RANSOMWARE REALITIES: Understanding Ransomware and Preventing Damaging Attacks

frontline
MANAGED SERVICES

Understanding the Latest Trends in Ransomware Attacks

Ransomware attacks are generally deployed by malicious actors for financial gain through:

- An email phishing campaign;
- A known software vulnerability; and,
- Configuration scanning to identify an unsecure Remote Desktop Protocol (RDP) configuration. For example, if RDP, a capability that allows IT administrators to manage your desktop remotely, is not configured correctly, attackers can compromise administrator accounts and use the RDP or other update management capabilities to distribute their malicious software across an environment.

Unlike data exfiltration exercises or other types of malicious attacks that may take weeks or months to discover, once a ransomware attack begins, the intended targets will know it is happening. Locking users out of the system is commonly a disruptive experience.

Once the attackers have identified their entry points into the network environment, they may aim for a wide lateral distribution to install the ransomware onto as many valuable systems as possible before activating any of it. In some instances, sophisticated advanced threat groups or independent attack groups may obtain data, sell it off and then detonate ransomware for final financial exploit and to cover their tracks.

In most ransomware attacks, though, the objective is to compromise the system as much as possible. Spray-and-pray phishing campaigns that target general email addresses—such as sales@companyname.com or a list of tens of thousands of company names—tend to be a less effective method for gaining entry to a system. In response, there has been a shift toward more targeted attacks where the attacker identifies a company, group of companies or a unified supply chain to attempt to install ransomware into as many systems as possible to improve chances of access.

Another growing trend is for a ransomware attacker to confirm their access to information by encrypting the data where it resides on the system and publishing a small amount of the information. Whereas companies may not have been certain that information was actually compromised before, attackers now aim to increase their leverage by showing their hand before demanding a payment to decrypt the information and threatening to publish all of it on a public-facing website if the fee isn't paid.

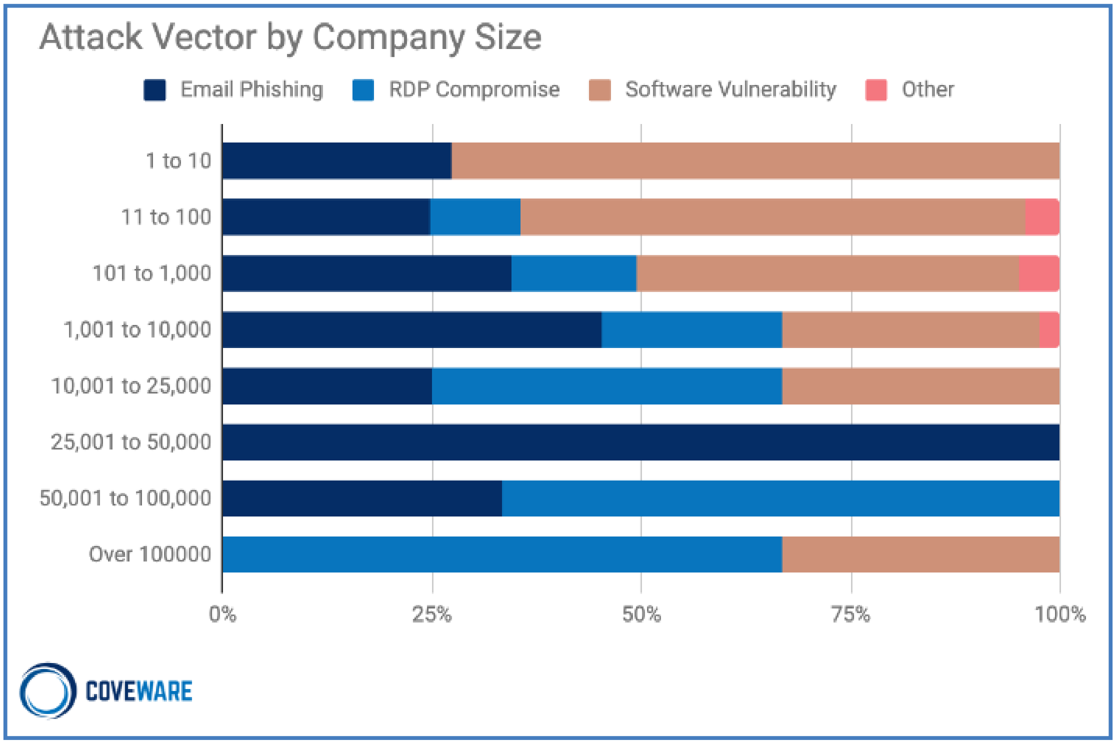

Figure 2: Attack Vector by Company Size Q1 2021