TechXplore

The increase in ransomware attacks during the COVID-19 pandemic may lead to a new internet

June 16 2021, by Michael Parent and David R. Beatty

Credit: Pixabay/CC0 Public Domain

Make no mistake: We are also in the midst of a digital pandemic of ransomware attacks. The recent ransomware attacks on Colonial Pipeline and JBS U.S. Holdings Inc.—the world's largest meat processors—underscore the growing brazen nature of organized, deliberate attacks on increasingly significant targets, and our chronic inability to defend against them.

What we need is a new internet. The old one is broken.

Origins of the internet

Today's internet originated from the Advanced Research Projects Agency Network (ARPANET) in the late 1960s—a conglomerate of research institutions connecting military, political and industrial actors during the Cold War in the United States. It allowed for secure communications in case of conflict, and to facilitate research and development through electronic sharing of information. It was a closed, tightly controlled, highly secure, invitation-only network.

The invention of the World Wide Web (WWW) by Tim Berners-Lee in 1990 led to the browser-based internet that we know today. The WWW introduced, and advocated for, an open, inclusive, universal and unconstrained mode for networks to communicate with each other. It introduced the notion of hyperlinks that a user could simply click on and be transported to a new web page on a separate network. This was the start of the unregulated, user-driven, content-rich internet.

The paradox of the internet is that it was born, has grown and exists in an environment where control and access have been in constant tension and conflict.

The rise of ransomware

Cybercrime is a growing, highly successful and profitable industry. It is estimated by industry that cybercrime costs will grow by 15 percent per year to reach US$10.5 trillion by 2025: the third greatest "economy" in the world, after those of the U.S. States and China.

A big part of this is ransomware, multi-pronged attacks capturing an organization's data and systems. Since the start of the pandemic, ransomware attacks have increased by nearly 500 percent since the start of the COVID-19 pandemic.

The average ransom payment has also continued to climb, up 43 percent from the last quarter of 2020 to an average of over US$200,000. What is especially insidious about these attacks is that a ransom demand is often accompanied by a breach and extraction of company data, and a concurrent extortion threatening to release this data unless additional payments are made.

In the first quarter of 2021, over three-quarters of ransomware attacks were tied to such a threat.

Criminals have also evolved to become increasingly systemic. The recent attack on Colonial Pipelines by the hacker collective DarkSide exemplifies this. Like their state-sponsored counterparts, criminal collectives have created virtual organizations and enacted focus strategies targeting specific sectors and companies. They have infinite resources, skills and patience. They are playing a long game where targets are identified, carefully reconnoitered and only acted upon when the maximum value can be extracted.

CNA Financial was attacked in late March, and paid a ransom of US$40 million—one of the biggest payments on record. The hackers were apparently interested in obtaining access to CNA's client database not only to blackmail the company itself, but to identify clients that had purchased cyberinsurance with a ransomware payment rider to identify the most lucrative targets. DarkSide are also selling ransomware packs to other hackers—Ransomware-as-a-Service (RaaS) is becoming a growing profit center.

The new old internet

Legislators have, predictably, responded to these attacks. U.S. President Joe Biden has directed federal agencies to bring all of their resources to bear on dealing with digital disruptions. The Department of Homeland Security is developing a set of mandatory rules for how pipelines, and likely other infrastructure providers, will need to safeguard their assets.

While a good first step, it will not be enough, and we will continue to react, to be behind the attack curve.

Intranets—closed, proprietary networks—might hold the key to solving this threat.

We foresee a new internet emerging, with two distinct sides. On one side, we'll have the wholly unfiltered, minimally regulated, Wild West internet that anyone can access.

On the other side, we might see the evolution of what could be called the "World Wide Intranet," that is, widely accessible but tightly controlled websites with stringent access controls to prevent criminal activity, much like the closed corporate intranets that gained popularity two decades ago.

Responsive security

Large online merchants like Amazon, the government, health-care providers or other large organizations will no longer tolerate criminal assaults on their and their stakeholders' data and resources. As such, as security measures like multi-factor authentification evolve, they will increasingly be adopted by these organizations and passed onto consumers as a condition of access.

As a society, we accept controls when the cost of not having them becomes greater than the restrictions they impose. We see this trend as an inevitable consequence of the growing security threats affecting not only networks but the individuals that transact with them.

By 2025, the world will store 200 Zettabytes (one trillion gigabytes) of data. The accompanying growth in transactions leaves us no other choice but to tighten identity and access controls.

One pathway might divide the web into one open, but inherently risky, internet and one closed, controlled, regulated and inherently untrusting one where security and privacy dominate.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: The increase in ransomware attacks during the COVID-19 pandemic may lead to a new internet (2021, June 16) retrieved 19 April 2024 from https://techxplore.com/news/2021-06-ransomware-covid-pandemic-internet.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.