

EXPLAINER: Why ransomware is so dangerous and hard to stop

June 3 2021, by Frank Bajak



In this Oct. 12, 2020 file photo, a worker heads into the JBS meatpacking plant in Greeley, Colo. A weekend ransomware attack on the world's largest meat company is disrupting production around the world just weeks after a similar incident shut down a U.S. oil pipeline. The White House confirms that Brazil-based meat processor JBS SA notified the U.S. government Sunday, May 30, 2021, of a ransom demand from a criminal organization likely based in Russia. Credit: AP Photo/David Zalubowski, File

Recent high-profile "ransomware" attacks on the world's largest meat-packing company and the [biggest U.S. fuel pipeline](#) have underscored how gangs of extortionist hackers can disrupt the economy and put lives and livelihoods at risk.

Last year alone in the U.S., [ransomware](#) gangs hit more than 100 federal, state and municipal agencies, upwards of 500 health care centers, 1,680 educational institutions and untold thousands of businesses, according to the cybersecurity firm Emsisoft. Dollar losses are in the tens of billions. Accurate numbers are elusive. Many victims shun reporting, fearing the reputational blight.

More recent known targets include a Massachusetts ferry operator, the [Irish health system](#) and the [Washington, D.C., police department](#). But the broadly disruptive hacks on Colonial Pipeline in the U.S. in May and Brazilian meat processor JBS SA this week have drawn close attention from the White House and other world leaders, along with heightened scrutiny of the foreign safe havens where cybercriminal mafias operate.

WHAT IS RANSOMWARE? HOW DOES IT WORK?

Ransomware scrambles the target organization's data with encryption. The criminals leave instructions on infected computers for negotiating ransom payments. Once paid, they provide decryption keys for unlocking those files.

Ransomware crooks have also expanded into data-theft blackmail. Before triggering encryption, they quietly copy sensitive files and threaten to post them publicly unless they get their ransom payments. That can present problems even for companies that diligently back up their networks as a hedge against ransomware, since refusing to pay can incur costs far greater than the ransoms they might have negotiated.

HOW DO RANSOMWARE GANGS OPERATE?

The criminal syndicates that dominate the ransomware business are mostly Russian-speaking and operate with near impunity out of Russia and allied countries. Though barely a blip three years ago, the syndicates have grown in sophistication and skill. They leverage dark web forums to organize and recruit while hiding their identities and movements with sophisticated tools and cryptocurrencies like Bitcoin that make payments—and their laundering—harder to track.

Some top ransomware criminals fancy themselves software service professionals. They take pride in their "customer service," providing "help desks" that assist paying victims in file decryption. And they tend to keep their word. They have brands to protect, after all.

The business is now highly specialized. An affiliate will identify, map out and infect targets using ransomware that is typically "rented" from a ransomware-as-a-service provider. The provider gets a cut of the payout; the affiliate normally takes more than three-quarters.

Other subcontractors may also get a slice. Those can include the authors of the malware used to break into victim networks and the people running so-called "bulletproof domains" behind which the ransomware gangs hide their "command-and-control" servers. Those servers manage the remote sowing of malware and data extraction ahead of activation, a stealthy process that can take weeks.



Tanker trucks are parked near the entrance of Colonial Pipeline Company Wednesday, May 12, 2021, in Charlotte, N.C. The operator of the nation's largest fuel pipeline has confirmed it paid \$4.4 million to a gang of hackers who broke into its computer systems. That's according to a report from the Wall Street Journal. Colonial Pipeline's CEO Joseph Blount told the Journal that he authorized the payment after the ransomware attack because the company didn't know the extent of the damage. Credit: AP Photo/Chris Carlson

WHY DO RANSOMS KEEP CLIMBING? HOW CAN THEY BE STOPPED?

Colonial Pipeline [confirmed that it paid \\$4.4 million](#) to the gang of hackers who broke into its computer systems last month.

The FBI discourages paying ransoms, but a public-private task force including tech companies and U.S., British and Canadian crime agencies says it would be wrong to try to ban ransom payments altogether. That's largely because "ransomware attackers continue to find sectors and elements of society that are woefully underprepared for this style of attack."

The task force recognizes that paying up can be the only way for an afflicted business to avoid bankruptcy. Worse, the sophisticated cybercriminals often have done their research and know a victim's cybersecurity insurance coverage limit. They've been known to mention it in negotiations.

That degree of criminal savvy helped drive average ransom payments to more than \$310,000 last year, up 171% from 2019, according to Palo Alto Networks, a task force member.

WHAT'S BEING DONE ABOUT IT?

President Joe Biden signed an executive order in May meant to strengthen U.S. cybersecurity defenses, mostly in response to Russia's hacking of federal agencies and interference in U.S. politics. But headline-grabbing ransomware attacks on private companies have started to dominate the cybersecurity conversation as Biden prepares for a June 16 summit with his Russian counterpart Vladimir Putin.

White House principal deputy press secretary Karine Jean-Pierre said this week that the ransom demand of JBS meat came from a "criminal organization likely based in Russia." She said the White House "is engaging directly with the Russian government" and "delivering the message that responsible states do not harbor ransomware criminals."

The new industry task force set up to combat ransomware says it's

important to have concerted diplomatic, legal and law enforcement cooperation with key allies.

Ransomware developers and their affiliates should be named and shamed—though they're not always easy to identify—and regimes that enable them punished with sanctions, its report urges.

It calls for mandatory disclosure of ransom payments and a federal "response fund" to provide [financial assistance](#) to victims in hopes that, in many cases, it will prevent them from paying ransoms. And it wants stricter regulation of cryptocurrency markets to make it more difficult for criminals to launder ransomware proceeds.

The task force also calls for something potentially controversial: amending the U.S. Computer Fraud and Abuse Act to let private industry actively block or limit online criminal activity, including of botnets, the networks of hijacked zombie computers that ransomware criminals use to sow infections.

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

Citation: EXPLAINER: Why ransomware is so dangerous and hard to stop (2021, June 3) retrieved 8 April 2024 from

<https://techxplore.com/news/2021-06-ransomware-dangerous-hard.html>

<p>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.</p>
--