AstraLocker 2.0 ransomware isn't going to give you your files back

blog.malwarebytes.com/ransomware/2022/07/astralocker-2-0-ransomware-isnt-going-to-give-you-your-files-back/

Christopher Boyd July 1, 2022

Reversing Labs reports that the latest verison of AstraLocker ransomware is engaged in a a so-called "smash and grab" ransomware operation.

Smash and grab is all about maxing out profit in the fastest time. It works on the assumption by malware authors that security software or victims will find the malware quickly, so it's better to get right to the end-game as quickly as possible. Adware bundles in the early 2000s capitalised on this approach, with revenue paid for dozens of adverts popping on desktops in as short a time as possible.

That smash and grab spirit lives on.

In a ransomware attack, criminals typically break into a victim's network via a trojan that has already infected a computer, by exploiting a software vulnerability on an Internet-facing server, or with stolen Remote Desktop Protocol (RDP) credentials. They then make their way silently to devices and servers where important data is stored. Anything of value is stolen and sent outside of the network. When the attacker is good and ready, ransomware is deployed, encrypting the files on the machines and rendering them useless. From here,

double or even triple threat extortion (blackmail and the threat of data leakage) is deployed. This careful approach, which can sometimes take weeks, allows attackers to stop organisations dead in their tracks and demand multi-million dollar ransoms.

It is so successful that almost all major ransomware families are used in this way.

But AstraLocker is not a major ransomware family, and it doesn't do this. (These two things may be connected.)

Click to run

In the attacks observed by Reversing Labs, AstraLocker just arrives and encrypts.

It starts life as a rogue Word document attachmed to an email. The payload lurking in the document is an embedded OLE object. Triggering the ransomware requires the victim to double click the icon within the document, which comes with a security warning. As researchers note, this isn't as slick a process as the recent Follina vulnerability (which requires no user interaction), or even misusing macros (which some user interaction).

In its rush to encrypt, AstraLocker still manages to do some standard ransomware things: It tries to disable security programs; it also stops applications running that might prevent encryption from taking place; and it avoids virtual machines, which might indicate it's being run by researchers in a lab.

The sense of this being a rushed job doesn't stop there.

Reaffirming (and then breaking) the circle of trust

When decryption doesn't happen, either because of a poor quality decryptor, or because no decryption process actually exists, the ransomware author's so-called circle of trust is broken. Too many decryption misfires is bad for business. After all, why would victims pay up if there's no chance of file recovery?

It's interesting, then, that the following text is in AstraLocker 2.0's ransom note:

> **What guarantees?**
> I value my reputation. If I do not do my work and liabilities, nobody will pay me. This is not in my interests. All my decryption software is perfectly tested and will decrypt your data.

So far, so good…you would think. Unfortunately, there's a sting in the tail.

The cost of their decryption software is "about $50 USD", payable via Monero or Bitcoin. There is some question as to who the author of this version of AstraLocker is, as the email addresses tied to the original campaign have been replaced. Unfortunately, this is where the

circle of trust falls apart.

You can certainly pay the ransom with no problem whatsoever. That side of things, the making money side, works perfectly. The getting your files back side of things? Not so much. The new contact email address mentioned above is only partially included.

There is currently no way to ask the ransomware author for the decryption tool. Unless some sort of update is forthcoming, this is the quickest way you'll ever lose both your files and $50.

Whether this is by accident or design, the circle of trust here is more of a downward curve.