Microsoft's cybercrime unit files first case

December 18 2013, by Janet I. Tu

When Microsoft opened its sleek new Cybercrime Center last month, the company said the center was designed to showcase some of its latest technologies and to bring together different units that work on fighting everything from malware to intellectual-property theft.

Now, Microsoft is filing its first case emerging from the work of the Cybercrime Center team, which works out of its new offices on the Redmond, Wash., campus. On Tuesday, Microsoft filed a civil lawsuit in the U. S. District Court of Western Washington against Sichuan Changhong Electric Co., a Sichuan, China-based manufacturer of household appliances such as refrigerators and TVs.

Microsoft is accusing Changhong of using product keys - a series of numbers and letters that a user enters into a computer in order to activate Microsoft software - that were stolen from organizations that had legitimately purchased licenses for the software.

Those organizations include a U.S. public university, a U.S. public-school district, a U.S.-based engineering company and an Asia-based semiconductor manufacturer, all unidentified in the suit.

Microsoft says it doesn't know how those product keys were stolen and believes that will be made clear during the discovery process.

Microsoft contends that, since 2011, Changhong's employees, contractors or other agents have activated numerous copies of Microsoft software products using stolen product-activation keys.

Representatives of Changhong could not immediately be reached for comment.

Microsoft believes it's the first time any company has used the Computer Fraud and Abuse Act to go after those allegedly stealing software product keys. The law prohibits unauthorized access to a protected computer system such as those used in interstate commerce.

The level of proof required under that law to show product keys were stolen would not have been possible even a few years ago, Microsoft says.

It's now possible, the company says, because of technological advances used in the field of cyberforensics - the gathering and analysis of digital evidence and data to prove cases.

The cybercrime team first got suspicious about eight months ago when they were looking into patterns involving a known stolen product key.

They traced the key back to an educational institution in the U.S. that had legitimately purchased licenses to use Microsoft's software.

The cyberforensics team then plotted onto maps where that organization's licenses were being activated. Those maps showed big spikes in activation attempts in places far from the U.S.

They then started looking for "a pattern under the map," said Zoe Krumm, a member of the cyberforensics team.

The team wanted to find persistent, systematic, intentional attempts to use stolen product keys to access Microsoft's servers.

But at that point the team didn't have the algorithms needed to show that

sort of pattern.

"You don't just shake the Excel tree and have all that come out at the bottom," said Donal Keating, another member of the cyberforensics team.

So they built the algorithms - ones specifically designed to show piracy behaviors.

In this case, those algorithms produced data that showed repeated attempts to activate product keys coming from computers registered to Changhong's domain, according to Microsoft.

Microsoft's analysis showed, for instance, that within short periods of time, computers controlled by Changhong had tried to activate different product keys for certain Microsoft programs, such as Office or Project. Some of the attempts failed, and the user kept trying until he or she succeeded with a key that Microsoft had not yet blocked.

"That's what I'm looking for," Krumm said. "They try multiple keys within minutes of each other until they find a pass."

Microsoft said in its lawsuit that its analysis also showed the activation attempts took place on "numerous devices controlled by Changhong" during regular business hours in China.

The data collected, along with data visualization tools and the work of data scientists and investigators, "allowed us to know when a company like Changhong has attempted over 2,000 times to activate unlicensed software with over 200 product keys," said Matt Lundy, Microsoft's assistant general counsel for the digital-crimes unit.

While the Computer Fraud and Abuse Act has been used commonly in

cases involving malware, "there's a good reason" the law has most likely not been used in stolen software-product key cases before, said Rob McKenna, former Washington state attorney general who's now a partner specializing in technology and intellectual property with law firm Orrick, Herrington & Sutcliffe.

"It's the proof problem - collecting the evidence and documenting that a computer used stolen license keys to gain unauthorized access to Microsoft servers " said McKenna, who is not working on this case but has been briefed on it by Microsoft. He also works with Microsoft on other cases.

Microsoft is seeking a jury trial and a judgment that would bar Changhong from using product keys that it hasn't purchased to access Microsoft's servers in the future.

It's also seeking an unspecified amount for damages.

Citation: Microsoft's cybercrime unit files first case (2013, December 18) retrieved 16 August 2024 from https://phys.org/news/2013-12-microsoft-cybercrime-1st-case.html