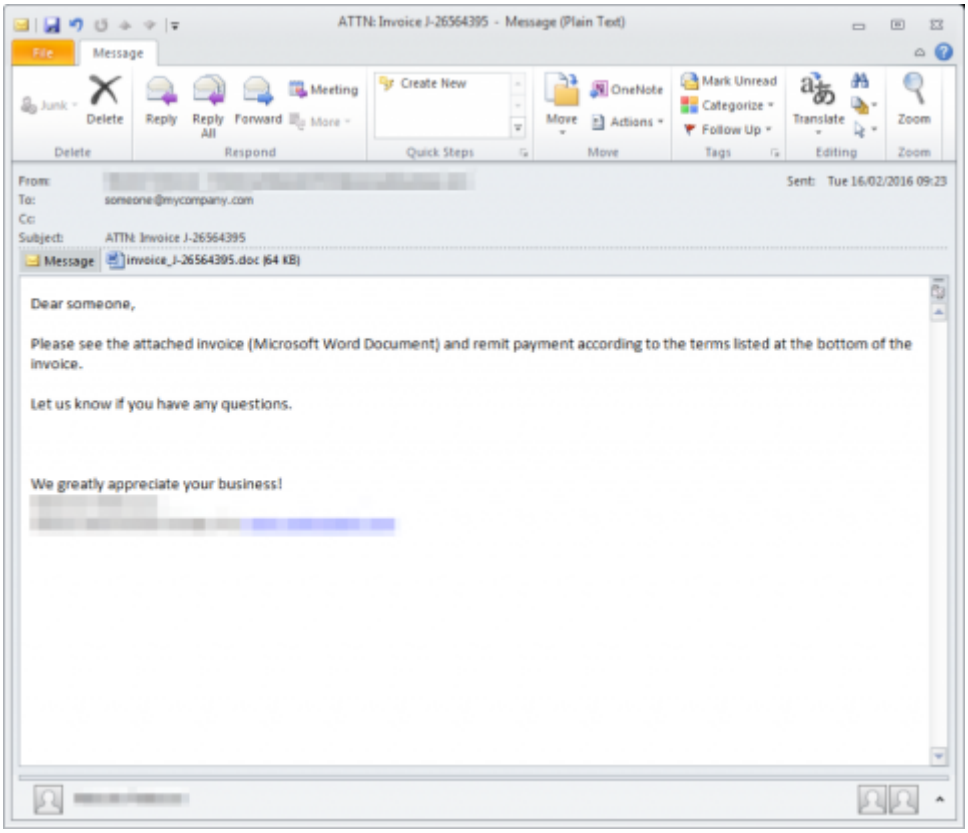
News von Proofpoint

Locky tauchte bereits Mitte Februar in Mails auf

Proofpoint entdeckte Erpressungstrojaner Locky als erster in Word-Anhängen – Demo-Video: So arbeitet Locky

Am 16. Februar sind die Forscher des IT-Security-Experten Proofpoint zum ersten Mal auf einen Anhang gestoßen, in dem sich die Ransomware Locky verbarg. Das Botnet, das den Spam verschickt, ist dasselbe, das den Banking-Trojaner Dridex in Umlauf brachte.



E-Mail-Köder, verknüpft mit Locky

Forscher von Proofpoint haben den Erpressungstrojaner „Locky“ bereits am 16. Februar entdeckt, der durch seine Anhänge Rechner verseucht und Nutzer erpresst, wie sie im Corporate Blog beschreiben. Eine Nachricht mit dem Betreff „ATTN: Invoice J-12345678" enthielt den Anhang "invoice_J-12345678.doc“ enthielt ein MS Word-Dokument mit einem Makro, das den Erpressungstrojaner Locky herunterlädt und installiert. Öffnet der Benutzer das Dokument, wird sein Rechner infiziert, wenn in Word standardmäßig Makros freigeschaltet sind.

Eskenzi PR Germany
fon + 49.241.43 53 74 84
Sabine Faltmann
faltmann@eskenzipr.com

News von Proofpoint

Locky verschlüsselt die Dateien auf dem Rechner und im Netz und nutzt Notepad, um als Desktop-Hintergrund eine Erpressungsnachricht anzuzeigen. Diese verlangt vom Benutzer, Bitcoins zu kaufen, damit er seine Daten wieder entschlüsseln kann. Zurzeit ist kein Fall bekannt, in dem nach Zahlung tatsächlich der Schlüssel geliefert wurde.

Spam

Locky wird über Spam mit angehängten Dokumenten in Umlauf gebracht, was bei den Malware-Kampagnen des letzten Jahres die gängigste Methode war. Das Botnet (eine Gruppe infizierter Rechner, auf denen ein Spambot läuft), das den Spam verschickt, ist dasselbe, das den Großteil der Nachrichten verschickt, die den Banking-Trojaner Dridex im Schlepp haben.

Hier geht es zum **Blogbeitrag** von Proofpoint mit den detaillierten Ergebnissen: **http://www.proofpoint.com/de/dridex-akteure-reihen-ransomware-spiel-mit-locky**

Demo-Video: So arbeitet Locky

http://resources.proofpoint.com/h/i/212068800-proofpoint-locky-demo

Kurzlink: http://bit.ly/218cYIP

253 Worte, 1726 Zeichen

Proofpoint Germany

Landsberger Straße 302
80687 München

www.proofpoint.com

KONTAKT
Monika Schaufler, Regional Director DACH

mschaufler@proofpoint.com