Who Will Bend the Knee in RaaS Game of Thrones in 2022?

Stories

The latest cybersecurity trends, best practices, security vulnerabilities, and more

ARCHIVED STORY

By **John Fokker** and **Raj Samani** · November 07, 2021

McAfee Enterprise and FireEye recently released its 2022 Threat Predictions. In this blog, we take a deeper dive into a Game of Thrones power struggle among Ransomware-as-a-Service bad actors in 2022.

Prediction: Self-reliant cybercrime groups will shift the balance of power within the RaaS eco-kingdom.

For several years, ransomware attacks have dominated the headlines as arguably the most impactful cyber threats. The Ransomware-as-a-Service (RaaS) model at the time opened the cybercrime career path to lesser skilled criminals which eventually led to more breaches and higher criminal profits.

For a long time, RaaS admins and developers were prioritized as the top targets, often neglecting the affiliates since they were perceived as less skilled. This, combined with the lack of disruptions in the RaaS ecosystem, created an atmosphere where those lesser-skilled affiliates could thrive and grow into very competent cybercriminals, eventually with a mind of their own.

In a response to the Colonial Pipeline attack, the popular cybercrime forums have banned ransomware actors from advertising. Now, the RaaS groups no longer have a third-party platform on which to actively recruit, show their seniority, offer escrow, have their binaries tested by moderators, or settle disputes. The lack of visibility has made it harder for RaaS groups to establish or maintain credibility and will make it harder for RaaS developers to maintain their current top tier position in the underground.

These events have undermined their trusted position. Ransomware has generated billions of dollars in recent years and it's only a matter of time before more individuals who believe they aren't getting their fair share become unhappy.

The first signs of this happening are already visible as described in our blog on the Groove Gang, a cyber-criminal gang that branched off from classic RaaS to specialize in computer network exploitation (CNE), exfiltrate sensitive data and, if lucrative, partner with a ransomware team to encrypt the organization's network. McAfee Enterprise ATR believes, with high confidence, that the Groove gang is associated with the Babuk gang, either as a former affiliate or subgroup. These cybercriminals are happy to put aside previous Ransomware-as-a-Service hierarchies to focus on the ill-gotten gains to be made from controlling victim's networks, rather than the previous approach which prioritized control of the ransomware itself.

Trust in a few things remains important even among cybercriminals underground, such as keeping your word and paying people what they deserve. Cybercriminals aren't immune from feeling like employees whose contributions aren't being adequately rewarded. When this happens, these bad actors cause problems within the organization. Ransomware has been generating billions of dollars in recent years and with revenue like that, it was inevitable that some individuals who believe they aren't getting their fair share become unhappy and let the cybercrime world know it.

Recently, a former Conti affiliate was unhappy with their financial portion and decided to disclose the complete Conti attack playbook and their Cobalt Strike infrastructure online. In the past, McAfee ATR has been approached by individuals affiliated with certain RaaS groups expressing grudges with other RaaS members and admins, claiming they haven't been paid in time or that their share wasn't proportionate to the amount of work they put in.

In 2022, expect more self-reliant cybercrime groups to rise and shift the balance of power within the RaaS eco-climate from those who control the ransomware to those who control the victim's networks.

Less-skilled Operators Won't Have to Bend the Knee in RaaS Model Power Shift

The Ransomware-as-a-Service eco system has evolved with the use of affiliates, the middlemen and women that work with the developers for a share of the profits. While this structure was honed during the growth of GandCrab, we are witnessing potential chasms in what is becoming a not-so-perfect union.

Historically, the ransomware developers, held the cards, thanks to their ability to selectively determine the affiliates in their operations, even holding "job interviews" to establish technical expertise. Using CTB locker as an example, prominence was placed on affiliates generating sufficient installs via a botnet, exploit kits or stolen credentials. But affiliates recently taking on the role and displaying the ability to penetrate and compromise a complete network using a variety of malicious and non-malicious tools essentially changed the typical affiliate profile towards a highly skilled pen-tester/sysadmin.

The hierarchy of a conventional organized crime group often is described as a pyramid structure. Historically, La Cosa Nostra, drug cartels and outlaw motor gangs were organized in such a fashion. However, due to further professionalization and specialization of the logistics involved with committing crime, groups have evolved into more opportunistic network-based groups that will work together more fluidly, according to their current needs.

While criminals collaborating in the world of cybercrime isn't new, a RaaS group's hierarchy has been more rigid compared to other forms of cybercrime, due to the power imbalance between the group's developers/admins and affiliates. But things are changing. RaaS admins and developers were prioritized as the top targets, but often neglected the affiliates who they perceived to be less-skilled. This, combined with the lack of disruptions in the RaaS ecosystem, created an atmosphere where those lesser-skilled affiliates could thrive and grow into very competent cybercriminals.

As more ransomware players have entered the market, we suspect that the most talented affiliates are now able to auction their services for a bigger part of the profits, and maybe demand a broader say in operations. For example, the introduction of Active Directory enumeration within DarkSide ransomware could be intended to remove the dependency on the technical expertise of affiliates. These shifts signal a potential migration back to the early days of ransomware, with less-skilled operators increasing in demand using the expertise encoded by the ransomware developers.

Will this work? Frankly, it will be challenging to replicate the technical expertise of a skilled penetration tester, and maybe – just maybe – the impact will not be as severe as recent cases.