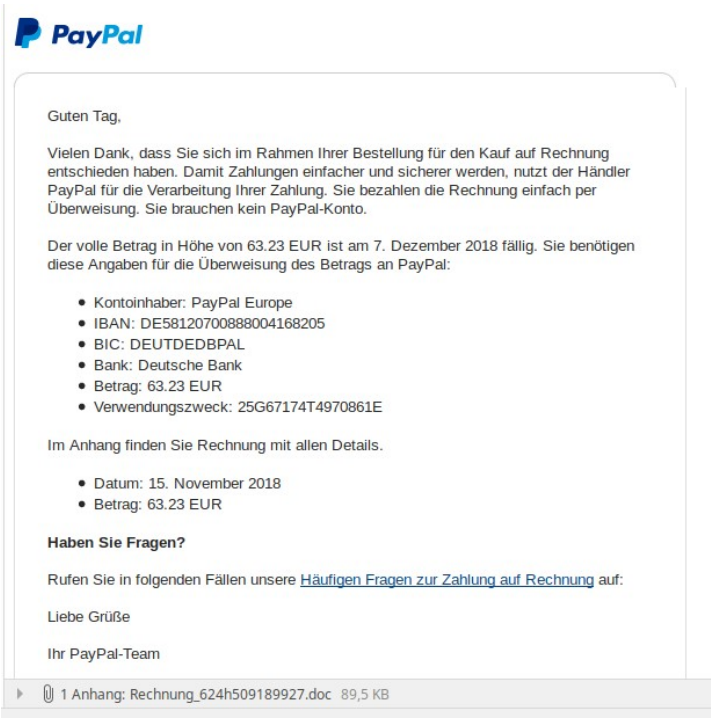
**Schadsoftware "Emotet" verbreitet sich weiter und zwar massiv!**
**05.12.2018**


Bereits im November haben wir darauf hingewiesen, dass sich die Malware "Emotet" massiv über E-Mailanhänge verbreitet. Da Emotet Adressbücher und die E-Mailkommunikationspartner ausliest, bekommt der Empfänger eine E-Mail von einem vermeintlich bekannten Absender und öffnet unter Umständen den verseuchten Anhang. Die Texte der Mail variieren, sind teilweise in deutscher Sprache gehalten und sollen den Empfänger zum Öffnen des Anhangs bewegen. Falls einmal aktiviert, hat Emotet darüber hinaus die Eigenschaft, sich über die Windows-Lücke **Eternal Blue** von System zu System zu verbreiten- falls es nicht gegen diesen Angriff gepatched worden ist.

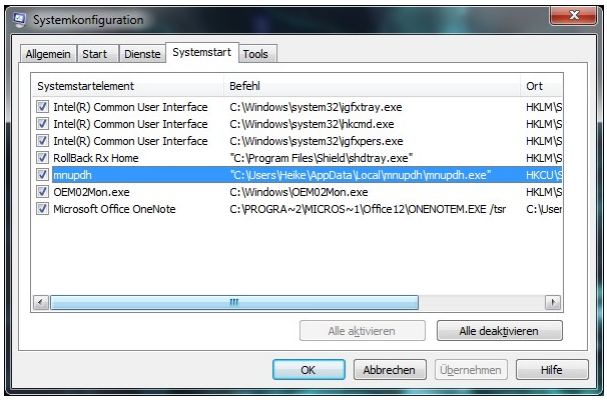
Aktuell (seit ca. 04.12.2018 gegen Mittag) ist jetzt eine **neue Variante** unterwegs:




E-Mails geben vor, von **Paypal** zu sein und enthalten ebenfalls den schadhaften Anhang in Form eines Makro-verseuchten Anhangs!

**Hinweise zur Detektion von Emotet:**
Nach dem Öffnen des Office-Dokumentes und dem Aktivieren von Makros wird durch die eingebetteten Skripte eine ausführbare Datei runtergeladen. Diese legt sich zunächst in einem temporären Pfad z.B. unter:
*"C:/Users/[Benutzername]/AppData/Local/Microsoft/Windows/[zufälliger_Name].exe"*
*"C:/Users/[Benutzername]/AppData/Local/[zufälliger_Pfad]/[zufälliger_Name].exe"*
*"C:/Users/[Benutzername]/AppData/Roaming/Temp/[zufälliger_Name].exe"*
ab.

Danach wird ein Autostart-Eintrag generiert, der beispielsweise mit **msconfig** oder dem Tool Autoruns zu detektieren ist:




Nach einem mehrstündigen Betrieb von Emotet sind meistens auch noch andere Module nachgeladen worden, die beim Systemstart ausgeführt werden! Diese liegen dann bereits in den Windows-Systemverzeichnissen- das System ist dann massiv verseucht.

Bei Emotet erfolgt in regelmäßigen Abständen eine Kommunikation mit mehreren C&C-Servern. Diese lässt sich aus einem Netzwerk-Mitschnitt anhand der Verwendung des Cookie-Feldes relativ gut erkennen. Die Kommunikation erfolgt auf verschiedenen **Ports > 80** (bspw. 6090 8080) und zwar unverschlüsselt. Damit lässt sich z.B. in **Wireshark** der Filter *"http.cookie"* anwenden, um so diese Pakete sichtbar zu machen und eine Infektion im Netzwerk zu erkennen.

**Weitere Informationen finden Sie hier:**

Pressemeldung des BSI zu Emotet
Link zur Heise-Meldung vom 05.12.2018
Link zur Heise-Meldung vom 12.11.2018
Programm Autoruns
Programm Wireshark
Virenprüfung Online bei VirusTotal

top

**Permanenter Link zu diesem Artikel auf zac-niedersachsen.de:**
**https://zac-niedersachsen.de/artikel/21**
**Klicken Sie hier und abonnieren Sie unseren Newsletter.**