Erpresser-Malware Cryptowall in neuer Auflage

Microsoft warnt vor einer neuen Version der Erpresser-Malware Cryptowall. Neben E-Mail verbreitet sich der Schädling auch über manipulierte Online-Anzeigen.

Der Schädling unterschiedet jetzt zwischen 32- und 64-Bit-Architekturen. Um die Verbindungen zu den Comand and Control-Servern zu verschleiern, setzt der Schädling gleich zwei Darüber Anonymisierungsnetzwerke ein.

Cryptowall 3.0 verschlüsselt Dateien eines Nutzers. Die Schadsoftware zeigt dann eine Website an, die das Opfer auffordert, innerhalb von sieben Tagen 500 Dollar in Bitcoins zu zahlen. Dann würden die Daten wieder frei gegeben. Nach Ablauf der Frist erhöhe sich das Lösegeld auf 1000 Dollar.

Microsoft ist nach eigenen Angaben durch einen Anstieg neuer Cryptowall-Infektionen auf die Variante 3.0 aufmerksam geworden. Allein am 12. Januar registrierte der Softwarekonzern 288 Computer, die mit der Malware infiziert wurden.

Wie der Sicherheitsexperte Pierluigi Paganini in seinem Blog schreibt, hat neben Microsoft auch der französische Forscher Kafeine die neue Cryptowall-Variante analysiert. Ihm zufolge verschlüsselt sie ihre Kommunikation mit den Befehlsservern per RC4. Außerdem unterstützt sie neben Tor noch ein weiteres Anonymisierungsnetzwerk namens I2P. Die Hintermänner der Malware verbänden offenbar beide Netzwerke für die Entschlüsselung von Dateien.

Paganini weist außerdem darauf hin, dass auch der Nachfolger des Schwarzmarkts Silk Road, Silk Road Reloaded, zu I2P migriert ist. Er vermutet, dass die Cyberkriminellen es für sicherer halten als Tor.

Ransomware ist nicht nur eine Bedrohung für traditionelle PCs. Schon im Juni vergangenen Jahres hatte der slowakische Sicherheitsanbieter Eset die nach seinen Angaben erste Verschlüsselungsmalware für Android entdeckt. Zu dem Zeitpunkt war die mobile Schadsoftware allerdings nur in der Ukraine im Umlauf. Für die Freischaltung verschlüsselter Dateien verlangte sie zudem ein recht moderates Lösegeld von umgerechnet 16 Euro.

Im August war zudem eine spezialisierte Ransomware namens Synolocker aufgetaucht, mit deren Hilfe Cyberkriminelle Daten auf NAS-Systemen des taiwanischen Anbieters Synology verschlüsselten. Sie verlangten 270 Euro Lösegeld, das sich nach Ablauf von sieben Tagen ebenfalls verdoppelte. Die Schadsoftware gelangte über eine schon im Dezember 2013 geschlossene Sicherheitslücke auf ungepatchte Geräte.

[mit Material von Stefan Beiersmann, ZDNet.de]

Tipp: Wie sicher sind Sie bei der Sicherheit? Überprüfen Sie Ihr Wissen – mit 15 Fragen auf silicon.de