US recovers over half of ransom paid to pipeline hackers

7 June 2021, by Paul Handley

Russia-based ransomware hackers forced the shutdown of the largest fuel network in the eastern United States, run by Colonial Pipeline.

The US Justice Department announced Monday that it had recovered more than half of the $4.4 million paid by Colonial Pipeline to Russia-based ransomware extortionists Darkside, who had forced the shutdown of a major fuel network.

"Today, we turned the tables on Darkside by going after the entire ecosystem that fuels ransomware and digital extortion attacks, including criminal proceeds in the form of digital currency," said Deputy Attorney General Lisa Monaco.

The seizure came one month after the group gave the US government a security scare by breaking into the computer systems of Colonial and forcing the shutdown of its 5,500 mile (8,850 kilometers) pipeline serving much of the eastern United States.

The cyberattack caused short-term fuel shortages and drew attention to the broader threat that the burgeoning ransomware "industry" posed to essential infrastructure and services.

The Justice Department said the US Federal Bureau of Investigation was able to track the 75 bitcoin Colonial paid in ransom—$4.4 million at the time—as it moved through multiple anonymous transfers.

Eventually it was able to seize from a cryptocurrency wallet 63.7 bitcoin, which due to the digital currency's fall over the past month, was only worth $2.3 million on Monday.

Colonial boss Joseph Blount thanked the FBI for its "swift work and professionalism," saying the company had "quietly and quickly" contacted its agents when the attack was detected on May 7.

"Holding cyber criminals accountable and disrupting the ecosystem that allows them to operate is the best way to deter and defend against future attacks," he said in a statement.

It was the first seizure of a paid ransom by the Justice Department's new Ransomware and Digital Extortion Task Force, tasked to go after the so-called "ransomware as a service" industry that has extracted hundreds of millions of dollars from targets like schools, hospitals, local governments, and businesses over the past several years.

US President Joe Biden has said he is "looking closely" at possible retaliation against Russia over their alleged involvement in the ransomware hacking of global meat processing giant JBS.

"Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises," said Monaco.

Monaco gave no details on how the money was recovered from Darkside, but analysts believe it could have involved both FBI investigators and possibly the US military's offensive cyber warfare operations.

One week after Colonial was forced to shut its operations on May 7, an online comment believed to be by Darkside operator "Darksupp" admitted that it had lost control of part of its operating infrastructure, including payment and other servers, and that ransom payments had been removed from its servers.

Its dark-web site also went down.

Cyber security experts say many of the independent ransomware extortionists appear to be located in Russia or former Soviet satellites in eastern Europe.

The attacks have grown so frequent that the issue has been elevated in seriousness in the Justice Department to the level of terror attacks.

On May 31 the US subsidiary of the world's largest meat processing group, Brazil-based JBS, said its systems had been hacked by ransomware extortionists, whom the US government tied to Russia.

Last week the company that operates the ferries between the Massachusetts mainland and the popular tourist destinations Nantucket and Martha's Vineyard was also hit, just as the summer season was opening.

After the JBS attack, last week US President Joe Biden said he was "looking closely" at possible retaliation over the cyberattacks.

The issue is likely to figure in Biden's summit with Russian President Vladimir Putin in Geneva later this month.

© 2021 AFP

APA citation: US recovers over half of ransom paid to pipeline hackers (2021, June 7) retrieved 20 October 2021 from https://techxplore.com/news/2021-06-recovered-ransom-payment-pipeline-hack.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.