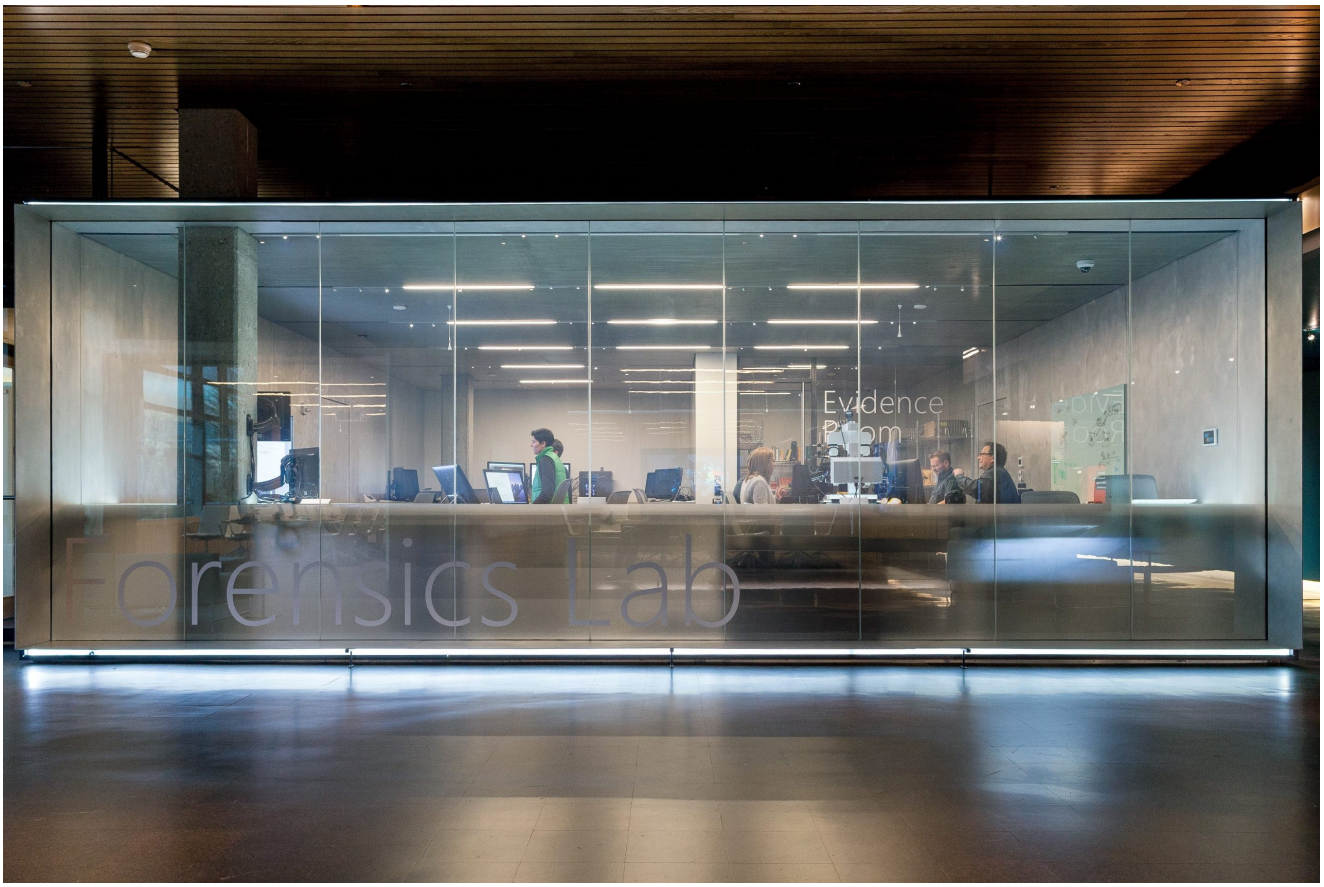
New steps to protect customers from hacking

blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/

March 27, 2019



Today, court documents were unsealed detailing work Microsoft's Digital Crimes Unit has executed to disrupt cyberattacks from a threat group we call Phosphorus – also known as APT 35, Charming Kitten, and Ajax Security Team – which is widely associated with Iranian hackers. Our court case against Phosphorus, filed in the U.S. District Court for Washington D.C., resulted in a court order enabling us last week to take control of 99 websites the group uses to conduct its hacking operations so the sites can no longer be used to execute attacks.

Microsoft's Digital Crimes Unit (DCU) and the Microsoft Threat Intelligence Center (MSTIC) have been tracking Phosphorus since 2013. Its activity is usually designed to gain access to the computer systems of businesses and government agencies and steal sensitive information. Its targets also include activists and journalists – especially those involved in advocacy and reporting on issues related to the Middle East.

Phosphorus typically attempts to compromise the personal accounts of individuals through a technique known as spear-phishing, using social engineering to entice someone to click on a link, sometimes sent through fake social media accounts that appear to belong to friendly

contacts. The link contains malicious software that enables Phosphorus to access computer systems.

Phosphorus also uses a technique whereby it sends people an email that makes it seem as if there's a security risk to their accounts, prompting them to enter their credentials into a web form that enables the group to capture their passwords and gain access to their systems.

Both attack methods employ the use of websites that incorporate the names of well-known brands, like Microsoft, to appear authentic. Websites registered and used by Phosphorus include, for example, outlook-verify.net, yahoo-verify.net, verification-live.com, and myaccount-services.net.

While we've used daily security analytics tracking to stop individual Phosphorus attacks and notify impacted customers, the action we executed last week enabled us to take control of websites that are core to its operations. Our work to track Phosphorus over multiple years and observe its activity enabled us to build a decisive legal case and execute last week's action with confidence we could have significant impact on the group's infrastructure.

The action we executed last week enabled us to take control of 99 websites and redirect traffic from infected devices to our Digital Crime Unit's sinkhole. The intelligence we collect from this sinkhole will be added to MSTIC's existing knowledge of Phosphorus and shared with Microsoft security products and services to improve detections and protections for our customers.

Throughout the course of tracking Phosphorus, we've worked closely with a number of other technology companies, including Yahoo, to share threat information and jointly stop attacks. We are grateful for their partnership. We also worked with each domain listing company listed in our suit prior to filing it and are grateful for their support and help in transferring the website domains registered by Phosphorus to us once a court order was granted. Our case against Phosphorus is similar to cases we've filed against another threat group called Strontium. We have used this approach 15 times to take control of 91 fake websites associated with Strontium. The legal filings in our case against Phosphorus can be found here.

Tags: cybersecurity, Digital Crimes Unit, Microsoft Digital Crimes Unit, Microsoft Threat Intelligence Center