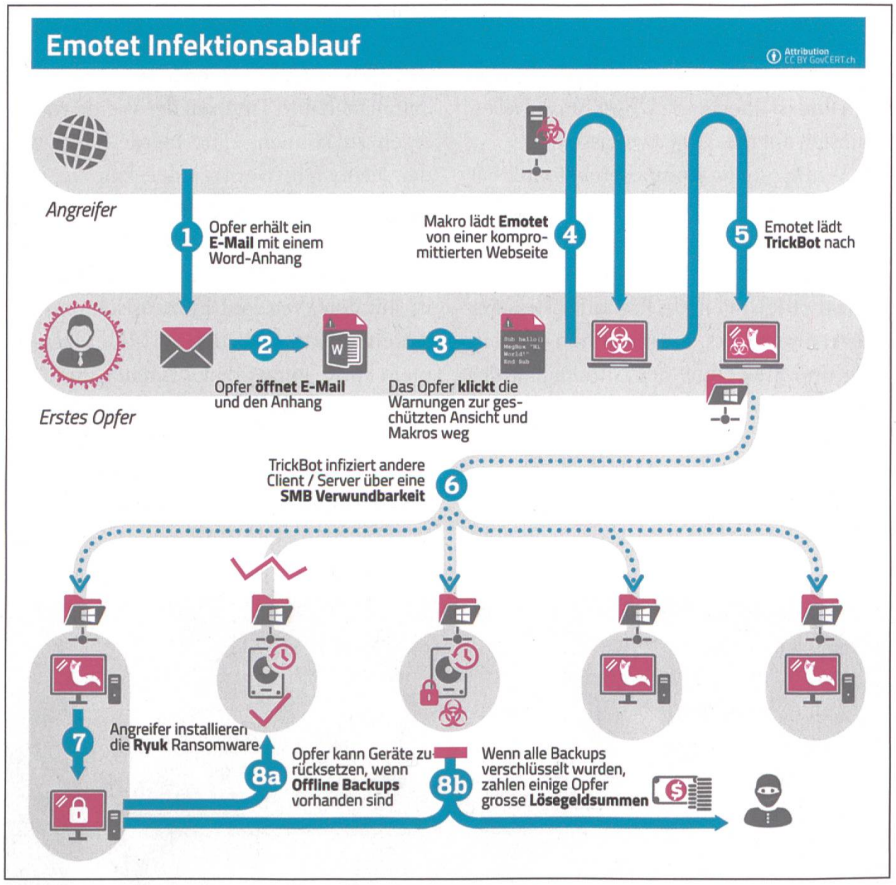
Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 94 (2019)
Heft: 2

Artikel: Cyberwar : Behörde warnt vor Trojaner
Autor: [s.n.]
DOI: https://doi.org/10.5169/seals-868353

Cyberwar: Behörde warnt vor Trojaner

MELANI, die Meldestelle des Bundes, beobachtet Malspam-Wellen mit infiziertem Word-Dokumenten. Dabei handelt es sich um den Trojaner Emotet, bekannt auch als Heodo.

Warnung der Melde- und Analysestelle MELANI vom 12. Dezember 2018 zu Emotet im Wortlaut



Grafik: MELANI

Die grafische Darstellung des Infektionsablaufes von Emotet durch MELANI.

Ursprünglich als E-Banking-Trojaner bekannt, wird Emotet heute vor allem für den Versand von Spam sowie das Nachladen von weiterer Schadsoftware verwendet.

200 000 Franken und mehr

Gemäss Informationen, die MELANI vorliegen, wird Emotet aktiv dazu verwendet, um gezielt Computer und Server in Unternehmensnetzwerken mit einem Verschlüsselungstrojaner (Ransomware) namens Ryuk zu infizieren. Dabei verschlüsselt Ryuk auf dem Computer oder Server abgelegte Dateien und fordert nach erfolgter Verschlüsselung vom betroffenen Unternehmen eine erhebliche Summe an Lösegeld, 200 000 Franken und mehr.

MELANI empfiehlt

- Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten. Die Sicherungskopie sollte offline auf einem externen Medium wie einer externen Festplatte gespeichert werden.
- Stellen Sie daher sicher, dass Sie das Medium, auf welche Sie die Sicherungskopie erstellen, nach dem Back-up-Vorgang vom Computer bzw. Netzwerk trennen. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium unbrauchbar.
- Betriebssysteme und alle auf den Computern und Servern installierten Applikationen müssen konsequent auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update-Funktion.
- Netzwerk-Segmentierung nach unterschiedlichen Vertrauenszonen, Anwendungsbereichen und Regionen.
- Einhalten des Prinzips der minimalen Rechtevergabe besonders auch bei Netzwerklaufwerken (es sollte kein Benutzer Zugang zu allen Daten haben, wenn er diesen Zugang gar nicht benötigt).
- Verwenden von dedizierten Geräten mit keinem oder nur eingeschränktem Internet-Zugang für das Management der Systeme sowie für das Durchführen von Zahlungen.

Technisch unterbinden

MELANI empfiehlt den Unternehmen und den Betreibern kritischer Infrastrukturen zudem:

- Den Empfang von Office Dokumenten, die Makros enthalten, auf dem E-Mail Gateway bzw. Spam-Filter technisch zu unterbinden.
- Das Ausführen von unsignierten Office-Makros zu unterbinden.
- Um eine Infektion durch Emotet zu verhindern sowie das Nachladen von weiterer Schadsoftware zu unterbinden empfiehlt MELANI, jene Webseiten, die aktiv für die Verbreitung von Emotet verwendet werden, am Netzwerkperimeter zu sperren.
- Eine Liste von solchen Webseiten wird von abuse.ch gestellt:
- MELANI rät, die Netzwerk-Kommunikation mit Servern, die zur Steuerung von mit Emotet infizierten Geräten verwendet werden, zu blockieren. Eine Liste von IP-Adressen, die Emotet zugeordnet werden können, werden unter anderem von Feodo Tracker publiziert.

mel.