

A sign of ransomware growth: Gangs now arbitrate disputes

February 9 2022, by Alan Suderman



The sign outside the National Security Administration (NSA) campus in Fort Meade, Md., June 6, 2013. A new report says cyber criminal gangs are getting increasingly adept at hacking and becoming more professional. The report by the United States, Australia and the United Kingdom paints a bleak picture of ransomware trends in 2021, with ransomware operators even setting up an arbitration system to resolve payment disputes among themselves. Credit: AP Photo/Patrick Semansky, File

Cyber criminal gangs are getting increasingly adept at hacking and becoming more professional, even setting up an arbitration system to resolve payment disputes among themselves, according to a new report by the United States, Australia and the United Kingdom that paints a bleak picture of ransomware trends.

Ransomware gangs, which hack targets and hold their data hostage through encryption, caused widespread havoc last year with high-profile attacks on the world's largest meat-packing company, the biggest U.S. fuel pipeline and other targets. Western governments have pledged to crack down on the cyber criminals, who operate largely in and around Russia, but have little to show in the way of progress.

The [new report on 2021 ransomware trends](#) highlights the growing maturity and specialization of the ransomware market, with independent operators filling a lucrative niche market. Specialists now range from the hackers who can break into networks or develop ransomware to the nontechnical operators who negotiate payments with victims. The United Kingdom's National Cyber Security Centre said it's seen some ransomware gangs offer a 24/7 help center to victims to expedite ransom payments and restore encrypted data.

There's even money to be made by arbitrators who can settle payment disputes among the various ransomware criminals, according to the report.

"The criminal marketplace is incredibly, incredibly efficient and constantly evolving," said John Hultquist, vice president of intelligence analysis at the cybersecurity firm Mandiant. "The fact that they can operate like this, it's evidence of our failure to get a good grip on this problem."

The report also describes the growing technical skills of ransomware

gangs, which have been able to target cloud infrastructure—often touted as a safer alternative to storing data locally—and developed code to stop industrial processes. U.S. authorities said they'd seen ransomware attacks involving 14 out of 16 designated critical infrastructure sectors, including the defense industrial base, agriculture and information technology sectors.

"When critical infrastructure is held at risk by foreign hackers operating from a safe haven in an adversary country, that's a national security problem," National Security Agency Cybersecurity Director Rob Joyce said in a statement, adding that addressing ransomware is a "significant focus" of the NSA.

The joint report was issued Wednesday by the FBI, the NSA and the Cybersecurity and Infrastructure Security Agency in the U.S. as well as the United Kingdom's National Cyber Security Centre and the Australian Cyber Security Centre.

The report said that after major highly disruptive hacks on the Colonial Pipeline in the U.S. in May and on Brazilian meat processor JBS SA in June, "ransomware groups suffered disruptions from U.S. authorities in mid-2021" and have targeted midsize victims to reduce scrutiny.

But the UK and Australian authorities said they'd not seen any similar trend in their countries. Kaspersky Labs reported in December that ransomware-related incidents in 2021 accounted for 47% of its global response, up from 38% the previous year. In the U.S., however, targeted ransomware attacks that its intelligence network detected were down 33% in 2021 compared with the previous years. That compares with a 30% rise globally.

In the past month, ransomware victims have included operators of [maritime fuel depots](#) in Belgium and Germany and media outlets in

Portugal. A cyberattack on the [wireless provider Vodafone](#) in Portugal this week had all the hallmarks of ransomware, though the company's CEO for Portugal said it received no [ransomware](#) demand.

© 2022 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: A sign of ransomware growth: Gangs now arbitrate disputes (2022, February 9)
retrieved 9 April 2024 from
<https://techxplore.com/news/2022-02-ransomware-growth-gangs-disputes.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>
--