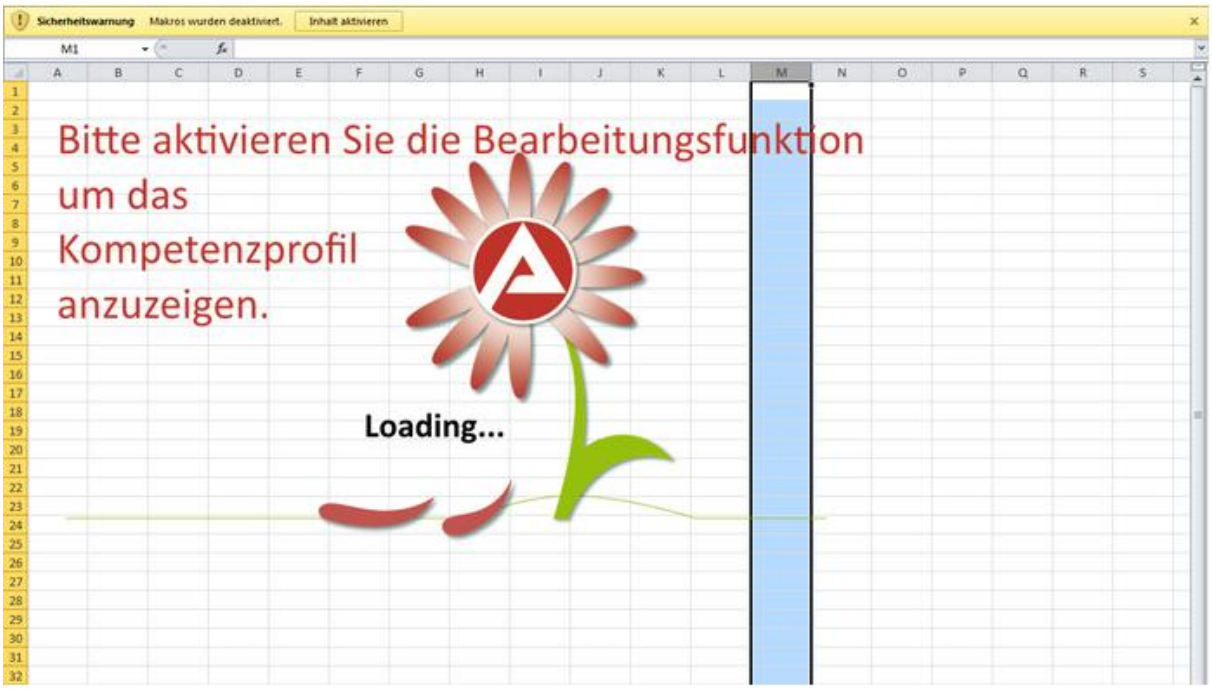
Schützen Sie sich jetzt vor einem neuen Verschlüsselungstrojaner in E-Mail-Bewerbungen

Unsere Step-by-Step Anleitung informiert Sie über alles, was Sie wissen müssen: Erkennung, Behandlung und Prävention.

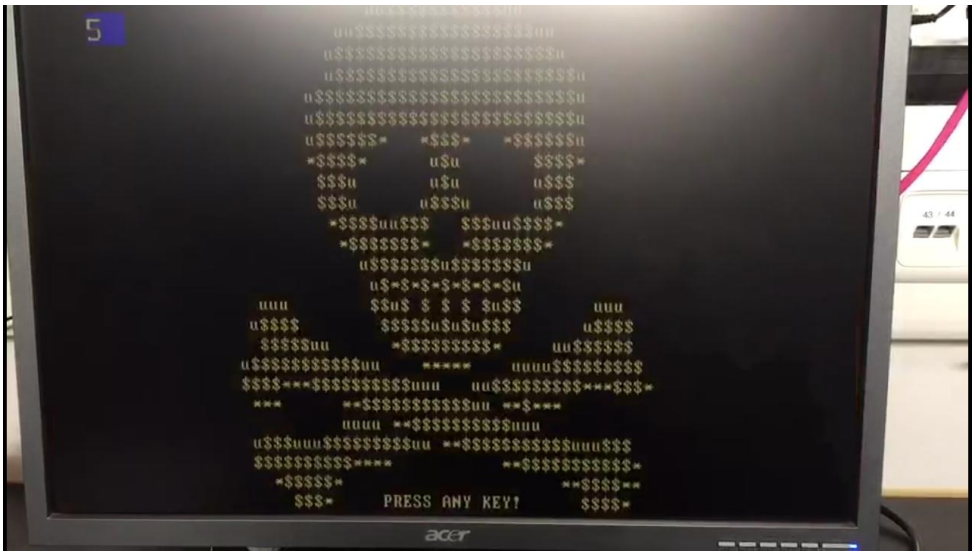
Seit Anfang Dezember 2016 ist ein neuer, sehr schwer identifizierbarer Verschlüsselungstrojaner im Internet unterwegs und treibt sein Unwesen, indem er ganze Computersysteme verschlüsselt.

Ziel des Trojaners sind hauptsächlich Personalabteilungen von Unternehmen. Bei ihnen geht der Trojaner - getarnt als Bewerbung per E-Mail – vorzugsweise ein. Natürlich können auch andere Unternehmensbereiche betroffen sein. Da die E-Mails in fehlerfreiem Deutsch formuliert sind und von den meisten Virenscannern noch nicht als Gefahr eingestuft werden, ist es sehr schwer die E-Mails als „gefährlich“ zu identifizieren und richtig zu reagieren. Deswegen ist in diesem Fall die schnellstmögliche Information und Sensibilisierung aller Mitarbeiter sehr wichtig.

So sieht der E-Mail-Anhang aus, nachdem er geöffnet wurde:

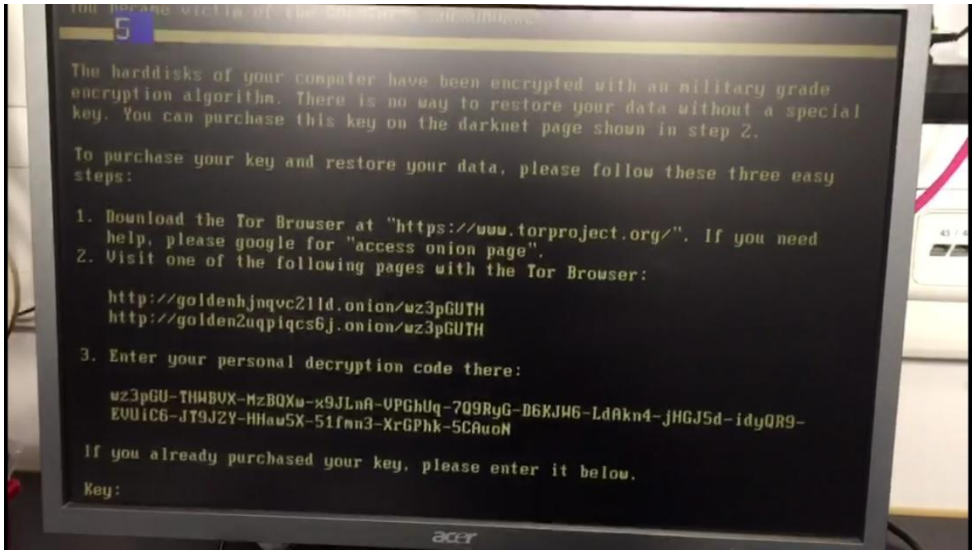


Öffnet ein User die angehängte Excel-Datei ist das zunächst noch nicht schlimm. Sobald aber die Bearbeitungsfunktion in der Excel-Datei aktiviert wird, beginnt der Trojaner mit der Verschlüsselung der Daten auf dem Rechner. Dies geschieht in Sekunden. Der Rechner wird neu gestartet und es erscheint folgendes Bild:



Drückt man nun wie aufgefordert eine Taste, wird man zum nächsten Bild (siehe unten) weitergeleitet und informiert, dass das System verschlüsselt wurde.

Ohne den richtigen Schlüssel ist eine Entschlüsselung des Systems in der Regel nicht mehr möglich. Den richtigen Schlüssel kann man nun käuflich erwerben, in dem man die angebotene Anleitung befolgt.



Die für den Trojaner anfälligsten Betriebssysteme sind **Windows 7**, **Windows 10** und **Windows Server 2008**. In den meisten Fällen werden nur lokale Daten verschlüsselt aber es wurden auch Fälle bekannt in denen sowohl lokale Daten als auch Daten von eingebundenen Netzlaufwerken verschlüsselt wurden.

Was können Sie und Ihre Mitarbeiter tun, um sich zu schützen?

Präventionsmaßnahmen:

1. Öffnen Sie keine E-Mail Anhänge die mit „.exe“, „.xls“ oder „.xlsx“ enden, wenn Sie den Absender nicht kennen.
2. Haben Sie bereits eine angehängte Excel-Datei geöffnet, aktivieren Sie niemals die Bearbeitungsfunktion.
3. Wenn Sie den Absender nicht kennen, antworten Sie zunächst auf die E-Mail und erkundigen sich, ob die E-Mail tatsächlich von diesem Absender gesendet wurde. Wenn es sich um eine bösartige E-Mail handelt, werden Sie in der Regel keine Antwort erhalten.
4. Sollten in der E-Mail Kontaktdaten angegeben sein, setzten Sie sich zunächst telefonisch mit dem Absender in Verbindung und klären ab, ob es sich tatsächlich um eine Anfrage, Bewerbung etc. handelt.
5. **Wenn Sie eine möglicherweise gefährliche Datei bereits geöffnet haben und Ihnen etwas merkwürdig vorkommt, ziehen Sie so schnell wie möglich den Netzstecker und das LAN Kabel Ihres Geräts.**

Wenn Sie Fragen haben oder doch zum Opfer geworden sind kontaktieren Sie uns. Wir können Ihre Geräte auf Schad-Software prüfen und unterstützen Sie auch mit Back-up- und IT-Sicherheitskonzepten.

Ihr MK-Technik Team

MK-Technik Informationstechnologie
Tel.: +49 821 / 450 403-0
E-Mail: info@mk-technik.de
www.mk-technik.de