AP finds hackers hijacked at least 195 Trump web addresses

November 5 2017, by Tami Abdollah

In this Jan. 19, 2017, file photo, then-President-elect Donald Trump and his wife Melania Trump and family wave at the conclusion of the pre-Inaugural "Make America Great Again! Welcome Celebration" at the Lincoln Memorial in Washington. Four years ago, well before the furor over allegations Moscow engaged in cybermeddling to help get Donald Trump elected, at least 195 web addresses belonging to Trump, his family or his business empire were hijacked by hackers who may have been operating out of Russia, The Associated Press has learned. The Trump Organization denied the domain names were ever compromised. But it was not until this week—after the Trump camp was asked about it by the AP—that the last of the tampered-with addresses were repaired. (AP Photo/David J. Phillip. File)

Four years ago, well before the furor over allegations Moscow meddled in the 2016 election that put Donald Trump in the White House, at least 195 web addresses belonging to Trump, his family or his business empire were hijacked by hackers possibly operating out of Russia, The Associated Press has learned.

The Trump Organization denied the domain names were ever compromised. But a review of internet records by the AP and cybersecurity experts shows otherwise. And it was not until this past week, after the Trump camp was asked about it by the AP, that the last of the tampered-with addresses were repaired.

After the hack, computer users who visited the Trump-related addresses were unwittingly redirected to servers in St. Petersburg, Russia, that cybersecurity experts said contained malicious software commonly used to steal passwords or hold files for ransom. Whether anyone fell victim to such tactics is unclear.

A further mystery is who the hackers were and why they did it.

The discovery represents a new twist in the Russian hacking story, which up to now has focused mostly on what U.S. intelligence officials say was a campaign by the Kremlin to try to undermine Democrat Hillary Clinton's candidacy and benefit Trump's.

It is not known whether the hackers who tampered with the Trump addresses are the same ones who stole Democratic officials' emails and embarrassed the party in the heat of the campaign last year. Nor is it clear whether the hackers were acting on behalf of the Russian government.

The affected addresses, or domain names, included donaldtrump.org, donaldtrumpexecutiveoffice.com, donaldtrumprealty.com and barrontrump.com. They were compromised in two waves of attacks in August and September 2013, according to the review of internet records.

The attacks took place as Trump was preparing to travel to Moscow for the Miss Universe pageant, which was held on Nov. 9, 2013, at a property owned by a wealthy Russian real estate developer.

Many of the addresses were not being used by Trump. Businesses and public figures commonly buy addresses for possible future use or to prevent them from falling into the hands of rivals or enemies. The Trump Organization and its affiliates own at least 3,300 in all.

According to security experts, the hackers hijacked the addresses by penetrating and altering the domain registration records housed at GoDaddy.com, a seller of web addresses.

Accounts at GoDaddy, like at any site that requires a user name and password, are often subject to malicious messages known as phishing attacks, which are designed to trick people to reveal that personal information to hackers.

Computer users who entered or clicked on one of those Trump addresses probably would have had no idea they were redirected to servers in Russia.

Within days after the AP asked the Trump Organization about the tampering, the affected web addresses were all corrected.

The White House referred questions to the Trump Organization. The FBI did not respond to a request for comment.

GoDaddy spokesman Nick Fuller said the company had no breaches of its system in 2013 and has measures in place to monitor for malicious activity. Fuller would not discuss any customers in particular.

Some cybersecurity experts said there is an outside chance the tampering was a probe—an attempt to test security for an eventual effort to gather information on Trump or his business dealings. But those experts were only guessing.

There was no evidence the hackers ultimately broke into server computers at the Trump Organization or other Trump interests.

"This is beyond me," said Paul Vixie, CEO of the San Mateo, California-based internet security company Farsight Security Inc. "I have simply never seen a benefit accrue from an attack of this kind. I'm at loss, unless it's a demonstration of capabilities."

Vixie said the Trump Organization's apparent failure to detect what was happening probably suggests inadequate cybersecurity at the company.

"There's no way something like this could go by in the Bloomberg empire without this being seen," Vixie said.