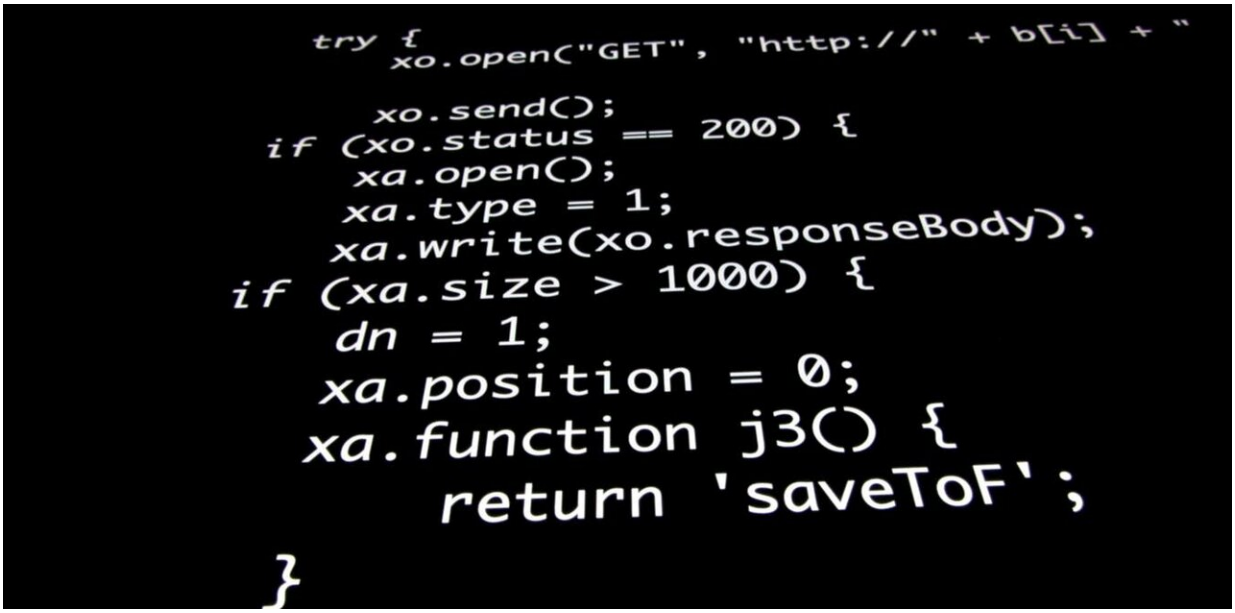
Hackers are now targeting councils and governments, threatening to leak citizen data

November 11 2019, by Roberto Musotto and Brian Nussbaum



Ransomware attacks are becoming increasingly complex, as hackers find creative ways to beat ordinary systems of defence. Credit: christiaancolen/flickr, CC BY

In recent weeks, Johannesburg's computer network was held for ransom by a hacker group called Shadow Kill Hackers. This was the second time in three months a ransomware attack has hit South Africa's largest city. This time, however, hackers didn't pose the usual threat.

Rather than denying the city access to its data, the standard blackmail in

a ransomware attack, they threatened to publish it online. This style of attack, known as leakware, allows hackers to target more victims in a single attack—in this case the city's citizens.

The latest Johannesburg attack was the second leakware attack of this type ever recorded, and a similar attack could hit Australia soon. And although our current cyberattack defences are more advanced than many countries, we could be taken by surprise because of the unique way leakware operates.

A new plan of attack

During the Johannesburg attack, city employees received a computer message saying hackers had "compromised all passwords and sensitive data such as finance and personal population information". In exchange for not uploading the stolen data online, destroying it and revealing how they executed the breach, the hackers demanded four bitcoins (worth about A$52,663) - "a small amount of money" for a vast city council, they said.

In this case, access to data was not denied. But the threat of releasing data online can put enormous pressure on authorities to comply, or they risk releasing citizens' sensitive information, and in doing so, betraying their trust.

The city of Johannesburg decided not to pay the ransom and to restore systems on its own. Yet we don't know whether the data has been released online or not. The attack suggests cybercriminals will continue to experiment and innovate in a bid to defeat current prevention and defense measures against leakware attacks.

Another notable leakware attack happened a decade ago against the US state of Virginia. Hackers stole prescription drug information from the

state and tried obtaining a ransom by threatening to either release it online, or sell it to the highest bidder.

The hacker group operated a Twitter account, on which they posted a photo showing the directories they had access to. Credit: ShadowKillGroup/twitter

When to trust the word of a cybercriminal?

Ransomware attack victims face two options: pay, or don't pay. If they choose the latter, they need to try other methods to recover the data

being kept from them.

If a ransom is paid, criminals will often decrypt the data as promised. They do this to encourage compliance in future victims. That said, paying a ransom doesn't guarantee the release or decryption of data.

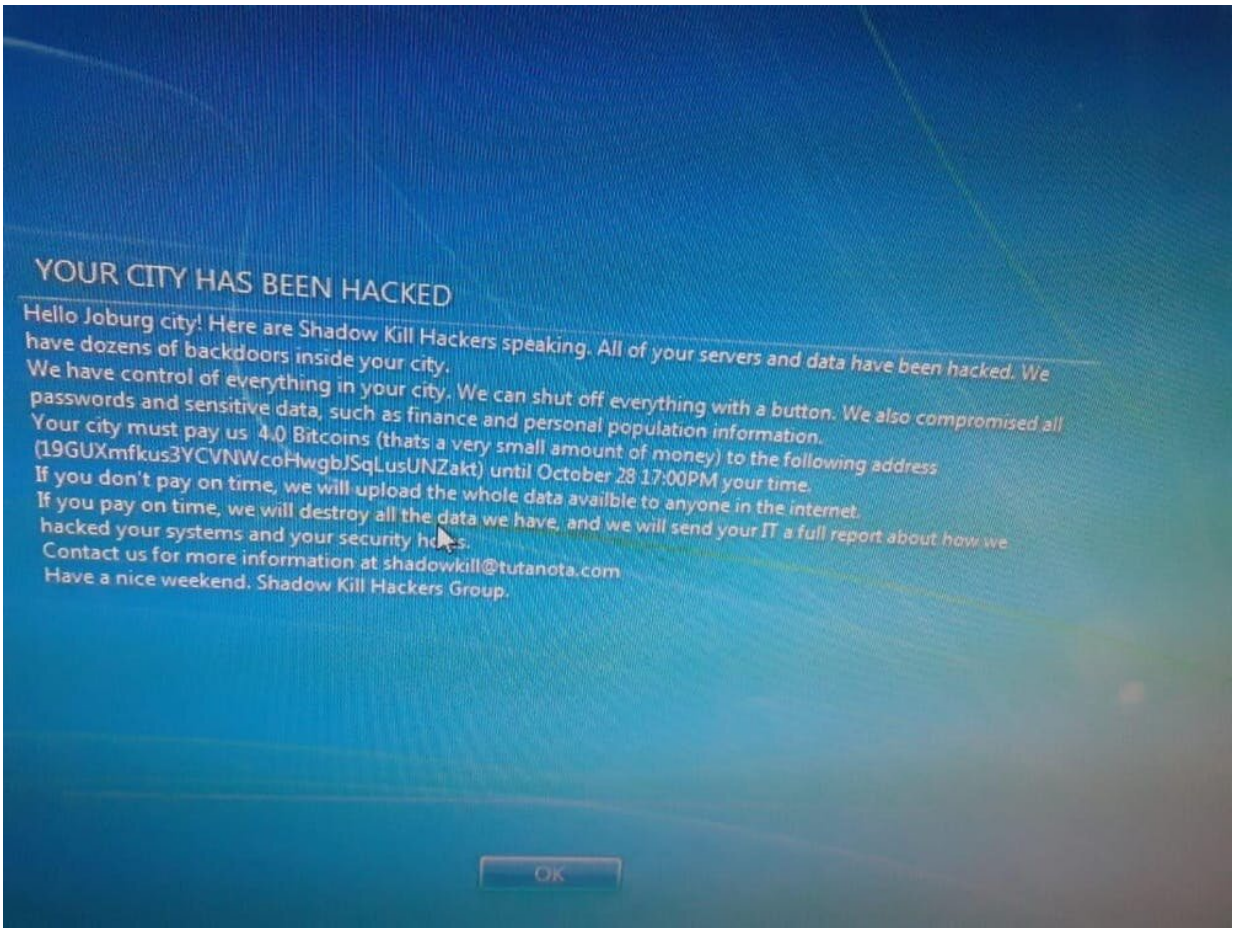
The type of attack experienced in Johannesburg poses a new incentive for criminals. Once the attackers have stolen the data, and have been paid the ransom, the data still has extractive value to them. This gives them duelling incentives about whether to publish the data or not, as publishing it would mean they could continue to extort value from the city by targeting citizens directly.

In cases where victims decide not to pay, the solution so far has been to have strong, separate and updated data backups, or use one of the passkeys available online. Passkeys are decryption tools that help regain access to files once they've been held at ransom, by applying a repository of keys to unlock the most common types of ransomware.

But these solutions don't address the negative outcomes of leakware attacks, because the "hostage" data is not meant to be released to the victim, but to the public. In this way, criminals manage to innovate their way out of being defeated by backups and decryption keys.

The traditional ransomware attack

Historically, ransomware attacks denied users access to their data, systems or services by locking them out of their computers, files or servers. This is done through obtaining passwords and login details and changing them fraudulently through the process of phishing.



This login screen message was displayed on computers in Johannesburg following the attack. Credit: pule_madumo/twitter

It can also be done by encrypting the data and converting it to a format that makes it inaccessible to the original user. In such cases, criminals contact the victim and pressure them into paying a ransom in exchange for their data. The criminal's success depends on both the value the data holds for the victim, and the victim's inability to retrieve the data from elsewhere.

Some cybercriminal groups have even developed complex online "customer support" assistance channels, to help victims buy

cryptocurrency or otherwise assist in the process of paying ransoms.

Trouble close to home

Facing the risk of losing sensitive information, companies and governments often pay ransoms. This is especially true in Australia. Last year, 81% of Australian companies that experienced a cyberattack were held at ransom, and 51% of these paid.

Generally, paying tends to increase the likelihood of future attacks, extending vulnerability to more targets. This is why ransomware is a rising global threat.

In the first quarter of 2019, ransomware attacks went up by 118%. They also became more targeted towards governments, and the healthcare and legal sectors. Attacks on these sectors are now more lucrative than ever.

The threat of leakware attacks is increasing. And as they become more advanced, Australian city councils and organizations should adapt their defenses to brace for a new wave of sophisticated onslaught.

As history has taught us, it's better to be safe than sorry.

Provided by The Conversation

Citation: Hackers are now targeting councils and governments, threatening to leak citizen data (2019, November 11) retrieved 4 May 2024 from https://techxplore.com/news/2019-11-hackers-councils-threatening-leak-citizen.html