

Try2Cry Ransomware verbreitet sich über USB-Sticks

G DATA Virusanalysten entdecken neues Schadprogramm mit Wurm-Komponente

Bochum (Deutschland), 6. Juli 2020

Die G DATA Security-Experten haben eine neue Ransomware entdeckt. Try2Cry verbreitet sich selbstständig über USB-Sticks und ist auf eine massenhafte Verbreitung aus. Ist ein Computer einmal infiziert, kopiert sich Try2Cry unbemerkt auf angeschlossene USB-Sticks und kann sich so weiterverbreiten. G DATA Kunden sind vor Try2Cry bestens geschützt.

Virusanalysten von G DATA CyberDefense haben eine Version der Try2Cry Ransomware entdeckt, die ähnlich wie die im Jahr 2017 entdeckte Ransomware Spora agiert. Try2Cry enthält eine Wurm-Komponente, durch die eine selbstständige Verbreitung erfolgt, sobald ein USB-Stick als Laufwerk erkannt wird. Das Schadprogramm legt dann im Stammordner des Geräts eine Kopie von sich selbst mit dem Namen Update.exe ab. Daraufhin werden alle Dateien auf dem Rechner verschlüsselt, für jede Datei wird zudem eine Verknüpfung erstellt, sodass die Originaldateien nicht mehr zugänglich sind. Öffnet der User die Verknüpfung, die das identische Symbol wie die Originaldatei trägt, erscheint die Lösegeldforderung.

„Für Ransomware ist der Übertragungsweg über USB-Sticks heutzutage eher ungewöhnlich“, sagt Tim Berghoff, Security Evangelist, G DATA CyberDefense. „Diese Art Schadsoftware wird eher über E-Mails oder manipulierte Webseiten verbreitet, weil sich damit mehr Nutzer erreichen lassen.“

Try2Cry gehört zu der Ransomware-Familie „Stupid“, die als Open-Source-Lösegeld-Software auf Github verfügbar ist. Im Gegensatz zu Spora gibt es Anzeichen für die Infektion des USB-Laufwerks, da sich in der Ecke der Verknüpfungssymbole ein Pfeil befindet und die Ordner mit arabischen Dateinamen beschriftet sind. Für die Verschlüsselung wird der Rijndael-Algorithmus genutzt – mit einem statischen und hartcodierten Passwort.

An den PC angeschlossene USB-Sticks werden von den G DATA Lösungen automatisch auf einen Schadsoftware-Befall überprüft. G DATA Kunden sind vor Try2Cry bestens geschützt.

Die Verbreitung von Malware über Speichermedien wie USB-Sticks erinnert an die 90er-Jahre, wo viele Viren über Disketten in Umlauf gerieten. Heute werden meist entweder infizierte Phishing-Mails mit Attachments oder manipulierten Links versendet oder Malware direkt über offene Schwachstellen auf einem Computer eingespielt.

Weitere technische Details und Grafiken finden Sie auf unserem englischsprachigen Techblog in dem Artikel [Try2Cry: Ransomware tries to worm](#).

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299