Microsoft's anti-hacking efforts make it an internet cop

August 22 2018, by Matt O'brien

In this Feb. 27, 2018, file photo Microsoft President and Chief Legal Officer Brad Smith, left, leaves the Supreme Court in Washington. Microsoft stands virtually alone among tech companies with its aggressive approach that uses U.S. courts to fight computer fraud and seize hacked websites back from malicious perpetrators. "What we're seeing in the last couple of months appears to be an uptick in activity," said Smith.(AP Photo/Andrew Harnik, File)

Intentionally or not, Microsoft has emerged as a kind of internet cop by

devoting considerable resources to thwarting Russian hackers.

The company's announcement Tuesday that it had identified and forced the removal of fake internet domains mimicking conservative U.S. political institutions triggered alarm on Capitol Hill and led Russian officials to accuse the company of participating in an anti-Russian "witch hunt."

Microsoft stands virtually alone among tech companies with an aggressive approach that uses U.S. courts to fight computer fraud and seize hacked websites back. In the process, it has acted more like a government detective than a global software giant.

In the case this week, the company did not just accidentally stumble onto a couple of harmless spoof websites. It seized the latest beachhead in an ongoing struggle against Russian hackers who meddled in the 2016 presidential election and a broader, decade-long legal fight to protect Microsoft customers from cybercrime.

"What we're seeing in the last couple of months appears to be an uptick in activity," Brad Smith, Microsoft's president and chief legal officer, said in an interview this week. Microsoft says it caught these particular sites early and that there's no evidence they were used in hacking.

The Redmond, Washington, company sued the hacking group best known as Fancy Bear in August 2016, saying it was breaking into Microsoft accounts and computer networks and stealing highly sensitive information from customers. The group, Microsoft said, would send "spear-phishing" emails that linked to realistic-looking fake websites in hopes targeted victims—including political and military figures—would click and betray their credentials.

The effort is not just a question of fighting computer fraud but of

protecting trademarks and copyright, the company argues.

One email introduced as court evidence in 2016 showed a photo of a mushroom cloud and a link to an article about how Russia-U.S. tensions could trigger World War III. Clicking on the link might expose a user's computer to infection, hidden spyware or data theft.

An indictment from U.S. special counsel Robert Mueller has tied Fancy Bear to Russia's main intelligence agency, known as the GRU, and to the 2016 email hacking of both the Democratic National Committee and Democrat Hillary Clinton's presidential campaign.

Some security experts were skeptical about the publicity surrounding Microsoft's announcement, worried that it was an overblown reaction to routine surveillance of political organizations—potential cyberespionage honey pots— that never rose to the level of an actual hack.

The company also used its discovery as an opportunity to announce its new free security service to protect U.S. candidates, campaigns and political organizations ahead of the midterm elections.

But Maurice Turner, a senior technologist at the industry-backed Center for Democracy and Technology, said Microsoft is wholly justified in its approach to identifying and publicizing online dangers.

"Microsoft is really setting the standards with how public and how detailed they are with reporting out their actions," Turner said.

In this May 11, 2017, file photo Alex Kipman, a technical fellow at Microsoft, stands on stage after speaking at the Microsoft Build 2017 developers conference in Seattle. Microsoft stands virtually alone among tech companies with its aggressive approach that uses U.S. courts to fight computer fraud and seize hacked websites back from malicious perpetrators. But in the process, the company is taking on a role that might look more like the job of government than a corporation. (AP Photo/Elaine Thompson, File)

Companies including Microsoft, Google and Amazon are uniquely positioned to do this because their infrastructure and customers are affected. Turner said they "are defending their own hardware and their own software and to some extent defending their own customers."

Turner said he has not seen anyone in the industry as "out in front and open about" these issues as Microsoft.

As industry leaders, Microsoft's Windows operating systems had long been prime targets for viruses when in 2008 the company formed its

Digital Crimes Unit, an international team of attorneys, investigators and data scientists. The unit became known earlier in this decade for taking down botnets, collections of compromised computers used as tools for financial crimes and denial-of-service attacks that overwhelm their targets with junk data.

Richard Boscovich, a former federal prosecutor and a senior attorney in Microsoft's digital crimes unit, testified to the Senate in 2014 about how Microsoft used civil litigation as a tactic. Boscovich is also involved in the fight against Fancy Bear, which Microsoft calls Strontium, according to court filings.

To attack botnets, Microsoft would take its fight to courts, suing on the basis of the federal Computer Fraud and Abuse Act and other laws and asking judges for permission to sever the networks' command-and-control structures.

"Once the court grants permission and Microsoft severs the connection between a cybercriminal and an infected computer, traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft," Boscovich said in 2014.

He said the process of taking over the accounts, known as "sinkholing," enabled Microsoft to collect valuable evidence and intelligence used to assist victims.

In the latest action against Fancy Bear, a court order filed Monday allowed Microsoft to seize six new domains, which the company said were either registered or used at some point after April 20.

Smith said this week the company is still investigating how the newly discovered domains might have been used.

A security firm, Trend Micro, identified some of the same fake domains earlier this year. They mimicked U.S. Senate websites, while using standard Microsoft log-in graphics that made them appear legitimate, said Mark Nunnikhoven, Trend Micro's vice president of cloud research.

Microsoft has good reason to take them down, Nunnikhoven said, because they can hurt its brand reputation. But the efforts also fit into a broader tech industry mission to make the internet safer.

"If consumers are not comfortable and don't feel safe using digital products," they will be less likely to use them, Nunnikhoven said.

© 2018 The Associated Press. All rights reserved.

Citation: Microsoft's anti-hacking efforts make it an internet cop (2018, August 22) retrieved 26 June 2024 from https://phys.org/news/2018-08-microsoft-anti-hacking-efforts-internet-cop.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.