CASE STUDY

Venafi CodeSign Protect helps transportation company thwart ransomware attacks

Challenge: Ransomware attack linked to malicious macros

Recently, a transportation company was hit by ransomware. The ransomware infiltrated a group of internal virtual servers and as a result, brought down a significant portion of the company's network. The company chose to take down all the virtual servers infected by the ransomware and restore them from previous backups rather than comply with the attacker's demands of a multimillion dollar payoff.

Although the company did not pay the ransom, a great deal of damage had been done during the recovery. Logistics were halted, and customer service was down for more than an hour. Although InfoSec wasn't sure how the servers had been compromised, they did know that a phishing email with an attached malicious Microsoft Office macro was sent to several company employees not long before the ransomware attack took place.

Said the company's CISO: "Employees are required every year to take cybersecurity training, and we also send them fake phishing emails to test them and keep them on their toes. But it only takes one distracted or careless employee to let malware in."

Solution: Venafi CodeSign Protect

The company already was in the process of evaluating code signing security solutions to protect their internally built logistics software used with their partners and customers. They wanted to avoid software supply chain attacks, especially after seeing firsthand how the highly publicized SUNBURST attacks impacted some of their customers.

When Venafi came to demo CodeSign Protect, the director of PKI services mentioned his frustration at the company's struggles with phishing—and his suspicion that some connection existed between the malicious macro and the subsequent ransomware attack. Venafi asked if the company knew that internal macros and scripts could be code signed—and that any macro that wasn't signed could be prevented from executing with the proper security controls in place.

Said the director of PKI: "No, we didn't. In fact, it hadn't occurred to any of us. When it clicked that our Office macros and PowerShell scripts were code just like anything else—well, it was a real 'smack-my-head' moment."

Venafi told the company that CodeSign Protect could manage and protect all their macros and scripts, in addition to protecting the company from attacks. Venafi expanded their proof of concept (PoC) to demo how CodeSign Protect signed internal code and automated security controls that could disable and remove all unsigned macros. They also showed how CodeSign Protect integrated seamlessly with users' preferred toolsets, whether they were developers writing apps using DevOps methodologies or IT team members writing PowerShell scripts.

Even better, CodeSign Protect automated everything having to do with signing code, including managing the lifecycle of code signing keys and certificates, as well as enforcing security policy. Once the company saw how powerful the Venafi solution was, their biggest concern was whether CodeSign Protect could scale quickly to manage the security of their internal code. CodeSign Protect quickly proved it could deliver.

Flexible policy configuration with automatic enforcement

Using CodeSign Protect, the company's InfoSec team could now define code signing policy configurations that aligned with corporate security policies. And these policies could be configured using important parameters, such as restricting the issuance of code signing certificates only to approved certificate authorities (CAs), setting minimum encryption strength of private code signing keys, and specifying the management approvals required before a code signing key could be used to sign a given piece of code.

Moreover, CodeSign Protect enabled the company to set up multiple configurations they could uniquely tailor for each of the functional areas of the organization. "Not only is it easy to use, but it's also incredibly flexible. Now we can have one set of code signing security policies specifically for signing of Office macros, another, more stringent policy for critical IT infrastructure shell scripts and then an appropriate set of policies for the logistics software we share with our partners," said the director of PKI services.

Trusted, self-service code signing

Because CodeSign Protect automatically manages code signing certificate lifecycles, including issuance and renewal, it could make the appropriate keys and certificates available to authorized end users, depending on the use case. After the initial policy and enforcement configurations were completed, the company's IT department was then able to configure their employees' computers and Microsoft Office productivity suites to require that all shell scripts and macros be code signed with a company-authorized code signing certificate before they were allowed to execute.

Thanks to CodeSign Protect, the author of, say, an Excel spreadsheet macro, could run the code signing command from within Excel to sign their macro. They no longer needed to know where the private key was being stored or which code signing certificate they should use. And instead of having to depend on InfoSec to sign their code or have a grasp of how code signing works, CodeSign Protect gave these end users the ability to sign their code themselves with just a few clicks.

"No more complexity. No more overhead. My team now can support our thousands of employees without worrying about their levels of expertise or skill," explained the director of PKI services. "This level of simplicity is essential to ensure widespread adoption across our enterprise—the only way code signing serves as an effective means to help stop future ransomware attacks."

Companywide visibility of all code signing operation

Besides cutting down on third-party scripts and macros from spreading malware, CodeSign Protect gave the company's InfoSec team visibility into every code signing operation taking place across their enterprise, regardless of what was being signed or what code signing tools were being used. This single-pane-of-glass perspective supplied a historical record of all code signing activities, as well as an irrefutable audit trail.

Said the company's CISO: "CodeSign Protect has enabled us to secure all of our code regardless of the type. It's not only easy to use, but it also keeps us safe. And Venafi's expertise goes above and beyond their competitors because they anticipated problems we didn't know we had! It's great to have them in our corner."