

**CSM WRITER’S KIT**

TERMS & CONDITIONS

I understand that by submitting my article to Cyber Security Magazine, that this article will become copyright by Cyber Security Magazine and published online either on the website or eMagazine or both. Cyber Security Magazine will have exclusive ownership to this content. YOU CANNOT PUBLISH THIS ARTICLE ANYWHERE ELSE.

With this submission, I confirm that the content was created by me, that I have full rights and ownership to transfer it to Cyber Security Magazine and that I indemnify Cyber Security Magazine against any copyright claims on this content.

While I am not receiving compensation for my submission, I am allowed to reference my work as a guest writer for Cyber Security Magazine and add a link back to my email, personal web page or company website.

**An article should be added directly to this Word file below and the content should be in the following format:**

**The main title**

* Text Content
* About the Author (please include Author’s photo along with the Bio)

**Please include at least 2-3 images within article (to this Word file), if possible larger photos in higher resolution.**

**An Example:**

# The Frightening Trajectory Of Ransomware

AS THE AMERICAN ECONOMY REOPENS – IT’S TIME TO DO SOMETHING

**by Rob Cheng, CEO of PC Matic**

**Ransomware, the malicious software that encrypts user data then demands a ransom in exchange for a decryption key, has taken the nation by storm.** As the American economy begins to reopen, the frequency of ransomware attacks will once again skyrocket.  It’s time to do something.

During a recent meeting with the  FBI’s ransomware team, one of their ransomware analysts pushed over a report about a new threat. In addition to encrypting files, and demanding payment in crypto currency, the virus copies the files to a foreign server. If the ransom is not paid, the virus leaks the stolen data to the dark web for sale to cyber criminals.

The virus, known as Sodinokibi, infected Travelex, one of world’s largest foreign exchange banks, and the New York airport system with this ominous note:

“This is a small part of what we have. If there are no movements, we will sell the remaining, more important and interesting commercial and personal data to third parties including financial details.”

But the worst part?  Sodinokibi was just the beginning.  Since it’s release earlier this year, new ransomware threats like Maze have copied the model of infiltrate, encrypt, steal, and extort.  These attacks are successful in targeting businesses small and large, including its latest victim, multinational corporation, Cognizant.



**The FBI, perhaps not strongly enough, recommends that ransom payments be avoided at all costs with the rationale that the more ransoms paid, the greater the future attacks.** The reality is that many individuals and organizations ignore the FBI warnings and fork over hundreds of thousands of dollars if not millions to expediently restore operations and avoid embarrassment and public scrutiny.

And there is that ugly word, embarrassment, which drives more of our behavior than we care to admit. The new ransomware model threatens our privacy and safety with a clock ticking to make immediate payment to faceless cyber criminals. Even with the FBI’s advice ringing in our heads, as a society, people are going to pay. If embarrassment was driving behavior before Sodinokibi, the cyber criminals have hit the mother load, and ransom payments will flow out of the country like a river.

The latest ransomware model changes the economics of ransomware. Prior to Sodinokibi, the data was inaccessible, but the victim was still the owner of the information. Now, the victim has lost control of the security and dissemination of the information. The anonymous, never- to-be-known, cyber criminals have automated stealing and breaching our most important and private data sets.

## The trajectory of ransomware is frightening

In 2019 we saw an acceleration in infections in cities, counties, police departments and public schools. These are the public infections. More concerning are the infections that don’t make the news where the ransoms are paid quickly and quietly. The suits at publicly traded companies embarrass more easily than the rest of us, and a few million dollar extortion is a burp on their quarterly profit and loss statement. Wall Street won’t blink an eye.

Sodinokibi, Maze, and similar ransomware variants have begun pouring accelerant onto an already escalating ransomware fire. America’s aggregate response to the growing danger of ransomware has been lackadaisical at best.

Since the dawn of the personal computer, there has been a silent war waged between malware makers and the antivirus software designed to protect from malicious programs. Over the last four decades, a technical gap continues to grow between the technologies used to infect and those to protect. Sodinokibi has been viewed as an important technical advancement for the enemy.