NSA Kaspersky Hack Underscores Data Loss Prevention (DLP) Solutions

The NSA Kaspersky Hack

Early this month, Moscow based IT Security firm, Kaspersky Lab, was accused by the FBI of being connected to a Russian government hack of an NSA contractor in 2015. Allegedly working on new spy/hacking software for the NSA, the contractor had brought work home, leaving it vulnerable to theft.

The FBI says that Kaspersky operated as a front for a Russian government spy organization that deliberately hacked the contractor to steal the code. The contractor's home computer was running Kaspersky Antivirus at the time.

The following week, The New York Times reported that Israeli government techs claimed they had uncovered Russian government hackers operating through Kaspersky's network in 2015.

> *The Israelis maintained that the Russians employed Kaspersky software to hunt for classified U.S. documents all over the world.*

Eager to refute the charges, Eugene Kaspersky said his AV software did its job and correctly spotted the NSA code as malicious, sending a copy back to headquarters. He suggested that his own data was hacked by the Russian government.

Even though Kaspersky had recently boasted that his defenses were like Fort Knox, he conceded that his own product was "horrendously compromised."

Not without its consequences, the Kaspersky hacking incident may be the justification the U.S. government used in September to ban the use of Kaspersky products by all government agencies.

Trusted Resource Threats

Whether you believe Kaspersky or the Israelis and the FBI, the Kaspersky saga highlights a situation where data is stolen by or through a trusted resource. In the Kaspersky case, antivirus software was used as the tool to identify and allegedly steal the target data.

Is the apparent Kaspersky AV hack a new type of threat? Will we now be under attack from everything designed to protect our data?

Although it may be the first time you've heard of AV software being used as a hacking tool, it's not the only time a trusted resource has stolen data.

Sadly, this type of insider data theft is carried out frequently by third-party software, an employee, a competitor or other bad actor. Too often, it's successful. Recently, CCleaner utility software unwittingly infected thousands of computers with a virus hidden in its code by hackers. Likewise, the South Korean military was apparently hacked by way of Hauri AV software.

Blocking Data Exit

Current network defenses focus on preventing unauthorized access or malicious code from entering the network. But, what if a Kaspersky or trusted resource type of threat, is employed? Traditional network defenses can be more easily fooled, or in the case of bad actors with access, simply bypassed. Fortunately, another type of network defense, data loss prevention (DLP), is up to the challenge.

No matter where the threat enters, DLP software is designed to prevent sensitive data from leaving the network.

Rather than scanning for intruders, DLP works by pattern matching data as it exits the network. It scans hundreds of file types for data that should be staying put. This could be intellectual property, customer information or company financial data departing via email, FTP, web protocols, USB drive or smartphone.

Humans are the weakest link in data security and DLP can prevent them from accidentally or deliberately taking sensitive data from the network.

DLP users have the option to customize the DLP setup to look for each type of sensitive data they have. When a match occurs, appropriate action is taken such as alerting the security team or blocking the data transfer with a "no-no, you shouldn't do that" type of message.

Would DLP software have prevented the Kaspersky AV hacking incident? That's a great question that you should ask vendors of DLP solutions.

DLP in the Spotlight

One benefit of the Kaspersky saga is that it focuses more attention on the strategy of checking and blocking unauthorized outbound data. That's a good thing. Most IT security solutions just try to prevent inbound threats from entering the network.

When it comes to valuable data, there is always someone looking for a way to steal it. If they can use a trusted resource to accomplish the heist, they will.

So, don't be the victim of data theft from an inside, trusted resource such as AV software, third-party applications or employees. Consult with your local IT security experts to determine if you need DLP. WatchGuard, an award-winning security firm with affordable data security appliances designed specifically for small and mid-size businesses, provides excellent DLP solutions.