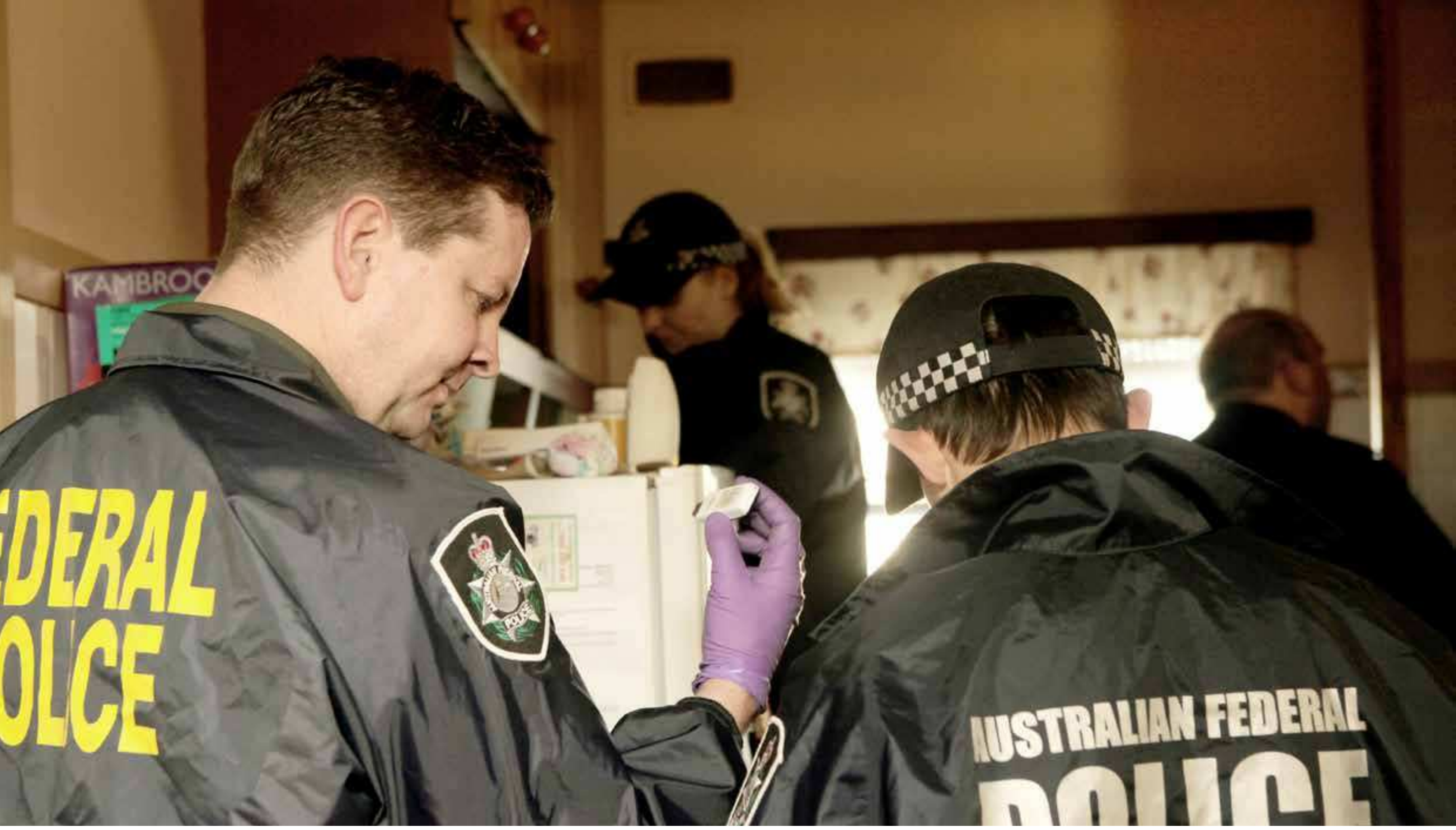

Malicious Mr Evil

Mr Evil's digital trail of destruction ultimately spelled his own downfall and a gaol sentence.

Probably the best illustration of how digital 'metadata' assists law enforcement agencies in bringing criminals to justice is an example of a crime itself. On that score, there is no better investigation than Operation Damara and the self-proclaimed Mr 'Evil'. It shows both the problem of not having metadata and, conversely, how having metadata enables a successful investigation.

Metadata is the computer and telecommunications records left when an individual accesses a communications network. Presently, there is no law in Australian that compels telcos and internet service providers (ISP) to retain telephone call records or metadata for a certain time. Retention of this vital investigation resource is inconsistent and essentially up to each company.

Detective Superintendent Brad Marden was the National Coordinator Cybercrime Operations during Operation Damara in the 2011 investigation that led to the arrest of David Noel Cecil (aka 'Evil' in the virtual world). Detective Superintendent Marden says it was computer metadata that finally enabled the vital connection between David Cecil and the moniker, Evil.

"Essentially, metadata allows us to retrospectively track someone who may have been at a certain place at a certain computer at a certain time," Detective Superintendent Marden says. "It goes back to the old days with the telephone. If you have made the phone call to set up the drug import you have left a record behind.

"It's no different in the computer world. But if you don't have that ability to see who made the contact; essentially your investigation stalls.

"If you know something is going to happen you can apply for telephone intercepts and you can use surveillance. But if you are looking retrospectively after an event has occurred the only data that will be ever available is the stuff that is captured prior to the event."

Detective Superintendent Marden says practically every investigation relies on obtaining metadata from telcos and ISPs.

"Essentially, it is a targeted request for metadata information and each individual request, if authorised, is made for a specific purpose to further the investigation," Detective Superintendent Marden says.

AFP Federal Agents end the digital vandalism of David Noel Cecil (aka Mr Evil).

"We are not collecting content data, we are not keeping a record of everybody's conversations and we don't do big data matching. We don't do it, we can't do it and we are not asking to do it."

Unfortunately, someone using the moniker, Evil, managed to cause $10 million in damage for which no one has been arrested precisely because there was no metadata retained that could link Evil to any known person at that time.

The moniker, Evil, had already come under suspicion of AFP investigators for computer intrusions. At that point he was identified as a suspect in the defacement of a prominent Australian university's website In January 2011. In May, the AFP's Cybercrime Operations received further notification from a US internet service provider of a system intrusion believed to have come from Australia.

But it was in June 2011 that Evil struck his most malicious blow. On Saturday 11 June 2011, the website of a top-level domain registrar DistributeIT was defaced. The intrusions became increasingly more severe and the attacker subsequently issued commands inside the DistributeIT network itself.

Ultimately, Evil advanced to deleting websites hosted by the company including backup data. It is estimated that over 250,000 customers were affected by the incident. The attacks put DistributeIT out of business.

"The business was completely destroyed," says Detective Superintendent Marden. "About $10 million damage – a malicious actor.

"The stumbling block on the initial investigation was that Evil was using a 3G modem and there was no data retention. We could never prove it. It wasn't until we actually caught someone for another crime with the same nick."

What AFP investigators did discover was that the as yet unidentified person was continually using a unique nickname, Evil. "We then started looking on the web for this Evil character and through metadata identified somebody who was using that nick – David Cecil."

AFP investigators sought and were authorised to use telephone intercepts and listening devices. David Cecil was then caught in the act of attempting to destroy yet another company.

The sole motivation for the crime was malice. In a former age, this type of person would largely have been constrained to defacing shop windows with spray paint. But in the digital age he was enabled by technology and with skills he had learnt entirely from the internet. David Cecil had absolutely no formal IT training at all.