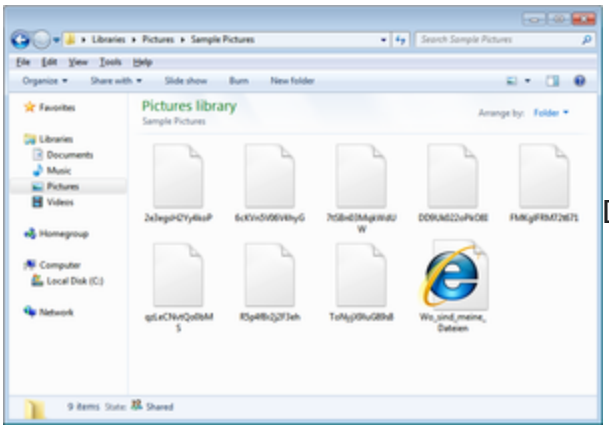
Ordinypt hat es auf Benutzer aus Deutschland abgesehen

gdata.de/blog/2017/11/30151-ordinypt

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.

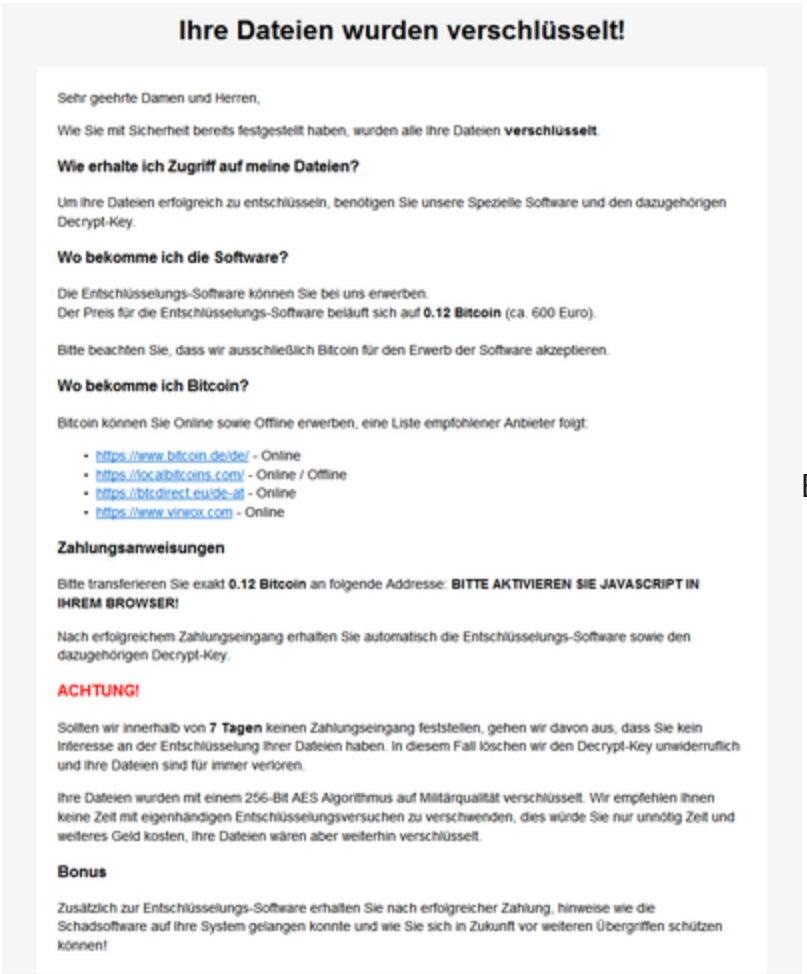
Auch sonst erscheint Ordinypt auffällig unauffällig – es gibt keine Anzeichen für einen beabsichtigten Wiedererkennungswert. Der Schädling setzt stattdessen auf Effizienz.

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.**



Ihre Dateien wurden verschlüsselt!

Sehr geehrte Damen und Herren,

Wie Sie mit Sicherheit bereits festgestellt haben, wurden alle Ihre Dateien **verschlüsselt**.

Wie erhalte ich Zugriff auf meine Dateien?

Um Ihre Dateien erfolgreich zu entschlüsseln, benötigen Sie unsere Spezielle Software und den dazugehörigen Decrypt-Key.

Wo bekomme ich die Software?

Die Entschlüsselungs-Software können Sie bei uns erwerben.
Der Preis für die Entschlüsselungs-Software beläuft sich auf **0.12 Bitcoin** (ca. 600 Euro).

Bitte beachten Sie, dass wir ausschließlich Bitcoin für den Erwerb der Software akzeptieren.

Wo bekomme ich Bitcoin?

Bitcoin können Sie Online sowie Offline erwerben, eine Liste empfohlener Anbieter folgt:

- https://www.bitcoin.de/de/ - Online
- https://localbitcoins.com/ - Online / Offline
- https://btcdirect.eu/de-at - Online
- https://www.vinexx.com - Online

Zahlungsanweisungen

Bitte transferieren Sie exakt **0.12 Bitcoin** an folgende Addresse: **BITTE AKTIVIEREN SIE JAVASCRIPT IN IHREM BROWSER!**

Nach erfolgreichem Zahlungseingang erhalten Sie automatisch die Entschlüsselungs-Software sowie den dazugehörigen Decrypt-Key.

ACHTUNG!

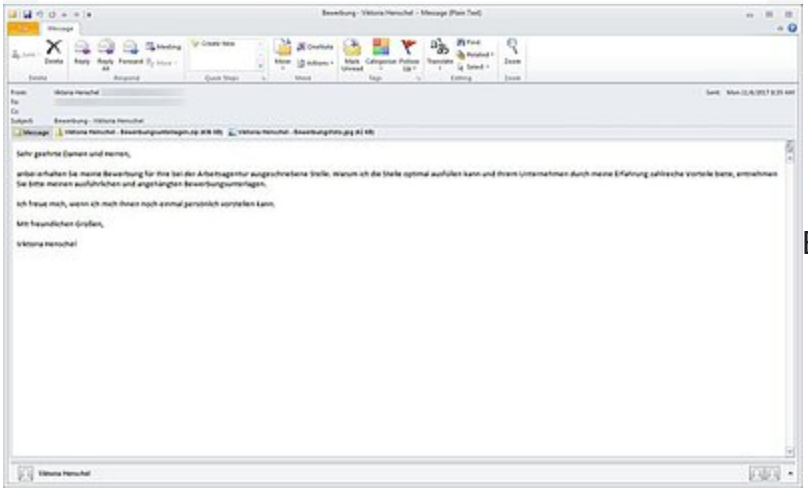
Sollten wir innerhalb von **7 Tagen** keinen Zahlungseingang feststellen, gehen wir davon aus, dass Sie kein Interesse an der Entschlüsselung Ihrer Dateien haben. In diesem Fall löschen wir den Decrypt-Key unwiderruflich und Ihre Dateien sind für immer verloren.

Ihre Dateien wurden mit einem 256-Bit AES Algorithmus auf Militärqualität verschlüsselt. Wir empfehlen Ihnen keine Zeit mit eigenhändigen Entschlüsselungsversuchen zu verschwenden, dies würde Sie nur unnötig Zeit und weiteres Geld kosten, Ihre Dateien wären aber weiterhin verschlüsselt.

Bonus

Zusätzlich zur Entschlüsselungs-Software erhalten Sie nach erfolgreicher Zahlung, hinweise wie die Schadsoftware auf Ihre System gelangen konnte und wie Sie sich in Zukunft vor weiteren Übergriffen schützen können!

Erpressernachricht von Ordinypt



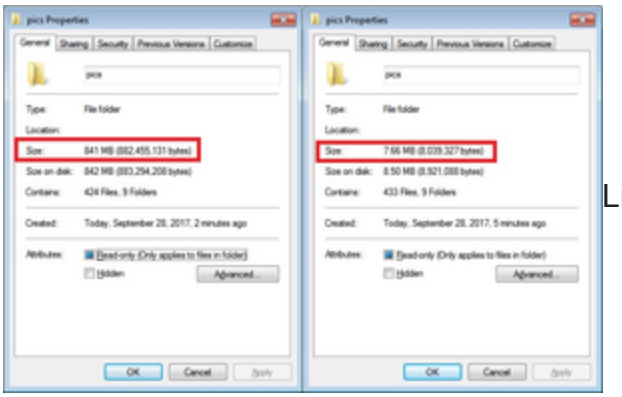
Eine E-Mail, in der Ordinypt versteckt ist

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

- Warning
- Malware
- CyberCrime

Die besten Beiträge per Mail

Alle wichtigen IT-Security-News bequem per E-Mail

Sparen Sie sich jede Menge Zeit – wir behalten für Sie den Überblick über die IT-Sicherheitslage.

Die mit * markierten Felder sind Pflichtfelder.

Vielen Dank für Ihr Interesse.

Sie erhalten in Kürze eine E-Mail. Bitte klicken Sie darin auf den Link, um Ihre **Daten zu bestätigen**.

Sollten Sie in Ihrem Posteingang keine E-Mail von uns vorfinden, kontrollieren Sie bitte auch Ihren Spamordner.

zurück zum Formular