how to not emotet?

binbash

07.01.2020

Übersicht

- Was ist dieses emotet überhaupt?
  - Übersicht
  - Zeitlicher Verlauf
  - Zusammenfassung
  - Schutz vor Emotet
- Exkurs: #JLUoffline
- Ausblick
- ~~Saufen~~

Übersicht Emotet

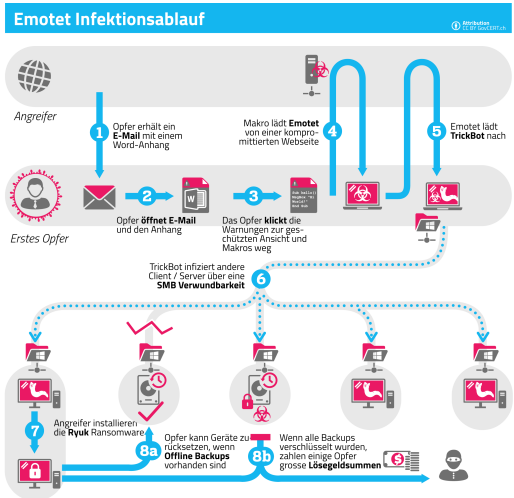

Abbildung 1: Infektionsverlauf
(Quelle:https://www.netzwoche.ch/sites/default/files/119835.png)

Übersicht Emotet (2)

- Angriff auf Outlook-Nutzer*innen
- Nutzt “Massen-Spearphishing” (Heise: “Dynamit-Phishing”)
  - Eigentlich: Gezielter und informierter Angriff auf Einzelpersonen
  - Hier:
    - Makros für Microsoft Word in DOC-Dateien werden ausgenutzt
    - Spionage von Mailaktivität
    - Mail mit Schadsoftware an plausible Kontakte (“Sozialer Graph” + extrem zugeschnittene Mails)
    - Optional: Ransomware, Cryptolocker oder manueller Zugriff

Zeitlicher Verlauf zu Emotet

Erste Beschreibung des ursprünglichen Trojaners durch TrendMicro (Schlangenöl)

- 11.06.2014: Aufnahme in deren Datenbank
- 27.06.2014: Erster Blogpost mit detaillierter Beschreibung

Zentrale Ansprechstelle Cybercrime (LKA Niedersachsen) zur modernisierten Fassung

- Warnung in Vergangenheitsform am 05.12.2018

Warnungen vom BSI und Heise

- Warnung in Vergangenheitsform am 06.12.2018

Zusammenfassung Emotet

- Technisch nichts bahnbrechend Neues
- Probleme sind seit Jahren und Jahrzehnten bekannt
- Betroffene Organisationen haben Gemeinsamkeiten
  - Ungepatchte Systeme
  - Makros
  - Windows + Outlook + Word
  - Wenig Ressourcen für IT
  - Wenig geschultes Personal
  - Teilweise: Admin-Accounts für tägliche Nutzung am Arbeitsplatzrechner

Schutz vor Emotet

- Kein Windows/Outlook/Word
- Installation von Sicherheitsupdates
- Deaktivierung von Makros über Gruppenrichtlinien
  - vollständig
  - Signierung eigener Makros
- Trennung von Abteilungen/Organisationen durch Firewalls & Zugriffsberechtigungen
- Regelmäßige Übungen zur Erhöhung der Achtsamkeit
- So wenige Computer einsetzen wie möglich

#JLUoffline (1)

- Infektion über Emotet –> Ransomware Ryuk
- Infrastruktur wird am 08.12.2019 heruntergefahren
  - Webauftritt verschwindet
  - keine Bücherausleihe möglich
  - Koordination über gmail-Adressen, twitter und Whatsapp
- Handgeschriebene Webseite (“index.html”) geht online
- Ausfall eines Teils der *HessenBox*

#JLUoffline (2)

- Manuelle Ausgabe von Passwörtern an 38.000 Personen
  - 60% bis Weihnachten, neue Runde im Januar
  - Suche nach rechtlich sicherer Lösung für das Vermitteln von Passwörtern an Betroffene im Ausland, im Feld, u.ä.
- Manuelles Scannen von PCs mit *desinfec't*
  - Zwei Aufkleber = ist sauber

#JLUoffline (3)

- Spekulative Ableitungen aus Handlungen auf Strukturen
  - Keine ausreichende zentrale Verwaltung der Rechner mit Management-Tools (z.B.: puppet, FAI, OPSI)
  - Nicht genügend IT-Personal
  - Keine Gruppenrichtlinien
  - keine signierten oder deaktiverten Makros
  - keine Trennung zwischen Buchrückgabesystemen und Netzlaufwerken

Keine Digitalstrategie, die diesen Namen verdient

#JLUoffline (4)

- ABER: Eine Uni-IT zu betreiben, ist wie einen Sack Flöhe zu hüten
  - Uni Marburg: 982 offene Dienste in Shodan

Abbildung 2: Shodan zur Uni Marburg

#JLUoffline (5)

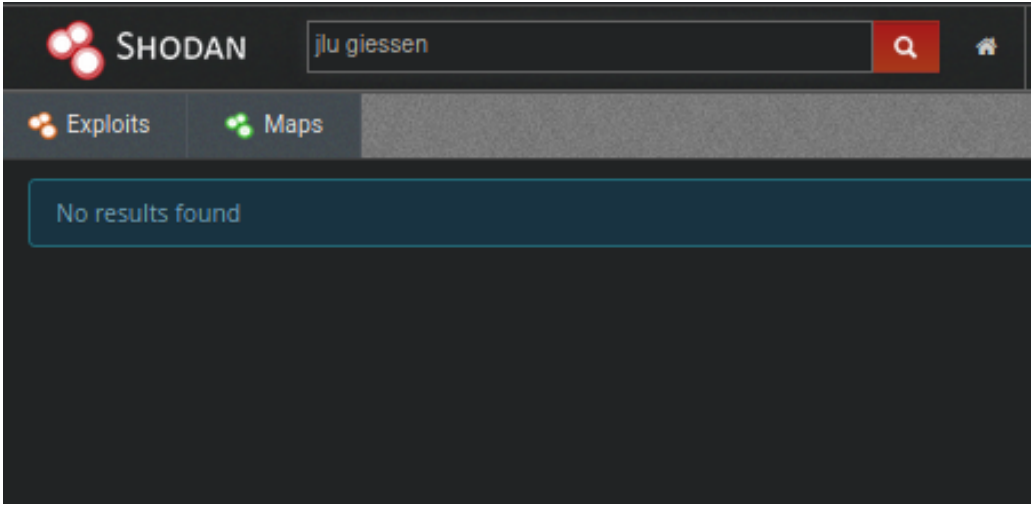

Abbildung 3: Online-Präsenz der JLU Gießen

#JLUoffline (6)

- Stand der Dinge
  - Neue Webseite in Plone
    - (= Uni Marburg)
    - Plone: Kein CVE seit 2018
    - Weiterhin: index.html
  - Diverse Dienste gehen diese Woche wieder online
  - Vielleicht bald größeres Budget für IT?

Ausblick

- Überkomplexe Strukturen sind anfällig
  - Linus überblickt den Kernel nicht mehr
  - Virtualisierung, Container und Managementsoftware sollen helfen
    - Security-Audit bei Kubernetes sagt, es ist zu komplex
- Wettbewerbsdenken und Verdienstmöglichkeiten fördern Verwahrlosung von IT-Infrastruktur
  - Keine Ressourcen für gute IT vorhanden
  - Ausnutzen von Schwachstellen lukrativer als fixen

Ausblick (2)

- Zeitnah eine Schreinerei eröffnen, irgendwas mit Blumen anfangen oder Alkoholismus entwickeln, denn:
  - Alles schlimm
  - Wird wohl schlimmer
  - ;____;
- Realistischerweise:
  - Menschen statt Technik als Angriffsziel
  - Marode Infrastruktur MUSS aktualisiert werden
- Jobgarantie für Datenreisende. Was das *den Steuerzahler* wieder kostet!

Weitere Informationen

- Erste Beschreibung bei TrendMicro: https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/
- c't: Was macht den Emotet-Trojaner so gefährlich? | nachgehakt: https://www.youtube.com/watch?v=XPl06aQivZk
- BSI: Aktuelle Information zur Schadsoftware Emotet: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html
- Linus Neumann: Hirne hacken: https://media.ccc.de/v/36c3-11175-hirne_hacken
- Frank Rieger und Ron: Security Nightmares 20: https://media.ccc.de/v/36c3-11164-security_nightmares_0x14