Recent cyberattacks require us all to be vigilant - Microsoft On the Issues

By Tom Burt

Published: 2019-10-04 · Archived: 2026-04-05 15:07:13 UTC

Today we're sharing that we've recently seen significant cyber activity by a threat group we call Phosphorus, which we believe originates from Iran and is linked to the Iranian government. We're sharing this for two reasons. First, it is important that we all – governments and private sector – are increasingly transparent about nation-state attacks and efforts to disrupt democratic processes. Second, while we have processes to notify customers about nation state activity and have AccountGuard to monitor accounts of campaigns and other associated organizations related to election processes in democracies around the world, publishing this information should help others be more vigilant and take steps to protect themselves.

In a 30-day period between August and September, the Microsoft Threat Intelligence Center (MSTIC) observed Phosphorus making more than 2,700 attempts to identify consumer email accounts belonging to specific Microsoft customers and then attack 241 of those accounts. The targeted accounts are associated with a U.S. presidential campaign, current and former U.S. government officials, journalists covering global politics and prominent Iranians living outside Iran. Four accounts were compromised as a result of these attempts; these four accounts were not associated with the U.S. presidential campaign or current and former U.S. government officials. Microsoft has notified the customers related to these investigations and threats and has worked as requested with those whose accounts were compromised to secure them.

Phosphorus used information gathered from researching their targets or other means to game password reset or account recovery features and attempt to take over some targeted accounts. For example, they would seek access to a secondary email account linked to a user's Microsoft account, then attempt to gain access to a user's Microsoft account through verification sent to the secondary account. In some instances, they gathered phone numbers belonging to their targets and used them to assist in authenticating password resets.

While the attacks we're disclosing today were not technically sophisticated, they attempted to use a significant amount of personal information both to identify the accounts belonging to their intended targets and in a few cases to attempt attacks. This effort suggests Phosphorus is highly motivated and willing to invest significant time and resources engaging in research and other means of information gathering. MSTIC works every day to track threat groups including Phosphorus so we can notify customers when they face threats or compromises and so that we can build our products to better defend against these threats.

As we've previously disclosed, our Digital Crimes Unit has also taken legal and technical steps to combat Phosphorus attacks and we continue to take these types of actions.

There are also a range of steps customers can take to help secure their consumer accounts. We strongly encourage all customers to enable two-step verification on their accounts which can be done in Account Security settings.

While there are a number of ways to enable this two-step verification, the most secure option is through a password-less solution like Microsoft Authenticator.

People can also periodically check their login history, and we recommend this for journalists, political campaigns staff, and others interested in assuring account security. These logs are made available through the Account Security Sign-In Activity tab. They are easy to read and look like this:


Screenshot of account security login information

Expanding any of these events in this tab will provide details on the device and IP address used to access the account in question. If any of the activity looks suspicious, you can notify Microsoft by clicking on the associated "Secure Your Account" link. If you detect suspicious activity, you should change your password and enable two-step verification. To better secure your Microsoft account, follow these tips for keeping your Microsoft account safe and secure.

While this advice relates to consumer accounts, we also provide a range of additional tools and advice to IT administrators to protect their corporate networks. A starting point for accessing these tools is here.

However, if you are part of a political campaign, a political party committee or an NGO or think tank working on issues related to democracy, you are eligible for Microsoft AccountGuard, an offering from our Defending Democracy Program, and can sign up here. There are currently 60,000 accounts in 26 countries protected by AccountGuard, which provides monitoring and unified threat notification across the Office 365 accounts you use for work and the personal accounts of your staff and others affiliated with your organization that opt-in for this protection. To date, we've made more than 800 notifications of attempted nation-state attacks to AccountGuard customers.

We hope all governments, companies and advocacy groups will consider joining the Paris Peace Call for Trust & Security in Cyberspace and that all companies will consider joining the Cybersecurity Tech Accord. These are two important initiatives that aim to keep the internet safer from the types of malign activity we're discussing today.

Tags: cybersecurity, Defending Democracy Program, Microsoft AccountGuard, The Digital Crimes Unit

---