CYBER SECURITY HUB

Five active ransomware gangs and their tactics (part one)

Discover some of the most recent cyber attacks carried out by the top cyber criminals active today

Crystel Saraie
06/20/2022

As ransomware gangs continue to threaten organization’s cyber security, it is important to make note of the most prominent groups at the moment and their techniques.

Today’s ransomware gangs continue to evolve and Ransomware-as-a-Service (RaaS), double extortion and cross-platform functionality are now common traits.

In this article we review just five of the top ransomware gangs active today, some of their recent attacks and the tactics they are deploying.

Hive

Hive, who first emerged in June 2021, has been become renown as an incredibly aggressive group targeting the healthcare sector.

On 31 May Hive attacked the Costa Rican Social Security Fund, Costa Rica's public health service. Other notable cases include the attack on the Missouri Delta Medical Center, where patient data was leaked, and the Memorial Health System in Ohio, where urgent surgeries and radiology exams had to be cancelled.

Healthcare organizations have been warned against the gang, and advised to apply strong cybersecurity systems and defenses by the US Department of Health and Human Services. Hive operates as RaaS and uses the double extortion method, where data is stolen as well as encrypted. Their malware design uses the Golang programming language.

AlphV (BlackCat)

AlphV, also known as BlackCat, was first observed by Microsoft in November 2021. It also works as a RaaS and uses the double extortion method. This organisation is unique for being the first ransomware gang using the RUST programming language.

The gang has attacked many high-profile organizations, such as fashion brand Moncler and the Swissport airline cargo handling service provider. In May 2022 the Austrian federal state Carinthia was targeted and BlackCat demanded US$5mn for the decryption of stollen data.

BlackCat continues to gain attention and on 14 June they debuted a dedicated website for victims to search for their stolen data, taking ransomware operations to the next level. The site exposes the personal information of organization employees and clients, such as names, US Social Security Numbers, addresses, emails, and more.

Lapsus$

Lapsus$ first became active in December 2021. The cybercriminals their private Telegram channel to communicate with the public, rather than traditional data leak websites. They also conduct polls, giving members a choice in who should be targeted next.

According to Microsoft the hacking group is known for using a pure extortion and destruction model without deploying ransomware payloads. The gang typically focuses on compromising user identities but using compromised credentials.

In late March 2022, seven people aged 16 to 21 were arrested in the UK in relation to the gang's activities, despite the gang initially believed to be based in Brazil as one of its first victims was the nation's Ministry of Health.

The UK arrests have not brought the group down as days later Lapsus$ released a 73GB archive from software services company Globant, whose clients include Disney and Google. The group, therefore, is seemingly still active.

Conti

Conti, thought to led by cybercriminal Wizard Spider, accounted for 20% of attacks in the first three months of 2022, according to Digital Shadows.

Operating on a double extortion system, they use a multithreading method, which allows a fast spread of malware.

The group is believed to have ties to Russia as it released a statement in solid support of the Kremlin's decision to invade Ukraine. They are responsible for a number of high-profile ransomware attacks, including the City of Tulsa and Japanese multinational electronics company JVCKenwood.

In May 2022, Costa Rica declared a national emergency after their government systems were attacked by Conti.

However, in the midst of this, the group disbanded.

The Conti cybercrime syndicate will, however, continue to live on, with reports of partnerships with smaller ransomware gangs, such as Hive, BlackCat, BlackByte, and more.

Members will spread to these gangs and work as part of those organizations but will still be a part of the larger Conti syndicate. The Costa Rica attack has been theorized to be a publicity stunt as Conti members slowly migrated to other gangs.

LockBit

A RaaS organization using double extortion methods, LockBit was responsible for 38% of ransomware attacks between January and March

2022 according to Digital Shadows. They have been present since 2019. Their malware tool Stealbit automates data exfiltration.

It was released allongside LockBit 2.0, which has been coined as the fastest and most efficient encryption system by its creators.

They have attacked large cooperations including tyre manufacturer Bridgestone Americas and the French electronics multinational Thales Group. Lockbit has also hit the French Ministry of Justice, threatening to release sensitive data.