Australian hospitals are under constant cyber attack. The consequences could be deadly

Paul Haskell-Dowland, *Edith Cowan University*

Last week, the Australian Cyber Security Centre (ACSC) issued warnings to Australian health-care providers that it had observed an increase in cyber incidents targeting the sector.

These attacks seem to be aimed at infiltrating networks and burrowing deep into their infrastructure before deploying further attacks.

The ACSC is tasked with improving Australia's cyber security posture, and provides advice and support to help ensure Australia is a secure place to live and work. As part of its warning, the ACSC flagged the possibility of "ransomware" being deployed, which could disable critical systems unless a ransom is paid. In a hospital or other health-care facility, this could be a life-threatening situation.

Attacks against the health-care sector are dangerous at any time. But when services are under pressure from COVID-19, and information-sharing (including tools such as contact tracing) is increasingly important, an all-out cyber attack against the health sector could be very damaging.

The current threat

The ACSC guidance identifies two significant threats.

The first is the SDBBot Remote Access Tool (often referred to as a RAT), whereas the second is a ransomware tool named Cl0p. While neither is desirable, the combination of the two is particular concerning in a health-care setting.

SDBBot Remote Access Tool (RAT)

A RAT is a piece of malicious software designed to allow criminals to remotely access and control one or more systems in an organisation. Once run, the SDBBot RAT installs itself, downloads additional components and deploys the remote-access capability.

Once fully installed, criminals will often use a compromised computer to explore other systems – a technique often referred to as "pivoting". As the criminals move through the network, they often take the opportunity to make copies of sensitive data. This can be a valuable asset to use for coercion, blackmail or even sell through the underground economy.

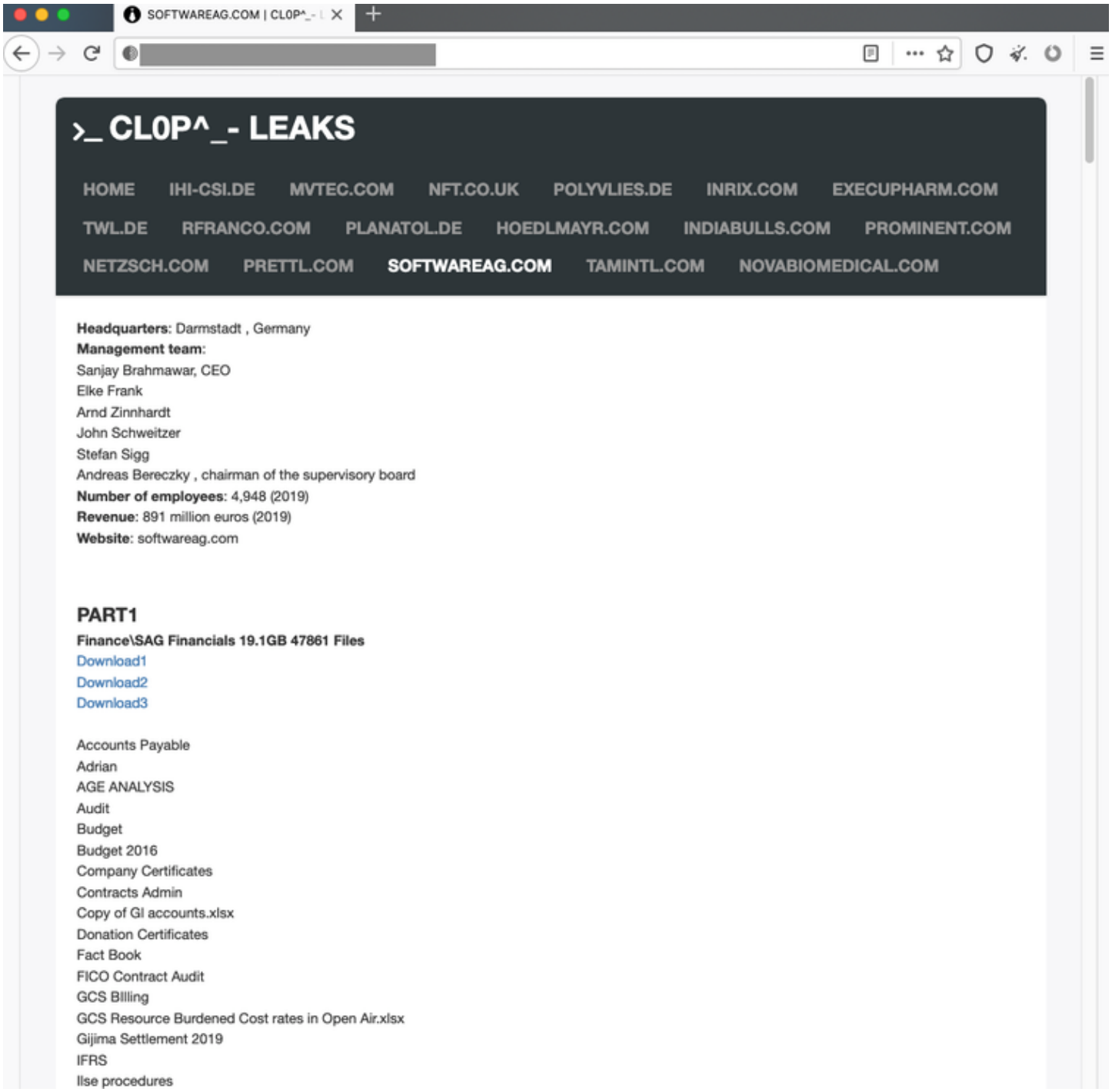
Cl0p ransomware

Having the SDBBot RAT successfully deployed enables other attacks – one of the most concerning is that of ransomware. While not an inherent feature of SDBBot, a frequent consequence of infection is the subsequent deployment of the Cl0p ransomware.

Ransomware generally encrypts an organisation's files or data so they are no longer accessible. Recovering the files typically involves paying a ransom, often in Bitcoin or another cryptocurrency.

In October, German company Software AG faced a US$20 million ransom demand after a Cl0p ransomware attack. In this incident, the criminals claimed to have more than a terabyte of stolen data,

including emails, financial records and even scanned copies of passports. This data trove was published online when the company failed to pay the ransom.

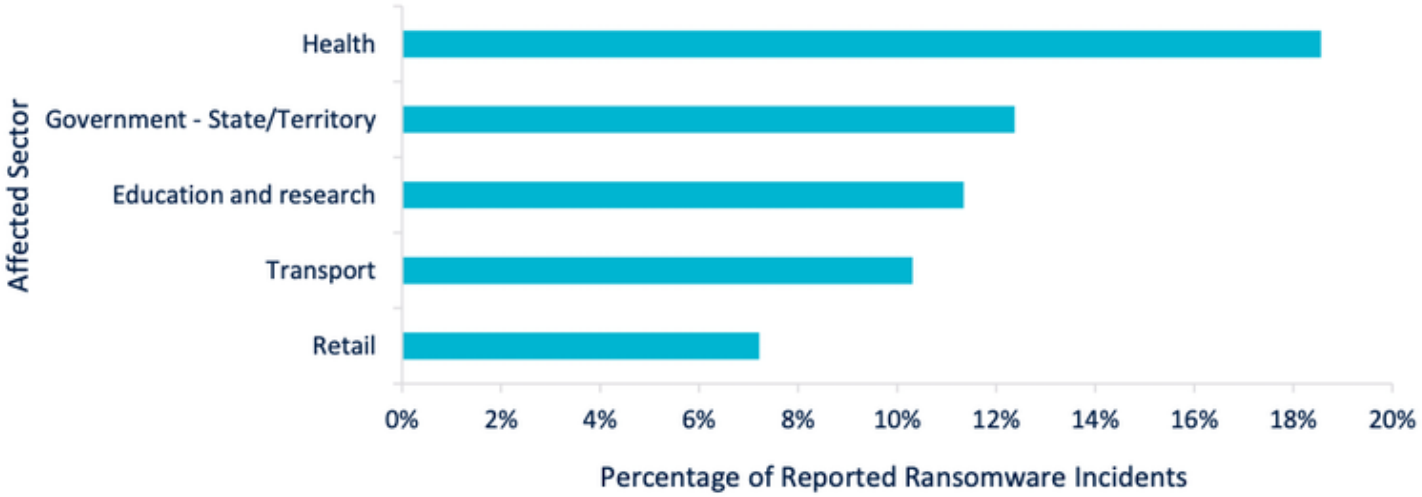


Screenshot of Cl0p Leaks website showing Software AG financial data available for public download (taken from dark web site).

This is an example of an increasingly common tactic referred to as “double extortion”, in which not only is data stolen and held to ransom, but there is the added threat the data will be posted in public or auctioned to interested parties. The threat of public exposure of the breach, coupled with the potential release of confidential data, can often encourage organisations to pay the ransom.

Potential consequences

A recent ACSC report on ransomware in Australia identified the health-care sector as the most targeted, by a significant margin. This is perhaps not surprising, given the sector’s lack of training, lax security practices and chronic underinvestment in technology and digital infrastructure.



ACSC report on impacted sectors for reported ransomware incidents – October 2020.
ACSC

Health-care providers face two significant consequences of cyber compromise. First, personal or sensitive data are valuable to criminals. Having such data leaked online is embarrassing and has significant legal implications for the organisation and the government.

A second, more serious, consequence can be seen when a ransomware attack impacts critical systems. The most notable example in recent years was the Wannacry attack in 2017 that targeted the UK National Health Service, among others.

The NHS suffered a major outage over several days following the Wannacry ransomware attack, resulting in thousands of operations and appointments being cancelled. Wannacry was estimated to have cost billions of dollars globally, with the UK NHS spending close to US$100 million to recover and strengthen its cyber defences.

Screenshot of Wannacry ransom demand.
Wikimedia

A ransomware incident earlier this year in Germany had deadly results. When ransomware crippled a hospital in Dusseldorf, an emergency patient was sent to another facility instead. She died, and her death has been attributed to the delay in treatment.

Australia has had similar incidents in the past. Last year saw seven hospitals affected by a ransomware attack.

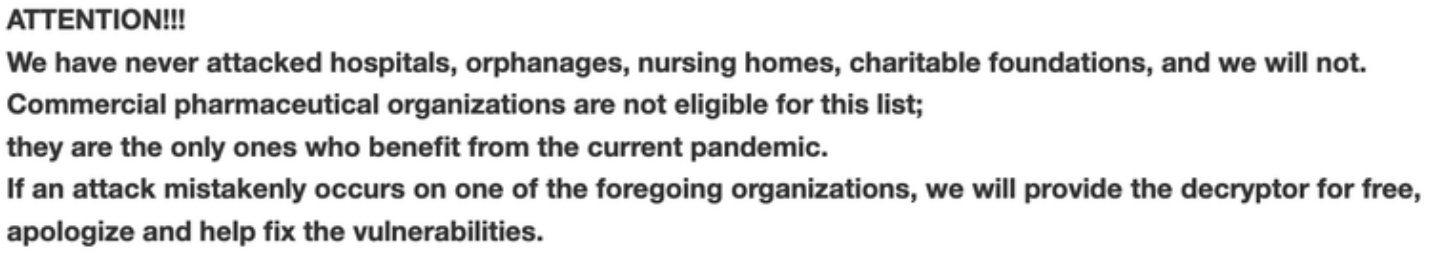
Should we be worried?

Cyber attacks are a constant threat, and most organisations are well aware of the risks to their business operations, intellectual property, sensitive data and reputation.

But in the health-care sector the stakes are higher. Losing data can cost lives, and patient records being stolen is a breach of privacy that can have long-lasting effects for the patient.

With systems intertwined and dependent on each other, just one compromised target can have major implications.

Interestingly, the Cl0p Leaks website (only available on the dark web through the TOR web browser) features the following reassuring statement in relation to hospitals – perhaps showing an ethical streak to the criminal group.



Cl0p Leaks screenshot (taken from Dark Web site)

Cyber criminals are usually motivated by profit. Ransomware attacks work because individuals within organisations make mistakes. When combined, there is a strong motivation for criminals to continue these actions and for organisations (and us) to continue to pay to clean up the mess that's left behind.

Paul Haskell-Dowland, Associate Dean (Computing and Security), *Edith Cowan University*