Cybercrime underground flush with shipping companies' credentials

intel471.com/blog/shipping-companies-ransomware-credentials

One of the lingering impacts of the COVID-19 pandemic is the havoc it has wreaked on the global supply chain. There have been extreme fluctuations in the availability of goods, ports around the world are severely backlogged with full containers, and shipping and logistics companies are having trouble finding workers to transport cargo. It is a precarious situation for this sector, especially as the holiday season approaches.

With things as volatile as they are, a cybersecurity crisis at one of these logistics and shipping companies could have a calamitous impact on the global consumer economy. Over the past few months, Intel 471 has observed network access brokers selling credentials or other forms of access to shipping and logistics companies on the cybercrime underground. These companies operate air, ground and maritime cargo transport on several continents that are responsible for moving billions of dollars worth of goods around the world.

The actors responsible for selling these credentials range from newcomers to the most prolific network access brokers that Intel 471 tracks. These actors have obtained these credentials by leveraging well-known vulnerabilities in remote access solutions like Remote Desktop Protocol (RDP), VPN, Citrix, and SonicWall, among others.

Among the advertisements observed by Intel 471:

> **Within the span of two weeks in July 2021**, one new actor and one well-known access broker claimed to have access to a network owned by a Japanese container transportation and shipping company. The new actor included the company's credentials in a dump of approximately 50 companies, allegedly all obtained via compromised Citrix, Cisco, virtual private network (VPN) and/or remote desktop protocol (RDP) accounts. The well-known actor claimed to have access to several accounts belonging to the company, but did not reveal how they were obtained.

In August 2021, one actor known to work with groups that have deployed Conti ransomware claimed access to corporate networks belonging to a U.S.-based transportation management and trucking software supplier and a U.S.-based commodity transportation services company. The actor gave the group access to an undisclosed botnet powered by malware that included a virtual network computing (VNC) function. The group used the botnet to download and execute a Cobalt Strike beacon on infected machines, so group members in charge of breaching computer networks received access directly via a Cobalt Strike beacon session.

In September 2021, an actor with ties to the FiveHands ransomware group claimed access to hundreds of companies, including a U.K.-based logistics company. It's most likely that access was obtained through a SonicWall vulnerability, given that FiveHands is known to use that access to launch its ransomware attacks. Additionally in September, a new actor claimed to have gained access to a Bangladesh-based shipping and logistics company through a vulnerability in the PulseSecure VPN.

In October 2021, a newcomer to a well-known cybercrime forum claimed access to the network of a U.S.-based freight forwarding company, alleging that he had had local administrator rights and could access 20 computers on the company's network. The actor claimed he obtained the credentials through a path traversal vulnerability in Fortinet's FortiGate secure sockets layer (SSL) VPN web portal (CVE-2018-13379). Also in October, a newcomer on a different well-known cybercrime forum claimed access to a Malaysian logistics company. Those credentials were part of a package that the actor was selling for $5,000. It was unknown how he allegedly obtained those credentials.

The world has previously seen the economic damage that can come from a cyber attack on the shipping and logistics industry. The NotPetya attack in 2017 devastated Danish shipping and maritime giant Maersk, shutting down several of its ports and costing the company $300 million to replace systems damaged by the malware. Adam Banks, head of technology at Maersk, told a business publication in 2019 that "there was 100 [percent] destruction of anything based on Microsoft that was attached to the network."

We have seen attackers try to go after ports this year. In August, suspected foreign government-backed hackers breached a computer network at the Port of Houston, one of the largest ports on the U.S. Gulf Coast. However, early detection of the incident thwarted any attempts to impede business operations.

Those two incidents show that the logistics industry is constantly targeted, and the ramifications of a cyberattack can have a crippling ripple effect on the global economy. At a time when this sector is struggling to keep things operating, a successful attack could bring this industry to a screeching halt, resulting in unforeseen dire consequences for every part of the consumer economy. It's extremely beneficial that security teams in the shipping industry

monitor and track adversaries, their tools and malicious behavior to stop attacks from these criminals. Proactively addressing vulnerabilities in times of high alert avoids further stress on already constrained business operations.