The rise of ransomware as a service

By David Strom 25 Mar 2021

The RaaS model means that almost anyone can enter the market and leverage the coding prowess of others

Ransomware continues to be a blight across the security landscape. Due to the pandemic, it has gotten new life and a growing collection of capabilities to make malware operators more formidable.

While the use of both cloud computing (also known as ransomware as a service, or for short, RaaS) and extortion techniques aren't new, they're being deployed more often and in more clever and targeted ways than ever before. This has brought a rise in overall ransom attacks and in demanded payouts.

RaaS uses a combination of a software subscription service, similar to other cloud service providers, and an affiliate program to sign up malware distributors. The affiliates earn commissions, just as they would if they were selling books on Amazon or crafts on Etsy. Typically, the commissions range from 10% to 40% of any successful ransom payouts received. The biggest difference from the legit world is that they are typically made in cryptocurrencies.

The RaaS model means that almost anyone can enter this market and leverage the coding prowess of others. The affiliates don't have to worry about building and maintaining any malware infrastructure — each affiliate is given a custom identifier code, similar to how the legit programs work. This ensures that the affiliate is given credit and collects the appropriate commissions for their attacks.

In a nutshell, the various RaaS groups can be categorized into three groups:

1. Emerging crews that are just getting started and have just a few notable incidents. These include Exorcist, Lolkek and Rush.
2. Rising power centers which have had successful attacks and maintain blogs that advertise their services and shame their victims. This group includes Darkside, Thanos, and Clop.
3. Top-tier organizations that have had numerous and well-publicized attacks and have been targeted by law enforcement, such as DoppelPaymer, Revil and Ryuk.

A detailed look at Darkside

The Darkside group deserves special attention. It has three important characteristics:

1. Very refined victim targeting, which seeks out the wealthiest data sources to extort
2. A more "corporate-like" approach in their operations, including a well-developed affiliate operation (paying about 25% affiliate commissions)
3. Customized ransomware delivery for each target and a fair amount of investigative work before selecting targets.

Darkside states that that they won't target hospitals or schools, but that hasn't always been the case. They also avoid Russian-language targets and have been recruiting Russian speaking programmers.


darkside
Image via bankinfosecurity.com

Darkside announced their creation thanks to a "press release" published on Tor back in the summer of 2020. This ploy is quite clever because releases tend to attract IT press coverage and also can be used to tout the provenance of any stolen data. (The Revil groups also uses this tactic.) Of course, accepting what they promise is probably not a good idea.


darkside2
Image via bankinfosecurity.com

The release is just one part of how "corporate" that Darkside appears — they also provide text chat support to their affiliates and create customized data storage mechanisms to hide the stolen data of their targets. Darkside also has developed both Windows and Linux-based exploits. Their initial compromise of Windows PCs installs a PowerShell script that immediately deletes Volume Shadow Copies and prepares various database and email repositories for encryption and copying offsite. The malware typically enters an organization through a compromised third-party account and tries to access a Virtual Desktop session.

Darkside also tried to donate funds to two charities last summer, but these donations are typically returned and aren't legal in most jurisdictions, since they rely on stolen funds. Speaking of stolen funds, one report has Darkside using Iranian hosting facilities for their criminal network, where command and control servers and stolen data are hosted. This helps keep their network out of the hands of authorities in the US and EU that are likely to try to stop their activities.

The group has had a spike in activity between October and December 2020, when the amount of Darkside sample submissions had more than quadrupled. Past ransom demands have ranged from $200,000 to $2 million, depending on the size of the compromised organizations.

However, they are once again picking up steam: In March 2021, the managed services vendor CompuCom fell victim to a Darkside attack. The company eventually revealed in a FAQ posted to its customers that Darkside was the suspected origin.

If you are compromised by Darkside, prepare yourself as you would against other forms of ransomware: Ensure your backups are intact and accurate, intensify phishing awareness and education, and lock down your accounts with MFA.
