The New York Times

NONFICTION

Who You Gonna Call? The Ransomware Hunting Team.

In their new book, Renee Dudley and Daniel Golden explain how a ragtag band of international tech nerds have defended the defenseless against cybercrime.

Credit...Stephanie Keith/Reuters

By Josephine Wolff
Oct. 24, 2022

THE RANSOMWARE HUNTING TEAM: A Band of Misfits' Improbable Crusade to Save the World From Cybercrime, by Renee Dudley and Daniel Golden

---

In May, the president of Costa Rica, Rodrigo Chaves, announced that the nation was "at war" with the Russia-based criminal gang Conti, which had infected 27 of the country's government institutions with ransomware and demanded $20 million to restore the encrypted data and computer systems. If entire countries can be brought to their knees by ransomware, then so too can cities, hospitals, individuals and schools, among many other entities. And for all of Chaves's rhetoric, the battles to defend these victims against ransomware are fought primarily by private companies and individuals, not by government agencies or militaries.

In "The Ransomware Hunting Team," the ProPublica journalists Renee Dudley and Daniel Golden profile several of those individuals, describing an informal, "invitation-only" coalition of roughly one dozen malware experts who work to decrypt victims' files and restore their computer systems so they don't have to succumb to extortion. The

members of the self-titled Ransomware Hunting Team are spread out across the United States and Europe. They communicate and coordinate their efforts via a private Slack channel as they scour source code to try to reverse-engineer decryption keys and recover the victims' data. Sometimes that turns out to be impossible, if the criminals have used strong enough algorithms and implemented them properly. But sometimes the perpetrators take shortcuts that enable the figures at the center of Dudley and Golden's story — security researchers like Michael Gillespie and Fabian Wosar — to come to the rescue.

Doing that work ("Or shall I call it a form of art?" one ransomware hunter muses) comes with significant costs, many of them personal. Dudley and Golden dig deeply into the emotional and financial tolls on people like Gillespie, who insists on offering his services to victims at no charge, only to end up struggling to pay his bills and fighting with his wife over his round-the-clock obsession with generating ransomware decryption keys, a process that consumes so much computing power it slows down his wife's avatars while she's playing the Sims.

But the larger costs of reverse-engineering ransomware lie in providing cybercriminals with real-time feedback about how to make their programs harder to crack. Any attempt by the ransomware hunters to publicize their findings for the benefit of future victims inevitably alerts these bad actors to the flaws in their own designs.

Dudley and Golden do a brilliant job of tracing the back-and-forth between attackers and defenders, like the little taunts the criminals embed in their programs after earlier versions are thwarted. After Wosar decrypts one program, its authors (a group called Apocalypse) fix the vulnerability he identified in a new variant named "Fabiansomware," encoded with a dare to "Crack me." His other nemeses leave messages in their source code ranging from "FWosar you are the man" to "If you crack this version then I will start taking heroin!"

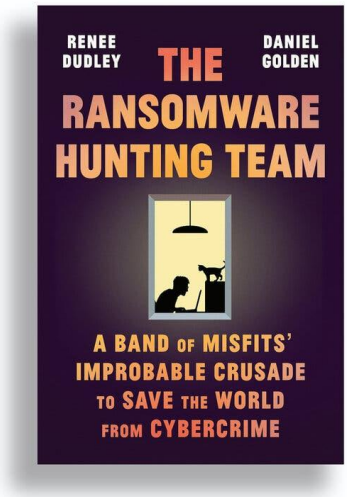
Even as they draw out these competitive and sometimes comical dynamics, Dudley and Golden are highly attuned to the havoc ransomware can wreak. They introduce us to a self-employed photographer in Manila who in 2019 lost access to hundreds of thousands of photos and videos he'd kept over five years, and a sixth-grade teacher in Maryland who in 2020 had to read "The Maze Runner" aloud to her students because all of her lesson plans had been frozen. Most tragically, they tell the story of a woman whose newborn daughter suffered severe brain damage because a ransomware attack prevented hospital obstetricians from detecting fetal distress. The baby later died.

A recurring theme across the book is the indifference and incompetence of government, particularly in America. Dudley and Golden note that when the city of Baltimore was hit by a ransomware attack in 2019, the Department of Homeland Security couldn't decide if it was their job to respond. Comparing the F.B.I., unfavorably, to the Dutch High Tech Crime Unit (the police team of tech-savvy officers who fight cybercrime), the authors note that the American bureau's technical experts are often looked down upon by their co-workers, one of whom nicknames them "dolphins" because they are "highly intelligent and can't communicate with humans."

But the book leaves other potential legal and regulatory defenses against ransomware underexplored, such as systematic targeting of cryptocurrency exchanges, botnet operators, hosting providers and internet service providers that facilitate ransomware and could potentially be leveraged to disrupt these attacks.

The book begins with an epigraph from Rudyard Kipling: “If once you have paid him the Dane-geld / You never get rid of the Dane.” But Dudley and Golden stop short of criticizing the victims who do pay ransoms, and the insurers who often cover those payments. In fact, their tone is much gentler than Dudley’s 2019 accusation that insurers are “both fueling and benefiting from” ransomware. The book is, however, openly critical of companies like Proven Data Recovery and MonsterCloud that purport to be able to retrieve victims’ data themselves, but often end up just paying the ransoms without telling their clients.

Instead of focusing on policy and institutional shortcomings, Dudley and Golden are most interested in the characters at the center of this fight. “Within the ranks of both hunters and hackers,” they write, “are self-taught, underemployed tech geeks who sometimes lack social graces, like video games and are familiar with some of the same movies.” The book offers lively portraits of these people — invoking Gillespie’s bachelor party, where “guests shot up worn-out computers with guns,” and Wosar’s habit of watching “sad, romantic” movies like “The Fault in Our Stars” or “Eternal Sunshine of the Spotless Mind” while he works — as it traces the evolution of ransomware into a more professionalized business for organized cartels. Unfortunately, that professionalization and its attendant resources are catapulting many strains of modern ransomware beyond the reach of the Ransomware Hunting Team.



THE RANSOMWARE HUNTING TEAM: A Band of Misfits’ Improbable Crusade to Save the World From Cybercrime | By Renee Dudley and Daniel Golden | 355 pp. | Farrar, Straus & Giroux | $30

Josephine Wolff is an assistant professor of cybersecurity policy at the Tufts Fletcher School of Law and Diplomacy and the author of “You’ll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches.” @josephinecwolff