VOTIRO
SECURED

Preventing Ransomware Attacks with Votiro's Advanced CDR

The Bar-Oz insurance company was a victim of multiple ransomware attacks that disrupted its day-to-day operations and threatened to cause serious damage to the company's finances and reputation. After deploying Votiro's Secure Email Gateway, with its Advanced Content Disarm and Reconstruction technology, Bar-Oz experienced no more ransomware intrusions.

Combating Attacks

1. Over a two-week period, the company received multiple email messages containing ransomware attacks in the form of Microsoft Word attachments.

2. Votiro implemented its Secure Email Gateway, with the patented Votiro Advanced Content Disarm and Reconstruction (CDR) technology. The Gateway blocked the ransomware by actively sanitizing all incoming traffic and delivering safe-to-edit files with their original functionality intact. The entire sanitization process takes less than a second and does not disrupt the company's business activity.

3. Malicious email messages keep on coming, but the Votiro technology continues to sanitize the files and successfully defeats the attacks.

"We chose Votiro because of its unique concept and its known success in stopping any exploit arriving through the email channel."

About Bar-Oz Insurance Company

Specializing in homeowners insurance, Bar-Oz has been serving customers for many years. As a well-known company, Bar-Oz receives many email messages and files on a daily basis, exposing the company's sensitive data to cyber attacks.

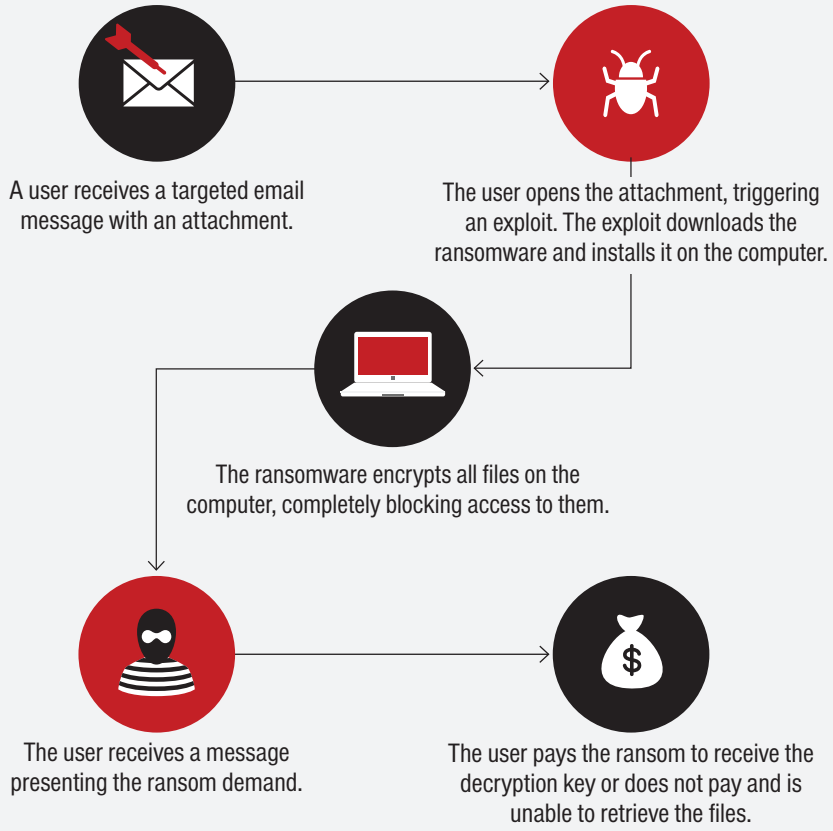
Votiro Solution vs. Employee Education

Although the employees at the insurance company had undergone multiple cybersecurity training sessions and were told on many occasions how to detect and prevent a cyber attack, those same employees opened malicious attachments and enabled ransomware to be deployed.

What Is Ransomware?

Ransomware is malicious software that, when activated, locks the victim's computer or encrypts the files in the computer. To regain access, the victim must pay a ransom to the hacker who injected the ransomware. One of the most popular types of ransomware among today's cybercriminals is Cryptolocker, which encrypts a victim's files. Only after paying a ransom does the victim obtain the decryption key for unlocking the files. Several ransomware removal tools are available online, but most of them are useless, especially on newer types of ransomware.

Votiro's patented Advanced Content Disarm and Reconstruction technology actively disarms malicious content in a file and reconstructs a clean, safe-to-edit version of the original file, keeping all of its functionality intact.
Votiro's technology does not rely on signatures and does not need to recognize a threat in order to sanitize it. Ransomware attacks depend on the manipulation of a file's active content to exploit a vulnerability in an application. Votiro's proven Advanced Content Disarm and Reconstruction technology renders any ransomware attack inert.



The Cost of Ransomware

According to a 2015 report from the Cyber Threat Alliance, CryptoWall ransomware was accountable for $325 million in damages in 2015.

Losses from a ransomware attack don't stop with the ransom itself. In a 2016 attack, Hollywood Presbyterian Medical Center was forced to pay $17,000 in Bitcoin to regain access to its files. However, the other costs involved in such an incident can easily surpass the ransom that is paid. Citing InfoSec Institute, Brad Brooks notes that "the cost of a computer forensic investigation varies greatly ($100-$600 per hour), depending on the number and types of systems involved and the complexity of the recovery of evidence." Add to that the financial harm stemming from the system's downtime, the loss of current and future customers because of the organization's damaged reputation, and the outlay required for patching the vulnerabilities in the system. In the end, ransomware attacks are expected to cost about $1 billion in 2016.

How Do You Get Infected by Ransomware?

The most common way of getting infected by ransomware is via a targeted email attack–specifically, a spear-phishing email message. The message contains an attachment, perhaps a Microsoft Office or Adobe PDF file, from what appears to be a reliable source. A user who opens the attachment unintentionally triggers an exploit, which installs the ransomware in the computer.

For more information, go to http://www.votiro.com/content-disarm-and-reconstruction.

Europe, Middle East & Africa
126 Yigal Alon St.
Tel Aviv 67443, Israel
Tel: +972 73 737 4102
Email: sales-emea@votiro.com

North & South America
640 W. California Ave., 2nd Floor
Sunnyvale, CA 94086, USA
Tel: +1 415 231 3725
Email: sales-us@votiro.com

Asia Pacific
435 Orchard Road
238877, Singapore
Tel: +65 3159 1224
Email: sales-apac@votiro.com

VOTIRO SECURED.
www.votiro.com