RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

SCHADSOFTWARE EMOTET

Risiken und Empfehlungen

19.11.2020
1. Kongress Digitale Sicherheit

Dr. Oliver Gabel

CISO-GESCHÄFTSSTELLE

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Informationssicherheit

Ressortübergreifendes ISMS auf Basis BSI-Standards mit agilen Methoden

Fachliche Steuerung und Kontrolle des CERT-rlp

AG Informationssicherheit

…

Cyber-Sicherheit

Vernetzt mit rheinland-pfälzischen Sicherheits-behörden, BSI

Kongress Digitale Sicherheit

LAG Cyber-Sicherheit

…

WAS IST EMOTET?

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

(Synonyme: Feodo, Bugat, Geodo, Heodo)

- Banking-Trojaner (2010)
- Schadprogramm mit Modulen
  - Ausspähen von Informationen,
  - Spam/Mail-Versand,
  - „Outlook-Harvesting“,
  - Kommunikation mit C2-Server,
  - **Nachladen von anderen Schadprogrammen wie Trickbot, Ryuk**
  - …

EINSCHÄTZUNG DES BSI

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

„Emotet: Neue Qualität fortschrittlicher Angriffe“

„[…] die Schadsoftware Emotet als eine der größten Cyber-Bedrohungen der Welt bezeichnet und vor einer professionellen Weiterentwicklung gewarnt.“

EIN LANGWIERIGER FALL

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

heise online › News › 07/2020 › **Emotet: Arbeit am Kammergericht nach Monaten weiter…**

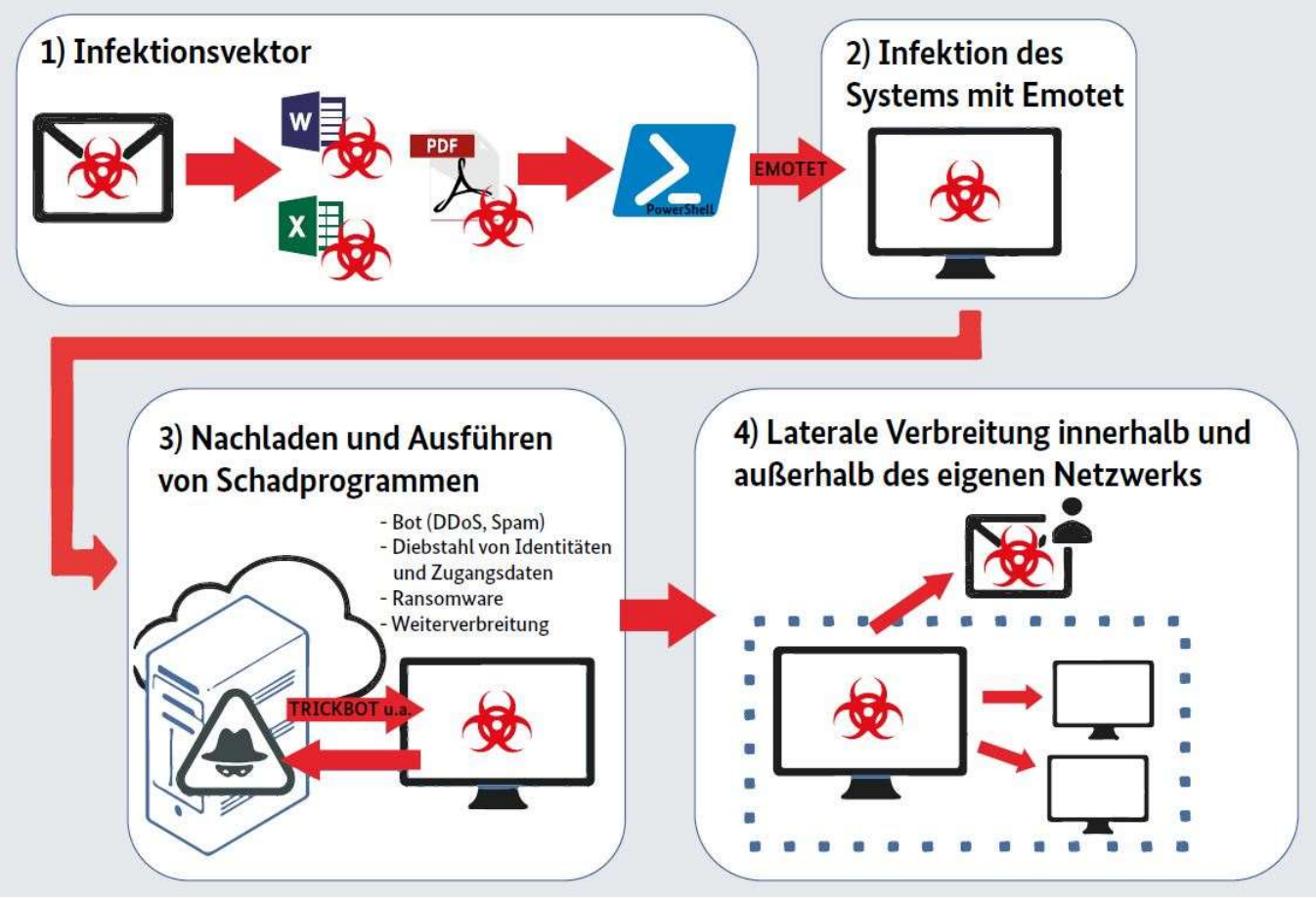
Emotet: Arbeit am Kammergericht nach Monaten weiter eingeschränkt

Ein Dreivierteljahr nach dem Trojaner-Angriff auf die Justizinstitution kann ein Großteil der Richter neue Laptops nur als Schreibmaschinen verwenden.

Lesezeit: **2 Min.** In Pocket speichern 65

TYPISCHER ABLAUF

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT



BSI: „Die Lage der IT-Sicherheit in Deutschland“, 2019

TYPISCHE VEKTOREN

E-Mail mit Anhang oder Link

- Word-Dokument mit Makro
- (doppelt) gezippt

Web-Mailer

Zugangsdaten auf privatem PC/Laptop

EMPFEHLUNGEN

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Emotet-Infektion! Was tun?

- Rechner vom Netzwerk ***SOFORT*** trennen
- IT und Informationssicherheitsbeauftragten verständigen
- Rechner neu installieren
- ***Alle*** Passwörter ändern
- Ggfs. Behörden informieren

EMPFEHLUNGEN

RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Prävention

- Software aktuell halten
- Niemals mit privilegierten Rechten dauerhaft am Rechner arbeiten
- Offline-Backups durchführen

www.allianz-fuer-cybersicherheit.de
„Maßnahmen zum Schutz vor Emotet“

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Oliver Gabel

Informationssicherheitsbeauftragter der Landesverwaltung

IT-Zentralstelle, Breitband

[redacted]