Rise in children’s identities being sold on the dark web

Information about teenagers being traded for as much as $3000

Byron Connolly (CIO) | **03 July, 2018 12:23**

Michael Connory’s firm
Security in Depth develops cyber security awareness programs for corporate organisations. This training involves discovering what information about company executives resides on the ‘dark web'.

But these searches often uncover something even more sinister: personally-identifiable information about children and teenagers, some residing in Australia, being sold by criminals across the internet’s dark underbelly.

“While we are researching maybe an executive from a multi-national organisation to demonstrate what is out there [on the dark web], we will see kids’ information being sold,” Connory told *CIO Australia*.

“There are kids in Australia but primarily we find that most of the information comes out of the US or Europe … mostly out of the UK.”

For instance, the company has discovered information about teenagers – including the tax file numbers and Medicare information – being sold online for as much as $3000.

Information of this type has been more prevalent on the dark web over the past 12 months, he said.

"And we are not just talking about one kid; [criminals] buy information in bulk. They can buy one child's identity but these organisations tend to sell in bulk so they would buy 100," he said.

Kids’ identities are generally clean, said Connory. There’s no credit history, often very little history whatsoever, and if criminals can access a Medicare number, date of birth or other pieces of information, it’s quite easy to create a new identity without anyone noticing, he said.

“A child is not going to check their credit score and banks and finance companies aren’t necessarily going to do deep background checks on these kids because there is no real background.

"There’s a trust factor that comes into it; you can take a child’s information, say that they are working in a job and the bank is not going to check those details out at a great level.”

Most of the information Security in Depth discovers is about children aged between 14 to 18 years old as people in this age group are very active on the internet, Connory said.

Security in Depth’s research suggests that 98 per cent of teenagers aged 14 and over in Australia have access to social media sites. When they access these sites, they accept terms and conditions and provide personally-identifiable information.

“Whilst they are on Facebook, they click on a game that captures of all their information … which is then siphoned off to a third-party provider,” he said.

“It’s not just Facebook, it’s other applications that do the same thing. This information is either on sold or the data is breached and accessed by somebody who wants to put it on the dark web for sale.”

There’s an even darker side to this trend too, he said. Having access to a child’s information – maybe a user name and password, what games they are playing and how old they are – provides much greater awareness for pedophiles, he said.

“It’s much easier for them to start a conversation and connect with these individuals.”

Child abuse online is an increasing problem. In March, a Queensland police squad secretly took over child-abuse forum on the dark web, rescuing more than 100 children in the process and leading to arrests.

Connory said Security in Depth doesn't report its findings to police.

"The challenge that we have is that police are looking at most of this information anyway," he said. "If we recognise a name or an individual, we will pass that information to the individual or [another] appropriate person.

"By the time we have seen things, most of the information is gone; it's been sold. These marketplaces pop up and get taken down pretty quickly. It's not easy to be able to track the information."

Connory said many social media sites are allowing children as young as 13 to share their information online.

"Does a child have the authority to accept all of the terms of and conditions of an organisation like Facebook or Snapchat? Our legal team does not believe that this is so," he added.

"I'm sure Facebook or whomever has a work around but kids are signing up and accepting the terms of having their personally-identifiable information being shared without understanding the consequences."

Follow CIO Australia on Twitter and Like us on Facebook… Twitter: @CIO_Australia, Facebook: CIO Australia, or take part in the CIO conversation on LinkedIn: CIO Australia

Follow Byron Connolly on Twitter: @ByronConnolly
