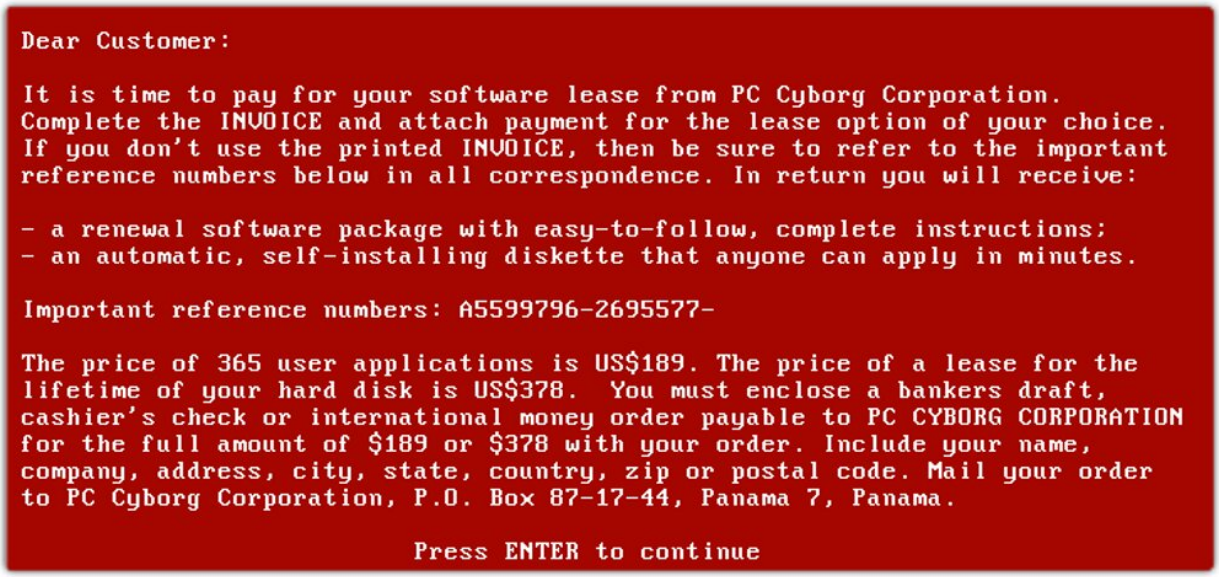
Australia is a sitting duck for ransomware attacks

July 14 2021, by Paul Haskell-Dowland and Andrew Woodward



The 1989 AIDS Trojan (PC Cyborg) ransom demand. Credit: Joseph L. Popp, AIDS Information Trojan author, Public domain, via Wikimedia Commons

Australian organizations are a soft target for ransomware attacks, say experts who yesterday issued a fresh warning that the government needs to do more to stop agencies and businesses falling prey to cyber-crime. But in truth, the danger has been growing worldwide for more than three decades.

Despite being a relatively new concept to the public, ransomware has

roots in the late 1980s and has evolved significantly over the past decade, reaping billions of dollars in ill-gotten gains.

With names like Bad Rabbit, Chimera and GoldenEye, ransomware has established a mythical quality with an allure of mystery and fascination. Unless, of course, you are the target.

Victims have few options available to them; refusing to pay the ransom depends on having good enough backup practices to recover the corrupted or stolen data.

According to a study by security company Coveware, 51% of businesses surveyed were hit with some type of ransomware in 2020. More concerningly still, typical ransom demands are climbing dramatically, from an average of US$6,000 in 2018, to US$84,000 in 2019, and a staggering US$178,000 in 2020.

A brief history of ransomware

The first known example of ransomware dates back to 1988-89. Joseph Popp, a biologist, distributed floppy disks containing a survey (the "AIDS Information Introductory Diskette") to determine AIDS infection risks. Some 20,000 of them were reportedly distributed at a World Health Organization conference and via postal mailing lists. Unbeknown to those receiving the disks, it contained a virus of its own. The AIDS Trojan lay dormant on systems before locking users' files and demanding a "license fee" to restore access.

Although the malware was inelegant and easily undone, it drew media attention at the time as a new type of cyber threat. The demand for payment (by cheque to a PO box in Panama) was primitive by comparison with modern approaches, which call for funds to be transferred electronically, often in cryptocurrencies.

It was well over a decade before ransomware truly began to proliferate. In the mid-2000s, stronger encryption allowed for more effective ransom campaigns with the use of asymmetric cryptography (in which two keys are used: one to encrypt, and a second, kept secret by the criminals, to decrypt), which meant even skilled systems administrators could no longer extract the keys from the malware.

CryptoLocker ransom demand. Credit: Nikolai Grigorik, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons

In 2013, CryptoLocker malware rose to global dominance, partly supported by the GameOver Zeus botnet. Cryptolocker encrypted users' files, sending the unlock key to a server controlled by the criminals with a three-day deadline before the key was destroyed. The network was shut down in 2014, thanks to a major global law enforcement effort called Operation Tovar. It is estimated to have impacted more than 250,000 victims and potentially garnered 42,000 Bitcoin, worth around US$2 billion at today's valuation.

In 2016 there were several high-profile incidents involving the Petya ransomware, which prevented users from accessing their hard drives. It was one of the first significant examples of Ransomware as a Service, whereby criminal gangs "sell" their ransomware tools as a managed service.

The following year saw arguably the most notorious ransomware attack of all time: the WannaCry attack. It struck hundreds of thousands of computers, including an estimated 70,000 systems at the UK National Health Service. The global impact of WannaCry has been estimated at up to US$4 billion.

More recent still was the Ryuk ransomware, which targeted local councils and national government agencies. But cyber-criminals have also attacked specific private companies, including the United States' largest refined oil distribution network, Colonial Pipeline, the multinational meat processor JBS Foods, and Australia's Channel Nine network.

Is all ransomware the same?

There are hundreds of types of ransomware, but they fit into a few broad categories:

Crypto ransomware

In modern crypto ransomware attacks, the malware encrypts users' files ("locking" the files to make them unreadable) and will typically involve a "key" to unlock the files being stored on a remote server controlled by the cyber-criminals. Early variants would require the victim to buy software to unlock the files.

Wannacry ransom demand with integrated multi-language support. Screenshot of a WannaCry ransomware attack on Windows 8. Credit: Public domain, via Wikimedia Commons

Locker ransomware

Locker ransomware is usually a more complex type of malware that targets a user's entire operating system (such as Windows, macOS or Android), hampering their ability to use their device. Examples can include preventing the computer from booting, or forcing a ransom demand window to appear in the foreground and preventing interaction with the other applications.

Although files are not encrypted, the system is typically unusable by most users (as you would likely need another system or software to extract the files). In some cases the ransom demands refer to government agencies with threats of investigations relating to tax fraud, possession of child abuse materials, or terrorist activities.

Leakware

In a leakware attack, the data are not encrypted but instead are stolen from the victim and held by cyber-criminals. It is the threat of public release alone that is used to secure a ransom payment. From 2020 to 2021, reported occurrences of non-encrypted ransoms have doubled.

Double extortion

Double extortion is an alarming development whereby not only is a payment required to secure release of encrypted organization data, but there is the added threat of public release.

This approach typically involves data being stolen from the organization during the malware infection process, then sent to servers run by the cyber-criminals. To encourage payment, extracts may be posted on public-facing websites to prove possession of the data—coupled with

threats to publish the remaining data.

Ransomware as a Service (RaaS)

Early ransomware was developed by individuals but, as with all software, ransomware has come of age. It is now a multibillion-dollar industry (an estimated US$20 billion in 2020) and is every bit as well designed and implemented as any commercial software.

Just as Microsoft's Office 365 has developed into a service, where instead of buying the software, you pay a monthly or yearly subscription, so has ransomware. Ransomware as a Service (RaaS) allows criminals to obtain services, typically in return for a cut of the ransom.

To pay, or not to pay?

Most law enforcement agencies recommend against ransom payments (just as many governments will not negotiate with terrorists), because it is likely to encourage future attacks. But many organizations nevertheless do pay up. Interestingly, the public sector hands over up to ten times more money to release their files than victims in the private sector.

Paying a ransom is frequently seen as the lesser of two evils, particularly for smaller organizations that would otherwise be shut down entirely by the disruption to their systems. Or, if you are lucky, the malware will already have a publicly available antidote.

> How to remove FBI Moneypak ransomware: http://t.co/UNu8ZVowtY pic.twitter.com/3bycJnEEUH
>
> — CGI Doctor (@CGIdoctor) August 2, 2013

But paying the ransom doesn't guarantee you'll get all your data back. By one estimate, an average of 65% of data was typically recovered after paying the ransom, and only 8% of organizations managed to restore all of it.

With criminal groups now reaping multimillion-dollar profits, ransomware attacks are likely to target larger organizations where the rewards are richer, perhaps focusing on holders of valuable intellectual property such as the health-care and medical research sectors. The Internet of Things (IoT) will likely be a target for cyber-criminals, with global networks of connected devices held to ransom.

While big organizations are likely to have appropriate technical safeguards, user education is still key—a lapse of judgment from a single person can still bring an organization to its knees. For smaller companies, seeking (and following) cyber advice is crucial.

Given the huge scale on which cyber-criminals are now operating, we have to hope law enforcement and software security engineers can stay one step ahead.

Provided by The Conversation