How to Make Life Miserable for Ransomware Attackers

cyber security ransomware

Summary: CFIs are among many financial services companies that have been hit by ransomware attacks, and the financial services sector is among those most likely to pay the ransom. To fight back, CFIs need to create a hostile environment for cyber attackers.

In the O. Henry short story “The Ransom of Red Chief,” the hapless kidnappers of a spoiled 10-year-old boy find that not only does the wealthy father refuse to pay the ransom, but also that the boy doesn’t want to go home. The kidnappers finally have to pay the father to take the kid back.

If only ransom cases could be so easily resolved in real life, where kidnappers threaten and sometimes carry out violent acts against their captives. Corporate ransomware cases are not as physically threatening, but the potential for damage to computer operational systems and business operations can be highly disruptive and costly.

Dole Ransomware Attack

One of the latest high-profile ransomware attacks was against the produce giant Dole, which confirmed in February that it had been the subject of an attack. Dole had to shut down plants and shipments while its own security team, bolstered by outside security experts, quickly contained the damage and got systems running again.

The incident serves as a reminder of how vulnerable US firms are to ransomware. Financial institutions are far from immune. For example, a 2022 report by the Federal Reserve counted seven attacks against community financial institutions (CFIs) since May 2021.

Once hackers breach a company’s data defenses, the company has two choices: refuse ransom demands and try to repel the attack or pay up to gain the release of data systems held hostage. In another high-profile attack in 2021, meat producer JBS USA paid $11MM to a ransomware attacker.

Most Likely Ransomware Victims

Recent surveys indicate which sectors are most often hit, as well as which ones most often pay the ransom. Financial services remain high on the list of targets. Security firm Cybereason ranked financial services in a tie with manufacturing as the second-most-often-attacked sector. Cybersecurity firm Nordlocker ranked financial services sixth.

As for which businesses would pay a ransom, more than half said they wouldn’t, according to a survey by the Wall Street Journal. But that left about four of every ten who said they would. Financial services ranked fourth on the list of sectors most likely to pay.

How Ransomware Works

In a typical ransomware attack, a hacker breaks into a company's computer system and encrypts data so it cannot be accessed by the company. A company under attack can be crippled and face significant disruptions or be unable to operate.

The attacker then demands payment, often in Bitcoin to thwart tracing, in exchange for unlocking the company's computers.

The persistence of ransomware attacks reinforces the need to be on guard and to have a procedure to take action. Here are some tips for defending and responding:

1. **Educate staff about phishing.** Phishing remains the most-often-used method of gaining entry for a cyberattack. Email attachments are the most-often-used phishing tool, so it is critical that CFIs regularly reinforce the need for staff to be cautious about incoming emails. Staff should be given regular training on how to spot a malicious email or attachment to minimize risks.
2. **Follow industry expert guidance.** The Center for Internet Security recommends seven steps for dealing with ransomware, including the following:
   - Performing regular backups
   - Developing strong response plans and policies
   - Keeping systems up to date
   - Maintaining an effective security awareness training program for employees.
3. **Constantly update cybersecurity measures.** This can involve both internal measures and outside consultants. You don't want to scrimp on cybersecurity when it comes to ransomware, which can be very costly if you are hit.

Ransomware remains a very real cybersecurity threat for CFIs. Strong security measures and employee training are needed in the battle to avoid and thwart attacks. The goal is to make life as miserable for cybercriminals as it was for the kidnappers in that O. Henry tale.

STRESS TESTING: TOP-DOWN OR BOTTOM-UP

In this market, it is important to stress test your loan portfolio. We offer multiple approaches that will fit your needs and your regulatory compliance requirements. Quickly stress test your loan portfolio and get pre-exam assistance. Learn more about stress testing today.

ECONOMY & RATES

Rates As Of: 05/04/2023 05:44AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.26	0.16	0.84
6M	5.08	0.02	0.32
1Y	4.63	-0.10	-0.07
2Y	3.84	-0.17	-0.59
5Y	3.33	-0.15	-0.67
10Y	3.38	-0.05	-0.50
30Y	3.73	0.05	-0.24

FF Market	FF Disc	IORB
4.83	5.25	5.15

SOFR	Prime	OBFR
4.81	8.25	4.82