CYJAX

Digital Intelligence
Securing the Future

Cyjax Darknet Review - Q3 2020

CLIENT CONFIDENTIAL

Like any exchange of goods and services, the darknet is not exempt from simple economic realities. Unlike state-sponsored threat actors, cybercriminals are generally motivated by one thing: profit. Yet the past few months have demonstrated that major developments on the darknet are likely to have a significant influence on the way in which cybercriminals operate, where they sell their products, and even the types of products they sell.

Fall of an Empire

For darknet markets, the single biggest development this quarter was the disappearance of Empire market. Having been set up in April 2019, Empire outlasted numerous rivals and eventually became the dominant darknet market. However, in August 2020, Empire went offline. This was not unusual, as the market had been subject to repeated DDoS attacks. However, one of the market moderators made a post on Dread claiming that the Empire admin had not been online for over two days. Soon after, this account was deleted, and Empire market has not been active since.

Empire's disappearance had significant repercussions on the darknet market community. It had been one of the top markets for over a year, and the dominant market for much of 2020. As such, there was no clear successor which Empire customers could migrate to, and no one market has yet managed to fill the void it left. White House market has experienced significant growth but still lags far behind the size of Empire at its peak. This can be partially explained by White House market's extensive security measures, including a requirement for all buyers to use PGP encryption, which a surprising number of casual buyers still seem reluctant to use.

Other markets, including Monopoly, Dark0de Reborn and Invictus all benefited from Empire's disappearance. But none of these has been able to consolidate a clear lead over their competitors. At this stage, none of the existing crop of markets appear likely to establish the stranglehold that Empire enjoyed. Of course, this could change swiftly, as the darknet market landscape is constantly shifting as new markets are introduced and existing ones disappear.

Rise of Ransomware

One of the dominant trends of 2020 has been an explosive increase in the number of ransomware attacks. A major driver of this has been the rapid introduction of multiple new ransomware groups, many of whom operate as a Ransomware-as-a-Service (RaaS).

The RaaS model involves the operators of a ransomware variant charging other cybercriminals, known in this context as affiliates, for access to the ransomware. Generally, affiliates pay either a fixed fee or a rolling subscription charge, alongside a percentage of each ransom they collect. In exchange, the operators provide access to the ransomware, customer support and software updates. Unlike traditional ransomware groups, the RaaS model provides operators with an additional source of income via affiliate fees.

Many of these RaaS groups are actively recruiting affiliates on the darknet. Well-established groups, such as REvil (aka Sodinokibi), can afford to be more selective with their recruiting. In comparison, smaller groups, such as Avaddon, are less strict in terms of accepting new affiliates, instead prioritising growth. For smaller ransomware groups, the RaaS model provides an invaluable path for growing their operation by increasing the volume of attacks they can conduct. While ransomware remains profitable, these smaller groups will continue to appear and contribute to the growing threat posed by ransomware to individuals and businesses around the world.

Access as a commodity

There has also been a notable increase in access sales being conducted on the darknet. Access sales are essentially where a user, referred to as an access broker, gains access to an organisation and then sells this access to other interested third parties. The name of the organisation is rarely disclosed. Instead, access brokers provide other information, including type of industry, general geographic location, as well as revenue and employment figures. Often, though not always, this access is to a compromised domain administrator account.

As the number of ransomware groups has grown, so too has the number of access sales conducted on the darknet. There is some indication of causality between these trends. The explosive growth in the number of ransomware groups has led to an increase in demand for access as a commodity. This can be seen with several well-established access brokers, many of whom have exclusive contracts with ransomware groups to give them right of first refusal on access sales. Moreover, for users with limited technical knowledge seeking to become affiliates of a ransomware group, purchasing access can be used to enhance their credentials. Again, this increases the demand for access as a commodity, which results in more users becoming access brokers because this is where the most money can be made.

What to expect in Q4 and beyond?

The disappearance of Empire had a significantly disruptive effect on the darknet, but it remains unclear whether it will have any long-term substantive impact. Notably, one darknet market substitute which has grown increasingly popular over the past few months is Televend. Unlike traditional darknet markets, Televend specialises in the creation of Telegram vendor bots, which are automated accounts that buyers can message to view products and place orders. The growing popularity of Televend, combined with the ongoing instability of darknet markets, will likely exacerbate the long-term trend of vendors moving towards instant messaging platforms. However, there have also been recent reports of Telegram assisting German authorities in conducting seizure operations against certain channels, which may dissuade vendors from moving to instant messaging platforms.

The threat posed by ransomware is expected to increase in the short- to medium-term. It is also highly likely that new ransomware groups will emerge, and many will adopt the RaaS model as a means of fuelling growth. But despite smaller ransomware groups being less strict when recruiting, many still struggle to gain a significant number of affiliates. Therefore, the gap between well-established ransomware groups and smaller groups will grow, both in terms of the scale of operations and volume of attacks.

STATEMENT OF CONFIDENTIALITY

This document contains confidential trade secrets and proprietary information of Cyjax Limited. The recipient is expected to treat this document as they would their own confidential internal material. Neither this document, nor any diagrams contained in this document, may be disclosed to any person outside of the recipient's organisation without express written permission from Cyjax Limited. By accepting this document, the recipient affirms that they will comply with these expectations.

Cyjax Limited, Registered in England and Wales no 08302026.
Registered Office Suite 53 Peek House, 20 Eastcheap, London EC3M 1EB.
United Kingdom.

CYJAX
Cyjax Limited
Suite 53 Peek House
20 Eastcheap
London EC3M 1EB
info@cyjax.com
+44 (0)20 7096 0668
CYJAX.COM