The ultimate breach indicator: A visit from the FBI

Wed, 2013-07-03 03:42 PM
By: Jeff Schilling

There are many ways for enterprise owners to discover their networks have been breached. Each "breach indicator" has its own level of certainty attached to it.

Jeff Schilling

However, when an FBI agent from its cyber division visits your organization and informs you that "you've got a problem," you can be nearly 100 percent certain that you've been breached.

I recently visited a senior security executive in the commercial space who is tracking how many times his security team knew about a breach incident *before* the FBI. At this point, his team is batting 1 for 5, or 20 percent.

The struggle of this security executive is not unique to the commercial space. Small to medium-sized government agencies' chief information officers struggle with the same problem. So, how does the FBI know about a breach in your organization, and how can you get the same or a better level of visibility to increase your organization's batting average?

First, you need to understand why your current batting average is low, and what you can do to improve it. The reason why most smaller government agency network owners can't get ahead of the FBI is because they only have visibility and intelligence on threat activity based on what they see happening inside of their networks.

In order to get ahead of the threats before the FBI learns about them, you have to do four things: (1) Know the methods of your threat actors, (2) be able to see the activity on your network, (3) quickly interdict the threat activity before the threat actors achieve their objectives, and (4) eradicate their presence. In order to do these four things, you have to have threat intelligence that has a global perspective and will inform your team as you execute these four activities.

The FBI, as well as the U.S. Intelligence Community, collect threat intelligence in cyber space through a multi-faceted approach of technical intelligence gathering through both classified (U.S. Code Title 50) and law enforcement (U.S. Code Title 18) operations. Most of the visits you get from the FBI letting you know you have a problem are prompted by these type of operations.

Law enforcement agencies share data and collaborate with other government organizations to learn about network breaches. These agencies then share what they have learned from one another, via reports to the wider government community of interest. Information in these reports can be used to proactively protect the network owners that subscribe to this data. That information might include things such as Internet addresses and domain names that are known to belong to threat actors and should be blocked, and binary signatures (MD5 Hashes) that can be used to scan your environment for threat activity.

Advanced cyber threats from nation-state and criminal gangs, are getting more sophisticated and targeted. These threats are so advanced that they routinely evade signature-based defensive strategies (anti-virus, fire walls) used detect and eradicate threats. A simple way to get ahead of the threat could be by joining the classified community of interest, so you can get the intelligence reports directly from the law enforcement/counter intelligence and intelligence community. However, most of the information from this community interest is classified and Top Secret. This "simple way" of collecting information becomes complex when you have to build facilities, which are approved to process classified material.

The alternative is to look to commercial industry for threat intelligence. Commercial vendors that provide managed information security services to thousands of commercial customers have the same ability as the FBI and the U.S. Intelligence Community to collect threat intelligence with a global context. This global context comes from two main activities: (1) hundreds of attempted cyber-attacks the management security service providers see hitting their customers' networks, and (2) other collection techniques, such as "sink-holing," (legally registering a domain address used by a bad actor and collecting intelligence from the tradecraft reporting to those domains).

The information from the commercial sources is unclassified and rivals the information you could get at the secret level from law enforcement and the intelligence community. If you want to improve your batting average and get ahead of the FBI visits, you must get a global perspective from your threat intelligence.

Jeff Schilling is director of the Dell SecureWorks Incident Response practice. He can be reached at:

jeff@secureworks.com