructure. While the political organizations targeted in attacks from these actors are not those that maintain or operate voting systems, this increased activity related to the U.S. electoral process is concerning for the whole ecosystem. We continue to encourage state and local election authorities in the U.S. to harden their operations and prepare for potential attacks. But as election security experts have noted, additional funding is still needed, especially as resources are stretched to accommodate the shift in COVID-19-related voting. We encourage Congress to move forward with additional funding to the states and provide them with what they need to protect the vote and ultimately our democracy.

Tags: cyberattacks, cybersecurity, Defending Democracy Program, Election Security Advisors, ElectionGuard, Microsoft 365 for Campaigns, MSTIC, security