FBI working to 'burn down' cyber criminals' infrastructure

4 March 2020, by Alanna Durkin Richer

In this Dec. 9, 2019, file photo, FBI Director Christopher Wray speaks during an interview with The Associated Press in Washington. Wray is delivering the keynote address at a conference on cybersecurity on Wednesday, March 4, 2020, at Boston College. (AP Photo/Jacquelyn Martin, File)

To thwart increasingly dangerous cyber criminals, law enforcement agents are working to "burn down their infrastructure" and take out the tools that allow them carry out their devastating attacks, FBI Director Christopher Wray said Wednesday.

Unsophisticated cyber criminals now have the power to paralyze entire hospitals, businesses and police departments, Wray said during a conference on cybersecurity at Boston College. The ever-changing threat has forced law enforcement to get creative and target the dark web sites and other tools at hackers' disposal, he said.

"The reality is we are long past the days where we can fight this threat just one by one, one bad guy at a time ... one victim company at a time. We've got to figure out ways to tackle the cyber threat as a whole," Wray told the crowd of FBI agents, university officials and others on the Chestnut Hill campus.

The U.S. saw a nearly 40 percent increase in ransomware attacks between 2018 and 2019, said Joseph Bonavolonta, the head of the FBI's office in Boston. There was an even more dramatic uptick in such attacks in just the four states—Massachusetts, Maine, Rhode Island and New Hampshire—that the Boston office covers, he said.

"The threat of ransomware is continuing to grow and evolve and we are seeing a shift to more sophisticated, smaller scale ransomware campaigns, which maximizes the impact on the victims to extort higher ransoms," Bonavolonta told the conference.

Foreign actors, especially those from China, are also using cyber attacks to steal research from the defense contractors and other companies to "avoid the hard slog of innovation," Wray said, adding that the thieves are then turning around and using that information to compete against the very companies they ripped off.

"In effect, they are cheating twice over," Wray said.

Wray stressed the importance of indicting cyber criminals, even when they are outside the grasp of U.S. law enforcement in places like Russia, China or Iran, saying such criminals must be held accountable "no matter where they are."

Those countries "aren't the tourism destinations they used to be and one day they will slip up and when they do, we are there. Because the FBI has a broad reach and an even broader memory," Wray said.

Assistant Attorney General for National Security John Demers was among other speakers expected at the conference, which was organized by the FBI and the Masters in Cybersecurity Policy and Governance Program at Boston College's Woods

College of Advancing Studies.

© 2020 The Associated Press. All rights reserved.
This material may not be published, broadcast,
rewritten or redistributed without permission.
APA citation: FBI working to 'burn down' cyber criminals' infrastructure (2020, March 4) retrieved 30 November 2021 from https://techxplore.com/news/2020-03-fbi-cyber-criminals-infrastructure.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.