Related news

cyberscoop.com/russia-temp-isotope-election-security-mandiant/

October 19, 2020

government

Industry alert pins state, local government hacking on suspected Russian group

Architecture and landmarks of Moscow, Russia. (Getty Images)
Written by Sean Lyngaas
Oct 19, 2020 | CYBERSCOOP
Suspected Russian hackers were behind multiple recent intrusions of U.S. state and local computer networks, according to an industry analysis obtained by CyberScoop.

The group responsible is known as TEMP.Isotope, according to a private advisory distributed by Mandiant, the incident response arm of security company FireEye. The alert notes that the same group has also been described as Energetic Bear, which multiple security firms have linked to Russia.

The FBI and the U.S. Cybersecurity and Infrastructure Security Agency on Oct. 9 publicized a hacking campaign in which attackers breached some “elections support systems,” or IT infrastructure that state and local officials use for a range of functions. Those systems are not involved in tallying votes, and the advisory from U.S. officials noted that there was no evidence that the "integrity of elections data has been compromised."

The federal advisory did not blame a particular hacking group for the activity, saying only that the campaign was the work of advanced persistent threat (APT) actors, or attackers linked to one or more foreign governments. It was unclear if any other APT groups, from other countries, were implicated in the advisory.

However, IP addresses used in the hacking were previously employed by the TEMP.Isotope group, according to Mandiant. The hackers exploited a recently revealed vulnerability in a protocol that Microsoft uses to authenticate its users. CISA on Sept. 18 ordered all federal civilian agencies to update their software to address the flaw because of the risk it carried.

The apparent Russian effort to breach state and local networks so close to the U.S. election has had federal officials and private sector experts focused on investigating and remediating the issue. Election officials were given additional information about the threat as part of a regular classified briefing on Friday, according to a CISA spokesperson.

From broad scanning to software exploits

The specific motive of the recent TEMP.Isotope activity is unclear. The hackers did not appear to be targeting state and local networks "because of their proximity to elections information," U.S. officials said in their advisory.

The activity described by the federal advisory started with broad scanning of vulnerable systems across federal, state and local networks, as well as critical infrastructure in the private sector, the CISA spokesperson said Monday.

"Once vulnerable systems are identified, the actors attempt to compromise the systems using a combination of techniques," the CISA statement continued. "While we are aware of limited instances where these efforts resulted in unauthorized access to IT systems used by elections officials, we have no evidence or reason to believe that election-related data like voter registration information, or voting machines or tabulation systems, have been affected."

Mandiant's advisory did not mention the Russian government.

FireEye itself has described TEMP.Isotope as a "Russian actor" and linked the group directly to a 2018 U.S. advisorythat blamed the Russian government for cyberattacks.

A FireEye spokesperson declined to comment on the advisory.

A group with a track record

TEMP.Isotope is perhaps best known for its aggressive campaigns to infiltrate energy companies in the U.S. and Europe. The alleged Russian hackers previously engaged in a years-long effort to breach U.S. energy firms,according to the aforementioned U.S.

government advisory and private sector cybersecurity specialists.

The cyberdefenses of state and local networks have improved from four years ago, when another set of Russian hackers, allegedly operating on behalf of the GRU military intelligence agency, probed IT systems across the country and compromised Illinois' voter registration database.

A spokesperson for the Russian Embassy in Washington, D.C., did not respond to a request for comment on the Mandiant advisory. Russia has repeatedly rejected allegations that it conducts cyberattacks.