MegaCortex Ransomware Revamps for Mass Distribution

By Tara Seals

Published: 2019-08-05 · Archived: 2026-04-05 18:43:33 UTC

Manual steps have been replaced by automation.

A dangerous enterprise-focused ransomware, MegaCortex, has been retooled to become a weapon for wide-scale attacks.

Previously used only in manual, post-network-exploitation, targeted campaigns on carefully selected targets, MegaCortex now has a second variant that adds automation to the kill chain. This gives the malware a path to wider distribution, according to researchers at Accenture's iDefense division.

The original version of MegaCortex protected its main payload with a custom password supplied by the adversary for each infection.

"The password requirement…prevented the malware from being widely distributed worldwide and required the attackers to install the ransomware mostly through a sequence of manual steps on each targeted network," explained Leo Fernandes, senior manager of malware analysis and countermeasures at iDefense, in research shared with Threatpost. "The authors of MegaCortex v2 have redesigned the ransomware to self-execute and removed the password requirement for installation; the password is now hard-coded in the binary."

Other upgrades in version 2.0 include anti-analysis features within the main malware module, and the functionality to stop and kill a wide range of security products and services automatically. This was also previously manually executed as batch script files on each host, Fernandes said.

MegaCortex has been used in enterprise attacks across various industries in Europe and North America, according to the researcher. Typically ransom requests have ranged between two and 600 Bitcoins (about $20,000 to $5.8 million). The new version could open the door to a significant expansion of the threat.

"With a hard-coded password and the addition of an anti-analysis component, third parties or affiliated actors could, in theory, distribute the ransomware without the need for an actor-supplied password for the installation," Fernandes said. "Indeed, potentially there could be an increase in the number of MegaCortex incidents if the actors decide to start delivering it through email campaigns or dropped as secondary stage by other malware families."

Ransomware that attacks enterprises continues to be a growth area in the malware landscape, even as variants used in "spray and pray" mass consumer attacks are on the wane.

To protect oneself, a defense-in-depth approach is always a good idea, according to Stuart Reed, vice president of cybersecurity at Nominet.

“Identifying malware and phishing attacks on the network early is critical to mitigating the risk of a ransomware attacks,” Reed said via email. “This needs to be combined with basic cyber-hygiene, such as not opening attachments or clicking links unless you know they are legitimate, keeping up to date with system patches and current versions of malware protection. A layered approach to security, combined with robust backups and a well understood incident response, will be fundamental to combating ransomware attacks.”

Malware analysis will be a focus next week at Black Hat 2019, taking place Aug. 7 and 8 in Las Vegas. Be sure to follow all of our Black Hat and DEF CON 27 coverage right here in Threatpost’s special coverage section.
