Success with Votiro Secure Email Gateway

One Bank's Story

Background

Seeking solution for the uprising security threats to defend its email gateway, a bank issued a request for proposals in 2013. In early 2014, the bank equipped itself with one of the best-known mail relay servers and a leading sandbox solution for detecting all threats trying to penetrate the bank. In addition, the bank licensed the Votiro Secure Email Gateway solution.

The bank also implemented a second sandbox (from a different vendor) for backup protection in case a threat managed to evade the Votiro Secure Email Gateway. This sandbox was configured to perform retroactive scanning of all original email messages—incoming messages that had not yet been modified by any defense process. The scanning would take place a few days after a message's arrival and again a few months later, to check for signatures of new threats.

VOTIRO
SECURED.

The Threat and the Defense

In 2016, a potentially serious incident occurred at the bank, with the following sequence of events:

02:06:23

Penetration

An incoming exploit bypassed the mail relay server's defenses because the sender's IP address and email account were not on the mail relay's blacklist, and the threat's signature was unknown to the mail relay.

02:06:24

Detection Attempt

The exploit evaded the sandbox by monitoring the services on the sandbox machine and locating services (on the Internet) associated with a specific sandbox vendor.

02:08:48

Neutralization

The Votiro solution's patented active content disarm technology, designed to remove unknown and zero-day exploits, successfully neutralized the exploit.

02:08:50

Validation

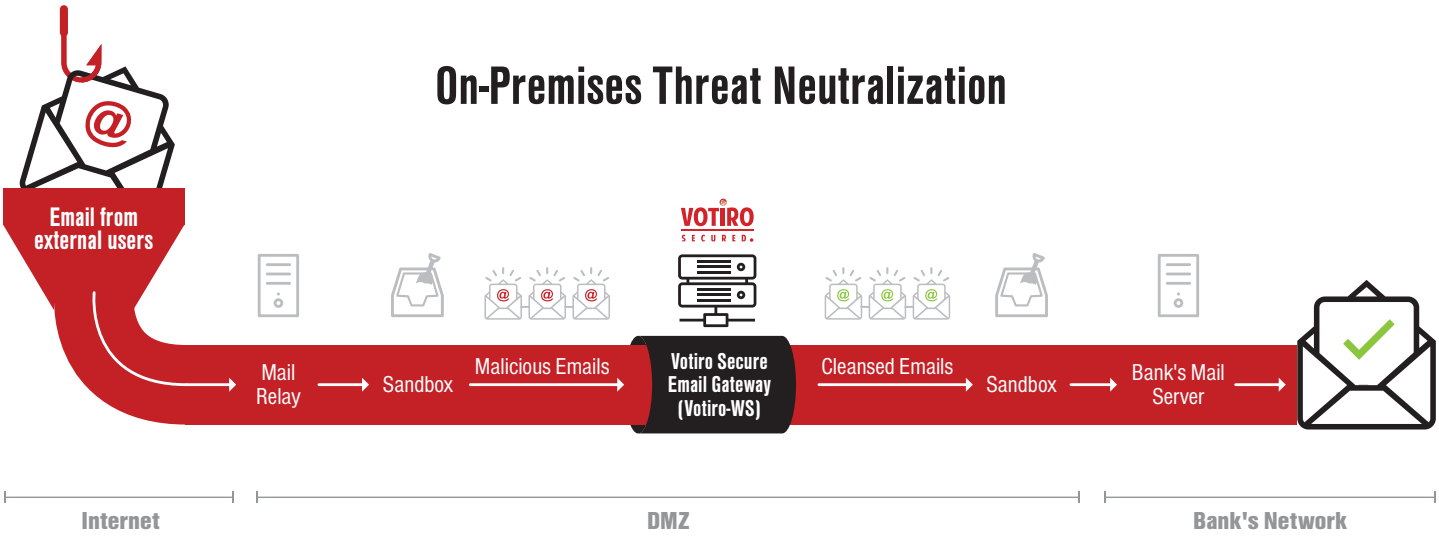
The cleansed email message was sent to a second sandbox machine for analysis.

02:11:20

Delivery

With all threats eliminated, the email message was delivered to the user's mailbox.

On-Premises Threat Neutralization



Subsequent Developments

A few days later, a retroactive scan of original email messages identified a signature that had been added in a recent update. A threat alert was issued. That threat was the exploit that the Votiro solution had successfully eliminated without identifying the signature! If it had not been neutralized, the exploit could have created a backdoor that would enable unknown ransomware to enter the bank's network.

"I must admit that seeing the alert during the retroactive scan really spooked me," said the bank's IT manager. "We immediately began checking for signs of damage. Each time we saw that a network segment hadn't triggered an alert for the same signature, we breathed a sigh of relief. When all the segments had been scanned and no evidence of the threat had appeared, we looked into the history of the threat's signature. The only traces of the threat's presence were in the original message, before it had undergone the Votiro cleansing. We reprocessed the original message with the Votiro gateway solution, and the exploit was completely neutralized!"

Eventually, it became clear that the bank would not need to renew its license for the second sandbox, because no exploit had evaded the Votiro gateway.

> "We chose Votiro because of its unique concept and its known success in stopping any exploit arriving through the email channel. The Votiro technology has really proved its worth for us."
>
> —The bank's CISO

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