IMA HIGHER EDUCATION
PROPERTY & CASUALTY INSURANCE
AND RISK MANAGEMENT PROGRAM

ENDORSED BY
THE COALITION FOR COLLEGE COST SAVINGS

HOW THE RYUK RANSOMWARE STOLE CHRISTMAS

THE LITTLE GREEN MONSTER LURKING IN YOUR COMPUTER

"It was the night before Christmas and all through the house, not a creature was stirring, not even a mouse"... the administrators were all nestled in their bed, while the Ryuk ransomware started messing with their head. This Christmas Eve, a sophisticated malware program sent from overseas locked up an entire school system's computer network. It was not until they paid over $150,000 in bitcoin that they were given the key to de-crypt all their data. Here is how the story goes:

BACKGROUND

Sometime around August 2018 a very effective ransomware program was first discovered when it hit Tribune Publishing and all of its newspapers across the country. It had similar characteristics as the Hermes malware. It also hit a large restaurant chain with 1,400 locations in Canada. Soon after many of Louisiana's school districts and municipal agencies were targeted with 1,500 servers being damaged. It is believed the same group from Russia called CryptoTech had made several improvements making it more difficult to detect, bypassing anti-virus software. This type of attack is called "big game hunting" and Ryuk has the distinction of having ransomware/extortion demands 10 times the average amount. It is estimated CryptoTech has made over $5,000,000 from ransomware attacks.

HOW IT WORKS

A user downloads an email that contains a Trojan (called a Trickbot or Emotet). This then steals the user's credentials and sends them back to the hacker. Next the malware is spread to the entire network, usually without detection, via the file sharing or print sharing portion of Windows software. The hackers can then deliver the payload, encrypting the entire computer network, rendering it useless unless the key is purchased from them. The ransom cost for this can range from $100,000 to $1,000,000 payable with bit-coins.

WHY IT WORKS SO WELL

In the initial phase of the attack the hacker learns about the user's email habits and sends a very deceptive message mimicking a typical email. The user has no idea the email was loaded with a malware virus and opens the file letting in the Trojan to "spy" on the network and learn its vulnerabilities. The attacker can then develop a payload with an undetected signature which will by-pass the anti-virus. If your back-up is not stored externally all your data is locked up. CryptoTech is selling the entire ransomware package to others on the Dark Web.

For more information about cyber insurance, contact:

imacorp.com/higher-education | **Ryan Archer,** *ryan.archer@imacorp.com* | 316.266.6293

BACK TO SCHOOL

A school district was attacked the morning of December 24, 2019, when an administrator tried to run a payroll function on the system. The school district called a short time later asking for assistance in the cyber-attack, indicating that they did not have their back-up data saved remotely. It was stored on a server that was subsequently fully encrypted by the hacker. The ransom amount was $150,000. The system was locked down, the banks closed, and the Superintendent was in a panic. The good news was they had purchased Cyber Insurance about a year ago, after their broker strongly recommended the coverage. A program, through CFC Underwriting, had the cyber response team immediately jump into action. They worked directly with the school district coordinating/advising every aspect of the cyber claim. Before all schools re-opened their data and network were successfully restored and fully functional.

THE RESULT

The $150,000 paid to the hackers was reimbursed by the CFC policy making the total out of pocket expense to the district the $5,000 deductible. The CFC response team consists of dozens of in-house cyber experts who have years of experience in cyber security and loss mitigation. This is the most valuable part of the cyber insurance program, and is often overlooked. They also have partnered with top tier forensic, legal and investigative firms that will assist during the claim process.

LESSONS LEARNED

- ✓ Have a cyber policy in place and understand what it covers and does not cover.
- ✓ Train employees to recognize potentially harmful emails, what to do with those emails and who to contact if there is any question. Train at hire and at least semi-annually thereafter.
- ✓ Back up data to an offsite service.

By Anthony Fardella, Cyber Underwriting Leader - WSI

The WRIGHT™ Insurance Group

IMA HIGHER EDUCATION
PROPERTY & CASUALTY INSURANCE AND RISK MANAGEMENT PROGRAM

For more information about cyber insurance, contact:

imacorp.com/higher-education | **Ryan Archer,** *ryan.archer@imacorp.com* | 316.266.6293