Ordinypt hat es auf Benutzer aus Deutschland abgesehen

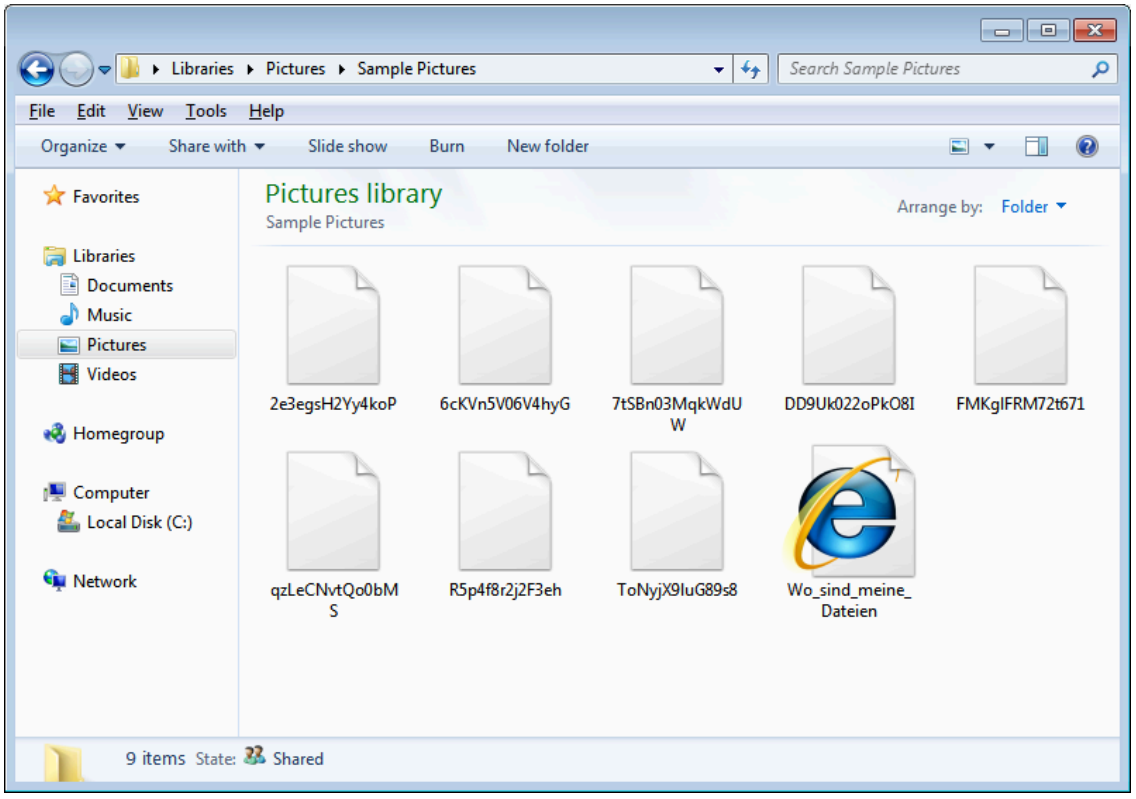
By Tim Berghoff, Karsten Hahn

Published: 2024-11-14 · Archived: 2026-04-05 19:04:39 UTC

07.11.2017

Lesezeit: 3 min (679 Wörter)

Die Ransomware "Ordinypt" (auch bekannt unter dem wenig handlichen Namen „HSDFSDCrypt“) befällt derzeit hautpsächlich Benutzer aus Deutschland. Unter der Haube hat sie einige Merkmale, die herausstechen. G DATA-Analyst Karsten Hahn hat einen genaueren Blick auf die Ransomware geworfen.



Durch Ordinypt verschlüsselte Dateien

Auffällig ist zunächst einmal, dass Ordinypt in einer für Ransomware unüblichen Programmiersprache verfasst ist (Delphi). Die Daten werden wie bei jeder Ransomware verschlüsselt, die Dateinamen scheinbar zufällig gewählt. In den Dateien selbst werden die verschlüsselten Daten noch einmal kodiert (in base64); warum das so ist und welchen Zweck die Macher damit verfolgen, ist zum gegenwärtigen Zeitpunkt noch unklar.

Auch sonst erscheint Ordinypt auffällig unauffällig – es gibt keine Anzeichen für einen beabsichtigten Wiedererkennungswert. Der Schädling setzt stattdessen auf Effizienz.

Besonders erwähnenswert ist die Erpressernachricht – sie ist in 100% fehlerfreiem Deutsch verfasst. Man kann davon ausgehen, dass der Verfasser des Textes ein Muttersprachler ist. Auffällig ist auch, dass in der Erpressernachricht ein Stück Programmcode versteckt ist, der jedes mal eine neue Bitcoin-Adresse generiert, an die eine Lösegeldzahlung gesendet werden soll. Bisher konnten wir dieses Verhalten noch bei keiner anderen Ransomware entdecken. Zweck dieser Vorgehensweise ist möglicherweise, die Verfolgung von Zahlungsströmen durch Strafverfolgungsbehörden zu erschweren. Anhand einer der E-Mails, in denen die Schadsoftware versteckt war, könnten Personalabteilungen ein erklärtes Ziel sein, wie seinerzeit bei Petya.

Genau wie viele andere Schadprogramme wird auch Ordinypt als PDF-Datei getarnt per E-Mail-Anhang verteilt.

G DATA - Kunden sind geschützt

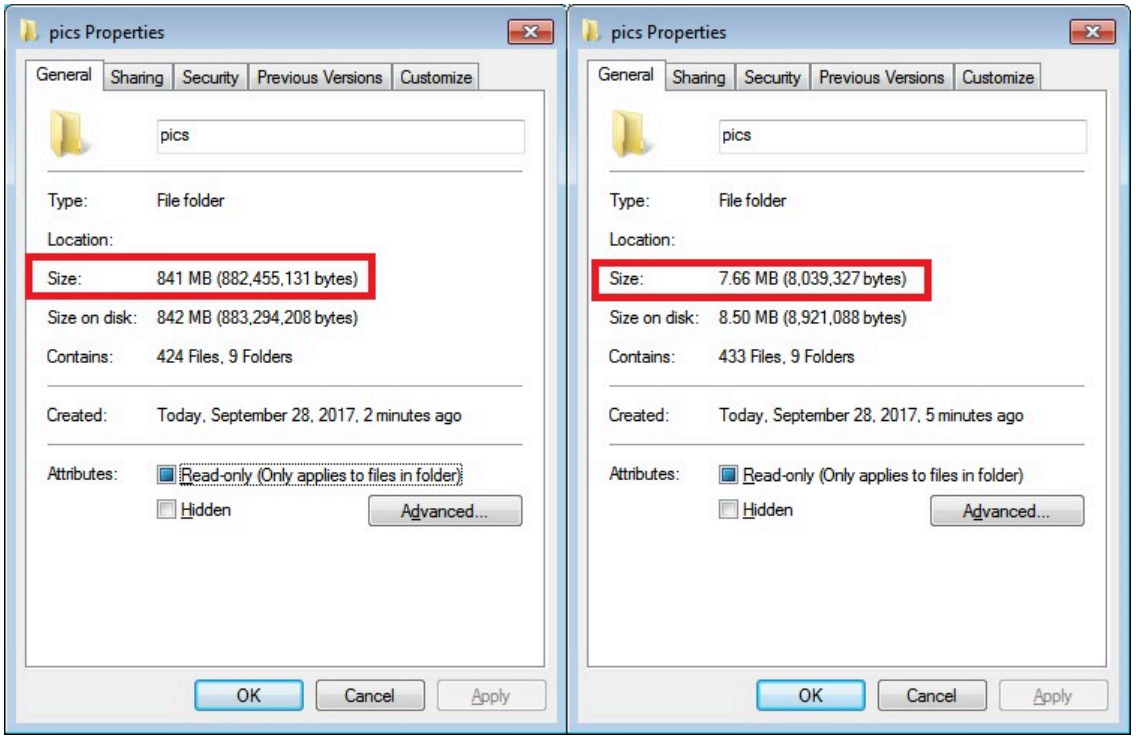
Die Schadsoftware wird unter dem Namen **Win32.Trojan-Ransom.Ordinypt.A** erkannt.
Der Anhang, in dem HSDFSDCrypt verschickt wird, hat die Signatur **Archive.Malware.FakeExt.N@susp.**

Details für Forscherkollegen

E-Mail: b7cb3160025a0bbdcd453a9be490a9e7b1d9505b4f290355e82a6965d0c9e5e4
E-Mail-Attachment (zip): d4e66191e4e8fc22986efc4a84247f3810e969b89a7c331550960e32c278cad3
Sample EXE: 085256b114079911b64f5826165f85a28a2a4ddc2ce0d935fa8545651ce5ab09

Update (8. November, 14:30) - Der Schein kann trügen

Nach weiteren Analysen steht nun fest, dass Ordinypt mehr ist als nur eine weitere Ransomware. Dateien, die augenscheinlich verschlüsselt wurden, sind nach Abschluss des Prozesses quasi "leer". Damit hat Ordinypt sich als eine Kombination aus Ransomware und einem "Wiper" (engl. wipe: auslöschen) entpuppt. Ein Testordner, der mit Bildern im JPG-Format gefüllt war, hat nach der "Verschlüsselung" plötzlich nur noch einen Bruchteil der ursprünglichen Größe.
Wer also das Lösegeld gezahlt hat, in der Hoffnung, seine Daten wiederzubekommen, wird feststellen, dass die Daten tatsächlich unwiederbringlich verloren sind.



Links der Ordner mit den Originaldateien, rechts der Ordner mit den "verschlüsselten" Dateien

---

Folgende Artikel könnten Sie auch interessieren:

Artikel teilen
