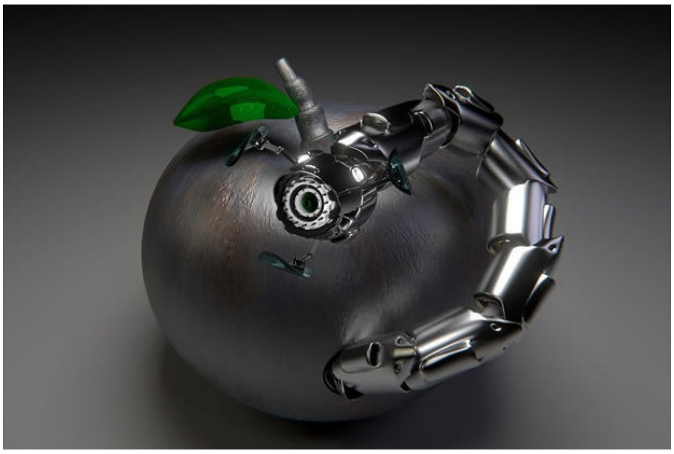
Cisco Warns Against "Cryptoworms"

Written by Marco Attard
15 April 2016

Hackers are taking inspiration from the past in the creation of the ransomware of the future, Cisco Talos warns. And the result is "cryptoworms," ransomware with self-propagation features inspired by worms from the 90s and early 2000s.



"Ransomware as we know it today has a sort of ‘spray and pray’ mentality-- they hit as many individual targets as they can as quickly as possible. Typically, payloads are delivered via exploit kits or mass phishing campaigns," the security division says. "Recently a number of scattered ransomware campaigns deliberately targeting enterprise networks, have come to light. We believe that this is a harbinger of what’s to come-- a portent for the future of ransomware."

One such "portent" is "SamSam," First spotted back in February 2016, SamSam was used in attacks on hospitals in the US. It targets unpatched server vulnerabilities, and is similar to worms in the way it penetrates an OS, spreads malicious code and traverses a network. Thus the "cryptoworm" descriptor.

SamSam is not entirely self-sufficient, but Talos says it can make the core for nastier, more autonomous ransomware able to target unprotected executable files, search networks for attached storage to copy itself to and use minimal resources to escape detection. SamSam attacks through the JBoss application platform, but Talos says that can change with future iterations.

In addition to enhanced attack capabilities, cryptoworms might also bring about higher ransom prices. Currently ransomware authors demand anything from 0.5 ($220) to 1 ($420) Bitcoins per infected machine.

But how can one defend against cryptoworms? Talos has a number of suggestions. First off, one should prevent initial access through port scans, vulnerability remediation and regular system maintenance. Company perimeter and public-facing network security should also be boosted, while regular backups remain of vital importance. In fact, Talos decribes reliable backups as nothing less than the Achilles Heel of the cryptoworm.

“For too long, critical security controls and best practice for enterprise network security has been publicly praised and privately ignored,” Talos insists. “If enterprises don’t start making strides towards defensible architecture today, massive ransoms may end up getting paid tomorrow."

Go Ransomware: Past, Present and Future