Published on *The National Law Review* https://natlawreview.com

Prometheus Ransomware Targeting Manufacturing Sector

Article By:

Linn F. Freedman

Since the Colonial Pipeline and JBS meat manufacturing security incidents, attention is finally being paid to the cybersecurity vulnerabilities of critical infrastructure in the U.S. and in particular, the potential effect on day to day life and national security if large and significant manufacturers' production are disrupted. In the wake of these recent incidents in the manufacturing sector, Unit 42 of Palo Alto Networks has published research that may be considered a warning to the manufacturing sector and is worth notice. The warning is about the activities of Prometheus, "a new player in the ransomware world that uses similar malware and tactics to ransomware veteran Thanos."

According to the Executive Summary, Unit 42 "has spent the past four months following the activities of Prometheus" which "leverages double-extortion tactics and hosts a leak site, where it names new victims and posts stolen data available for purchase." Prometheus claims to be part of REvil, but Unit 42 says it has "seen no indication that these two ransomware groups are related in any way." Unit 42 further states that Prometheus claims to have victimized 30 organizations in different industries, in more than a dozen countries, including the U.S.

Prometheus came on the scene in February 2021 as a new variant of the strain Thanos. Unit 42 is unable to provide information on how the Prometheus ransomware is being delivered, but surmise that it is through typical means, such as "buying access to certain networks, brute-forcing credentials or spear phishing for initial access." It then first kills backups and security processes and enables the encryption process. It then "drops two ransom notes" that contain the same information about the fact that the network has been hacked and important files encrypted and instructions of how to recover them. If the ransom demand is not met, the data will be published on a shaming site and publishes the "leak status" of each victim. According to Unit 42 "[M]anufacturing was the most impacted industry among the victim organizations we observed, closely followed by the transportation and logistics industry."

What we have seen in the past is that when ransomware groups are successful in one industry, they use the information learned from initial attacks to target other companies in that sector. They leverage the knowledge from one attack to future attacks assuming that since the first one was successful, subsequent attacks will be successful as well. Since industry specific networks are similar, it is seamless to attack one victim, learn from it, then leverage that knowledge to attack similarly situated victims.

With threat attackers' focus on the manufacturing sector right now, we anticipate seeing more attacks against manufacturers from groups such as Prometheus.

National Law Review, Volume XI, Number 160