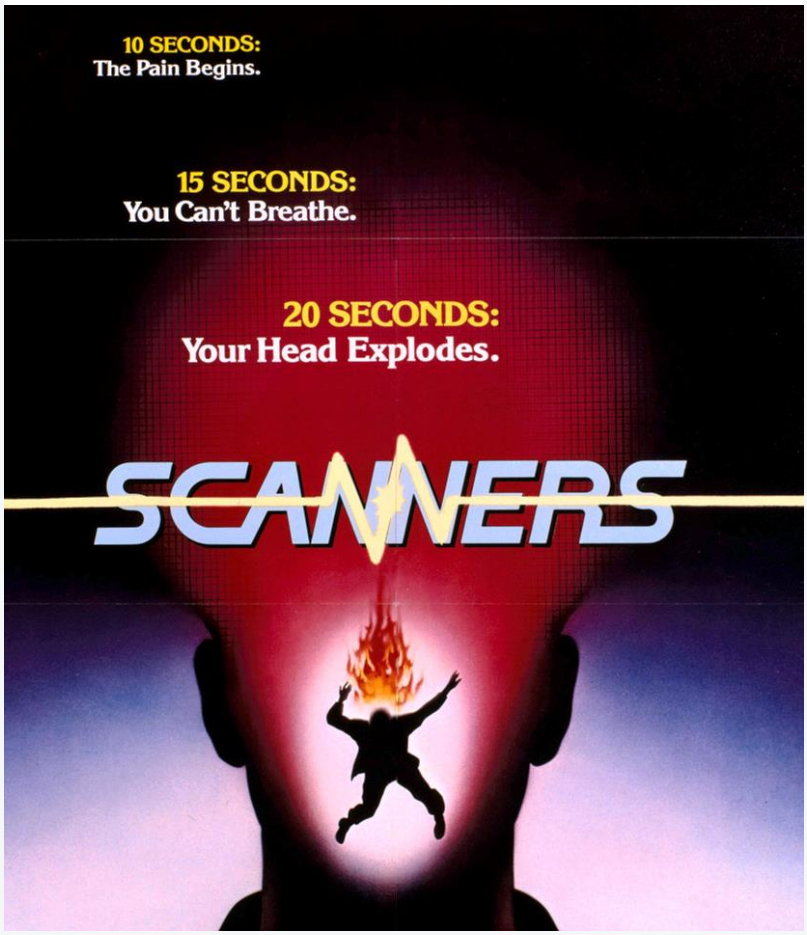
No images? Click here

Scanners: Computer & Internet Management/Monitoring Techniques

Brian J. Kelly, Cyber Analyst - IPPC Technologies



DISCLAIMER OF ENDORSEMENT. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement,

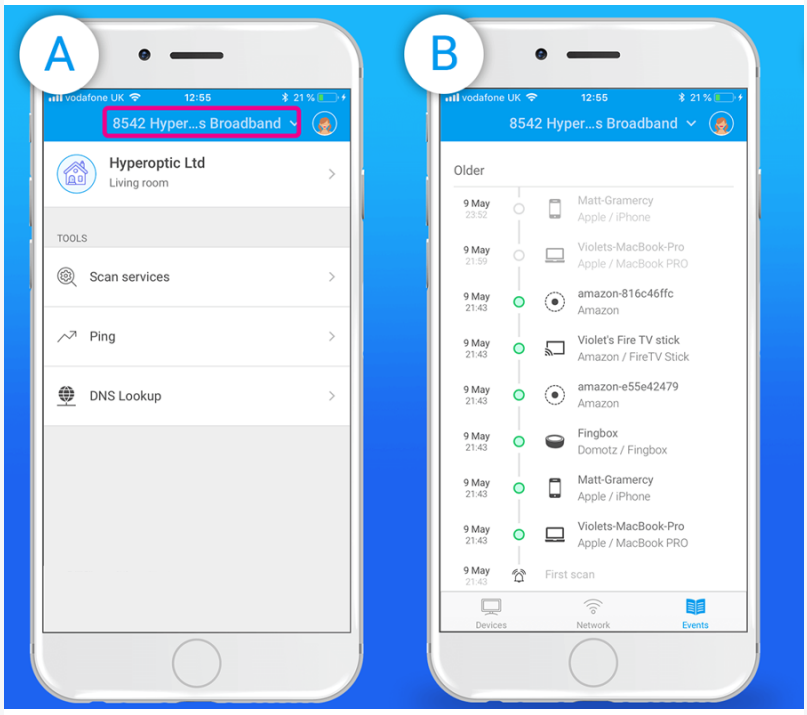
recommendation, or favor of IPPC Technologies.

Scanners is a 1981 science fiction horror film written and directed by David Cronenberg. In the film, "scanners" are psychics with unusual telepathic and telekinetic powers. The movie is known for its iconic head explosion scene, so for some in a figurative sense, this topic may be relatable...

The detection of the presence and use of unauthorized Internet-capable devices is a crucial component of a successful Computer and Internet Management/Monitoring Program (CIMP). The “Internet of Things” (IoT) has created smart homes for ease and convenience, but also provides persons under supervision (PUS) with computer/Internet monitoring and restrictions pathways to access prohibited/illegal content undetected. As part of initial supervision techniques and enrollment into an agency’s CIMP, officers should assess what connected devices are in the residence, what does the PUS need to access, what can be monitored, what can be “locked down”, either through physical (i.e. tamper tape) and/or digital means (i.e. parental controls), what should be removed, etc. Once the baseline is established, the real work begins.

While devices such as smartphones and tablets are small enough to conceal and hide from visual inspections, there are techniques officers can use to detect unauthorized Internet-capable devices. Most homes will now have a wireless network to allow all the various connected devices to communicate and access the Internet. As part of

CIMP enrollment, this network information should be collected (i.e. Internet provider, router information, SSID and password). Using this information during a home contact, officers with their own smartphones can utilize numerous free apps available, such as Fing (see screenshot below), to connect to the network and scan the network for all connected devices. The device typically needs to be powered up and connected to the network for a network scanning app to detect the device. There are advanced techniques for actually taking administrative control of a router and/or analyzing router logs, but this is a topic for another article. There may also be legal considerations before conducting a network scan, as discussed below.



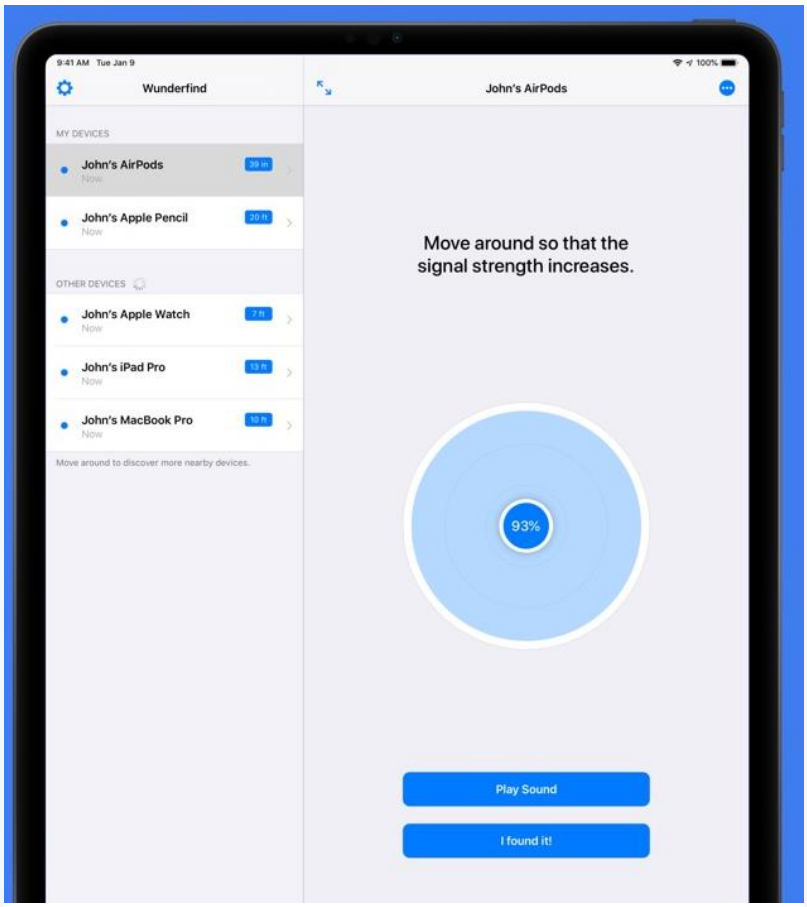
In August 2009, Assistant General Counsel for the Administrative Office of the United States Courts (AOUSC) responded to an inquiry from a Chief U.S. Pretrial Services Officer regarding the use of WIFI detectors in the field to determine if a defendant has access to a

wireless Internet connection inside his/her residence. The AOUSC AGC determined that use of such a device would violate the Fourth Amendment, and would require a special condition from the Court before the use of said device. Much has changed since 2009, and this topic has been discussed in length amongst officers across the country. There are also Court rulings that support the use of similar technology: In November 2012, Judge Joy Flowers Conti (Western District of Pennsylvania) ruled that a defendant had no expectation of privacy when he voluntarily transmitted his WIFI signal outside his residence to connect to a neighbor's router to download child pornography. Law enforcement utilized a software program (Moocherhunter) to pinpoint the exact location of a computer that is using a WIFI signal. The Third Circuit Court of Appeals upheld that conviction.; In August 2012, Chief Judge James Holderman (Northern District of Illinois), in a patent litigation involving Innovatio IP Ventures, LLC, granted a motion from the plaintiff to admit evidence collected from a "WIFI sniffer", stating that the use of the technology did not violate the Wiretap Act, or the Pen Registers and Trap and Trace Devices Act. Ultimately, it is critically important to be well versed on any requirements your agency and/or Court may have in place before engaging in these practices.

Along these same lines are the use of Bluetooth scanner apps. Many devices utilize Bluetooth to connect and communicate with other devices (i.e. wireless headphones). Understanding how Bluetooth communicates can be a bit of a nerd

adventure; Bluetooth works with broadcasting signals and that broadcasting power value is around 2–4 dBm (decibel-milliwatts) so the signal RSSI (Received Signal Strength Indicator) strength will be around -26 (a few inches) to -100 (40–50 meters). Due to external factors influencing radio waves, such as absorption or interference, RSSI tends to fluctuate. The further away the device is from the beacon, the more unstable the RSSI becomes. Bluetooth typically has a range limited to 33 feet for typical user devices like headphones, but can transmit up to a kilometer in certain scenarios. Bluetooth scanner apps, such as Wunderfind (see screenshot below), make it easy to detect devices transmitting a signal and give an estimated distance to that device. The use of Bluetooth scanner apps does require a bit more skill to locate a device, especially in dense urban areas. This is a bit less definitive than a wireless network scanner as this does not mean the device is in the residence or even owned/used by the PUS (unless it is connected to a known device). Again, be well versed on any requirements your agency and/or Court may have in place before engaging in these practices.

If you want to go full nerd James Bond-style, there are plenty of handheld radio frequency devices sold by "spy shops" or even Amazon, that can claim to detect WiFi, Bluetooth, GSM/CDMA (cellular) and other radio frequency signals within certain frequencies (MHz-GHz).



IPPC Technologies' computer & Internet monitoring solutions are continually being developed and improved upon to assist officers throughout the supervision process. IPPC Technologies monitoring solution for Windows devices does have the ability to scan the network the device is connected to for other devices. This must be configured by our technicians, so please contact IPPC if you are interested in running network scans For more information on IPPC's services such as Spotlight, please call IPPC at (888)-WEB-IPPC or contact me directly at bkelly@ippctech.net or by calling (516)341-4201.

Share

Tweet

Share

Forward

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET

Preferences | Unsubscribe