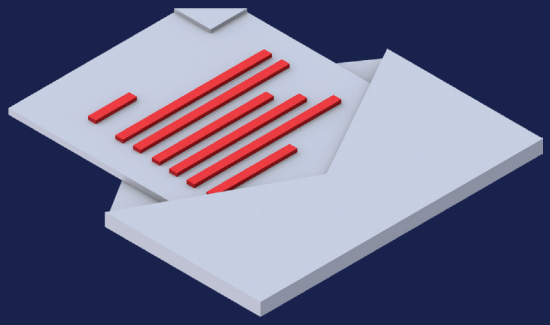
VOTIRO
SECURED.

Success with Votiro Disarmer for Email



Background

In 2014, seeking an innovative, best-of-breed solution to defend its email gateway, one bank had equipped itself with one of the best-known mail relay servers and a leading sandbox solution to detect all threats attempting to penetrate the bank's network. On top of those, the bank had also licensed Votiro Disarmer for Email.

The Attack

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

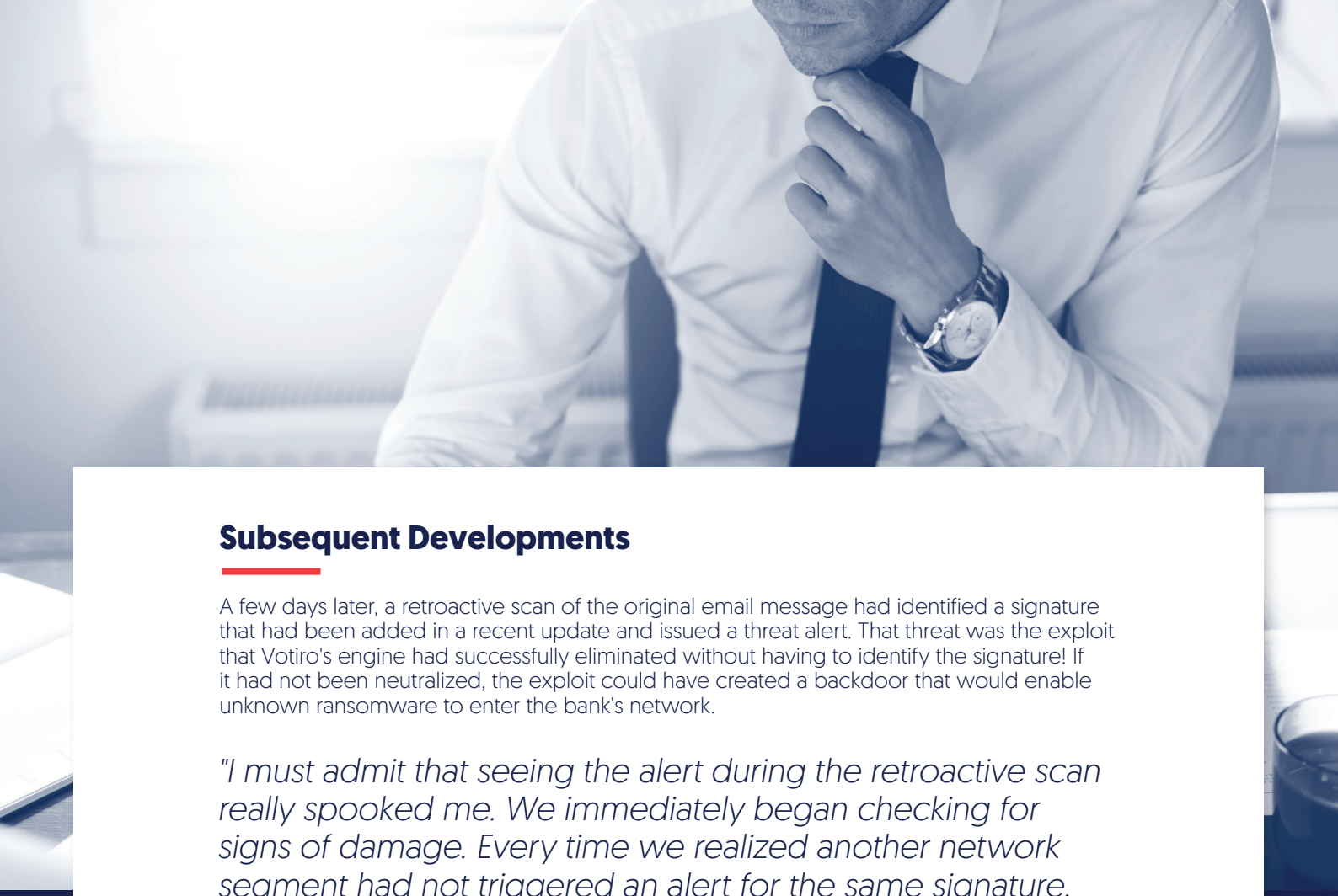
14:06:23 An exploit had arrived at the mail relay server and was able to quickly bypass its defenses because the sender had used a new IP address and new email account. As these were not on the mail relay's blacklist, the threat's signature was unknown to the mail relay.

14:06:24 The exploit had then evaded the sandbox through a well-known sandbox evasion technique: monitoring the services on the sandbox machine and locating services (readily found on the Internet) that are associated with a specific sandbox vendor.

14:08:48 The Votiro Disarmer's patented Content Disarm and Reconstruction technology, designed to eliminate unknown and zero-day exploits, had successfully neutralized the exploit.

14:08:50 The processed email message was sent for analysis by a second sandbox machine.

14:11:20 Cleansed of all threats, the email message was delivered to the user's mailbox.



Subsequent Developments

A few days later, a retroactive scan of the original email message had identified a signature that had been added in a recent update and issued a threat alert. That threat was the exploit that Votiro's engine had successfully eliminated without having to identify 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. We immediately began checking for signs of damage. Every time we realized another network segment had not triggered an alert for the same signature, we sighed in relief. Once all 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 Disarmer cleansing. So we reprocessed the original message with Votiro Disarmer, and the exploit was completely neutralized!"

Bank's IT manager

The Value

Eventually, it had become clear that the bank didn't need to renew its license for the second, backup sandbox, since no exploit had been successful in evading the Votiro Disarmer.

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

Bank's CISO

VOTIRO SECURED.

Learn more about Votiro's CDR technology.