Thursday, August 26, 2021

According to a report issued on August 24, 2021, by Unit 42 of Palo Alto Networks Ransomware Groups to Watch: Emerging Threats, four emerging ransomware groups “are currently affecting organizations and show signs of having the potential to become more prevalent in the future.”

The four emerging groups identified by Unit 42 include:

AvosLocker, a Ransomware as a Service that arrived on the scene in June 2021 using a blue beetle logo for communications. According to Unit 42, AvosLocker “has low detection rates and is capable of handling large files,” and operates an extortion site with demands between $50,000 and $75,000. It is actively trying to recruit affiliates.

Hive Ransomware also started operating in June 2021 and “is double-extortion ransomware.” Hive “has already shown notable disregard for its victims’ welfare,
attacking organizations including healthcare providers and mid-size organizations ill-equipped for managing a ransomware attack.” Twenty-eight victims have been listed on their leak site.

HelloKitty Linux Edition, a ransomware group that has existed since 2020, usually targets Windows systems, but in July 2021, Unit 42 found that HelloKitty has developed a Linux variant “targeting VBMware’s ESXi hypervisor, which is widely used in cloud and on-premises data centers.”

Lockbit 2.0 (aka ABCD ransomware), another Ransomware as a Service, has launched a marketing campaign to recruit new affiliates and “claims to offer the fastest encryption on the ransomware market,” It has listed 52 victims on its leak site.

Unit 42 confirms what we are seeing: as law enforcement takes the bad guys out of the picture one by one, new threat actors step into the void, and how “old groups can re-emerge and remain persistent threats.”

Copyright © 2021 Robinson & Cole LLP. All rights reserved.

National Law Review, Volume XI, Number 238

Source URL: https://www.natlawreview.com/article/emerging-ransomware-groups-getting-action