# Steal, then strike: Access merchants are first clues to future ransomware attacks

intel471.com/blog/ransomware-attack-access-merchants-infostealer-escrow-service

Cybercrime does not happen in a vacuum.

While ransomware variants like REvil, Ryuk and DoppelPaymer have become household names for cybersecurity professionals, those deploying ransomware only represent part of the process by which criminals are forcing organizations to either pay them millions or watch their business go under.

The broader picture shows an underground marketplace that is increasingly becoming more organized, borrowing best practices from legitimate businesses that understand the importance of resiliency, efficiency and return on investment. A key cog in this growing operation is the interdependency between those who specialize in selling access to compromised systems or stolen information, and those looking to launch ransomware attacks.

Data gathered by Intel 471 points to a pattern in numerous ransomware attacks that have occurred in the past 18 months: Criminals in underground forums will advertise access to various breached organizations, and quickly turn to sell access to the highest bidder or strike a deal with an ransomware affiliate in order to share in any profits pulled from a successful payment. These partnerships have resulted in a flourishing submarket, where access to corporate networks is sold for six-figure sums directly or via a partnership and cut of paid ransoms.

The compromised credentials are mostly obtained through attackers abusing flaws or security shortcomings in virtual private networks or remote desktop protocol endpoints, which provides the initial entry point into enterprise networks. Additionally, credential information can come from logs tied to infostealer malware, password spraying or other credential marketplaces in the criminal underground.

Instances show that anywhere from one week to six months after access is obtained and advertised, other known actors on various underground forums look to use or purchase that access to launch ransomware attacks. The targets run the gamut of regions and economic sectors, with the pattern playing out in ransomware attacks on every continent.

One of the highest-profile ransomware attacks to fit this pattern was the attack on Pemex, the state-run oil company based in Mexico. In November 2019, attackers hit Pemex with DoppelPaymer, demanding $4.5 million in bitcoin to decrypt and return the files.

Intelligence from Intel 471 found that beginning in June 2019, a separate actor was advertising access to 1,500 Pemex servers and personal computers, as well as administrator privileges to the company's domains, for $150,000. That transaction was facilitated through a third-party escrow service, which allows criminals to move money in order to shield themselves from making direct contact with the actors who are carrying out the crimes.

Another actor Intel 471 had been tracking started asking for access to ransomware-as-a-service affiliate programs, stating that deployment of ransomware on compromised networks should potentially return much more money than just selling the access. Days after this, Intel471 learned the actor obtained and modified a version of Thanos, and allegedly deployed it against U.S. businesses. Over the past three months, this actor has frequently tried to sell access to compromised organizations, which range in location, size, and economic sector.

Access merchant partnerships are not exclusive to any one particular ransomware variant or ransomware-as-a-service. Data from Intel 471 shows this pattern following attacks carried out with popular ransomware variants, such as DoppelPaymer, Maze, Netwalker, Ryuk and REvil, as well as lesser-known variants like LockBit, Nefilim, Pysa and Thanos.

The astronomical growth in ransom payments in 2020 has helped access merchants put a premium on their services. In years past, a large ransom payout would earn attackers somewhere between five- and six-figure sums. Now, it's becoming increasingly common for attackers to demand seven- and eight-figure ransoms, partly due to the need to pay off actors that have helped them obtain access to the victim's system.

One such attack drives home this point: Intel 471 obtained a chat log from a ransomware attack launched last month where a company — a U.S.-based healthcare provider — offered to pay a ransom of just under $400,000. Despite the company's quick response, the ransomware crew was insulted by the offer and threatened to dump the entire cache of stolen documents unless the figure was pushed several million dollars higher. With their backs against the wall, the company eventually settled to pay $2 million in bitcoin.

How long ransomware crews decide to stay with this partnership model will be something to watch in the coming year. Intel 471 has observed actions in underground marketplaces that show RaaS groups are beginning to undercut access merchants, by either purchasing their own credential-stealing malware or recruiting teams that specialize in obtaining access. Use of access merchants may not disappear completely, but the extent of their popularity could diminish.

To prevent being a victim, enterprises need to have continuous and proactive observation of the cybercriminal underground marketplace where these interdependent products, services and goods intersect. Additionally, ensuring token-based multi-factor authentication is enabled across an enterprise and scrutinizing all internet-facing remote network connections like RDP can be vital in preventing ransomware attacks.

*This article was part of a series on ransomware attacks in 2020. You can find the previous entries here: Part 1 and Part 2.*