WHAT’S HAPPENING?

The Valak Malware is a sophisticated malware previously classified as a malware loader. Though it was first observed in late 2019, the Cybereason Nocturnus team has investigated a series of dramatic changes, an evolution of over 30 different versions in less than six months. This research shows that Valak is more than just a loader for other malware, and can also be used independently as an information stealer to target individuals and enterprises.

KEY OBSERVATIONS & TTPS

› More recent versions of Valak target Microsoft Exchange servers to steal enterprise mailing information and passwords along with the enterprise certificate. This has the potential to access critical enterprise accounts, causing damage to organizations, brand degradation, and ultimately a loss of consumer trust.

› Valak’s basic capabilities are extended with a number of plugin components for reconnaissance and information stealing.

› Valak has evolved from a loader to a sophisticated, multi-stage modular malware that collects plugins from its C2 server to expand its capabilities. The Cybereason Nocturnus team has observed over 30 different versions in about 6 months.

› Read the full length research here.

CYBEREASON CUSTOMERS

We highly recommend every customer enable the following features:

› If you do not have Cybereason NGAV activated, consider doing so to prevent against threats like these.

› For Cybereason MDR customers, the Cybereason team will monitor and triage as well as assist in the mitigation of potential infections.