IMSI CATCHER

A San Francisco biotech company became suspicious of a digital intrusion when the competition accessed well-guarded secrets concerning the expansion of its product line. The National Sales Director approached the CIO about a potential intrusion after the customer requested information concerning their soon-to-be released product line. The customer indicated the biotech company's competitor claimed their product's performance was superior to the biotech company's newly developed product. The National Sales Director was immediately suspicious since details about the new product line were available only to a select group of employees who were bound by confidentiality requirements.

The CIO reviewed the company's risk management plan to ensure the required testing was performed at the required intervals. He also discussed the results of recent internal cyber security testing with their IT Manager. The CIO assured the National Sales Director that internal testing had not identified a data breach. The CIO then hired a cyber security consultancy to perform additional testing of their network security. When the cyber security consultancy also did not identify a network intrusion, ComSec LLC was contracted to perform a TSCM / Cyber TSCM survey.

ComSec's TSCM survey detects the presence of active and passive electronic eavesdropping threats, while the Cyber TSCM survey detects hybrid and other devices that utilize the cellular network to capture data. During the Cyber TSCM portion of ComSec's survey, an IMSI catcher threat was detected. The IMSI catcher was collecting voice, data and text communications from mobile devices in use at the biotech company by acting as a rouge cell tower for the mobile phones. A duplicate copy of all voice, data and text communications was routed to the rogue cell tower, without providing any indication of an issue on the breached mobile devices.

By performing a Cyber TSCM survey, ComSec LLC detected the use of the IMSI catcher and located the origin of the threat signal. ComSec also provided a "for purchase" leave behind cellular intrusion secure mobile communication solution for the biotech company executives.

DETECT • ISOLATE • SECURE

While IMSI catcher technology was once limited to use by government and law enforcement personnel, this is no longer true. Due to the limited effectiveness of security features on mobile networks, devices, software and services, hackers and others - who need little technical knowledge to employ the devices - now have access to the IMSI catcher technology.

If you suspect a cyber intrusion, contact ComSec LLC. Our Cyber TSCM surveys detect the presence of threats that IT/cyber security specialists are not equipped, or trained, to identify. The IMSI catcher threat is real and the solution available!