

Iranian Cyber-Attacks and the End of Support for Windows 7 and Windows Server 2008

Article By:

Sean Lawless

After the killing of Qassem Soleimani on January 3, 2020, by the U.S. government, the cybersecurity news industry has been abuzz about whether Iran will engage in cyber-terrorism, and if so, to what degree, as part of its pledge to strike back at the U.S. On January 5, Forbes reported that the first instance of Iranian cyber terrorism took place the day before. Hackers claiming to be associated with Iran defaced the home page of the Federal Depository Library Program website. The website was quickly taken down, but what do all this chatter and the possible increases of Iranian cyber-espionage mean for U.S. businesses?

The general consensus across multiple cybersecurity news outlets is that while Iran certainly has the capability to execute denial of service, malware, and phishing attacks, these types of attacks won't garner the press response and spectacle the Iranians might desire. However, notably absent from any of the reports I have read so far is the imminent end of security patching for both the Windows 7 and Windows Server 2008 operating systems by Microsoft on January 14. While most of the news reports anticipate an increase in 'noisy' cyber activity from Iranian and proxy hackers, there is little mention of how those hackers might exploit that upcoming end of support. Is it possible that the Iranians could leverage an ultimately unpatched vulnerability in Windows 7 or Server 2008 to achieve a disruption on a massive enough scale to garner the press attention they desire?

What is your organization doing to protect itself against such attacks? If you have not finished migrating from Windows 7 or Server 2008, extended security support is available from Microsoft for a fee. Are you considering geofencing Iranian and other Middle Eastern nation-states' internet address space from your network? Most modern 'nextgen' firewalls have such capabilities with updatable databases of a nation state's address space. Finally, are you educating your users and alerting them to be vigilant about suspicious emails and other phishing campaigns?

Copyright © 2025 Robinson & Cole LLP. All rights reserved.

National Law Review, Volume X, Number 9

Source URL: <https://natlawreview.com/article/iranian-cyber-attacks-and-end-support-windows-7-and-windows-server-2008>

