Ukraine police seize cash in raids on major ransomware gang

16 June 2021, by Jim Heintz and Frank Bajak

Credit: CC0 Public Domain

Ukrainian police have carried out nearly two dozen raids targeting alleged associates of a Russian-speaking ransomware gang it blamed for a half billion dollars in cyberattacks and extortion that hit the United States and South Korea especially hard.

A police statement on Wednesday said 21 raids were conducted on the homes of suspects affiliated with the Clop ransomware in Kyiv and elsewhere, with computer equipment and about 5 million hryna ($185,000) in cash seized.

Six defendants carried out attacks on U.S. and Korean companies—for which they face up to eight years in prison for violating computer crime and money-laundering laws, the statement said. It did not say whether any suspects were detained, and said the investigation was ongoing.

The most potent ransomware gangs operate with Kremlin tolerance, based out of reach of Western law enforcement. Russia neither prosecutes not extradites them. Trying to persuade its president, Vladimir Putin, to change that was a priority of U.S. President Joe Biden in their meeting Wednesday in Geneva. It's not clear whether Biden made any headway.

Video posted by the Ukrainian police showed Korean police taking part in this week's raids, where cash, cell phones and cars were also seized. The police statement said four Korean companies hit by the gang with the ransomware—which scrambles data that can only be unlocked with a software key obtained by paying the criminals—had paid ransoms. It said the gang targeted U.S. universities, including Stanford Medical School and the University of Maryland.

Wednesday's raid "is a continuation of the much more aggressive posture that law enforcement has taken against ransomware gangs this year," said analyst Allan Liska of the cybersecurity firm Recorded Future. "It really does feel like law enforcement has figured out how to attack the ransomware scourge, and hopefully, will slow down the attacks."

After last month's attack on the Colonial Pipeline affected fuel shipments to the U.S. East Coast, the White House began taking ransomware criminals as seriously as it does terrorists, and many are now lying low. The author of the Colonial attack went into hiding and a different group, Avaddon, suddenly announced its retirement. Cybersecurity analysts caution, however, that such retirements are not new and can be a ruse to thwart law enforcement while the criminals reconstitute and create new products with different brands.

And while some arrests have been made and ransomware infrastructure disabled in recent months, no kingpins have been snared.

Clop is among the more prolific ransomware gangs, known for extorting victims by threatening to

publish data stolen from them. It has published the names of 65 victims to its dark web extortion site since August, said Liska.

In some cases, Clop has extorted victims with data it may not have obtained directly but purchased instead from third party cyberthieves. It's what security researchers suspect happened in the case of the Universities of Colorado and Miami, the rail transport company CSX Corporation, the Canadian aircraft maker Bombardier and the prominent law firm Jones Day. That data was stolen in the hack of a software tool made by the California firm Accellion, used to manage large email attachments.

© 2021 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

APA citation: Ukraine police seize cash in raids on major ransomware gang (2021, June 16) retrieved 15 October 2021 from https://techxplore.com/news/2021-06-ukraine-uncovers-million-hacking.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.